PENGEMBANGAN PERANGKAT LUNAK UNTUK SIMULASI *SCHNORR AUTHENTICATION DAN DIGITAL SIGNATURE SCHEME*

SKRIPSI

Untuk memenuhi sebagian persyaratan

Mencapai derajat sarjana S-1

DISUSUN OLEH:

JUSMAIL

(NIM : 06650029)

Kepada

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2011

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1204/2011

Skripsi/Tugas Akhir dengan judul	:	Pengembangan Perangkat Lunak untuk Simulasi Schnorr Authentication Dan Digital Signature Scheme
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Jusmail
NIM	:	06650029
Telah dimunaqasyahkan pada	:	27 Juni 2011
Nilai Munaqasyah	:	A / B

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Lukman Heryawan, M.T

Penguji I

Sumarsono,S.T, M.Kom
NIP.19710209 200501 1 003

Penguji II

Agung Fatwanto, S.Si, M.Kom
NIP. 19770103 200501 1 003

Yogyakarta, 1 Juli 2011
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA FAKULTAS SAINS DAN TEKNOLOGI YOGYAKARTA UIN SUNAN KALIJAGA

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

SURAT PERSETUJUAN SKRIPSI / TUGAS AKHIR

Hal : Permohonan
Lamp : -

Kepada
Yth. Dekan Fakultas Sains & Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Jusmail
NIM : 06650029
Judul Skripsi : Pengembangan Perangkat Lunak Untuk Simulasi *Schnorr Authentication dan Digital Signature Scheme.*

sudah dapat diajukan kembali kepada Fakultas Sains & Teknologi Jurusan / Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr.wb

Yogyakarta, 20 Juni 2011
Pembimbing I

Lukman Heryawan, M.T
NIP.

SURAT PERSETUJUAN SKRIPSI / TUGAS AKHIR

Hal : Permohonan
Lamp : -

Kepada
Yth. Dekan Fakultas Sains & Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Jusmail
NIM : 06650029
Judul Skripsi : Pengembangan Perangkat Lunak Untuk Simulasi *Schnorr Authentication dan Digital Signature Scheme.*

sudah dapat diajukan kembali kepada Fakultas Sains & Teknologi Jurusan/ Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr.wb

Yogyakarta, 20 Juni 2011
Pembimbing II

Bambang Sugiantoro, M.T
NIP.19751024 2009 12 1 0 002

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini:

Nama	:	Jusmail
NIM	:	06650029
Program Studi	:	Teknik Informatika
Fakultas	:	Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"PENGEMBANGAN PERANGKAT LUNAK UNTUK SIMULASI *SCHNORR AUTHENTICATION DAN DIGITAL SIGNATURE SCHEME*"** tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 20 Juni 2011

METERAI TEMPEL
PAJAK MEMBANGUN BANGSA
TGL. 20
31C3EAAF402628348
ENAM RIBU RUPIAH
6000 DJP

Mahasiswa

Jusmail

NIM. 06650029

KATA PENGANTAR

بسم الله الرحمن الرحيم

الحمد الذى جعلنا من الناصحين, وأفهمنامن علوم العلماءالراسخين, والصلاة والسلام على من تسخ دينه أديان الكفرة والطالحين, وعلى آله وأصحابه الذين كانو يتمسك شريعة صالحين.

Alhamdulillah akhirnya penulis dapat menyelesaikan penelitian tugas akhir yang berjudul Pengembangan Perangkat Lunak Untuk Simulasi *Schnorr Authentication dan Digital Signature Scheme*. Sebuah perangakat lunak yang membantu proses pemahaman terhadap konsep kerja dari *Schnorr Authentication dan Digital Signature Scheme*. Oleh karena itu, dengan segala kerendahan hati pada kesempatan ini penulis mengucapkan banyak terima kasih kepada:

1. Ibunda dan ayahanda tercinta, ketiga adik-adikku serta keluarga yang senantiasa mendo'akan, memotivasi, dan memberikan semangat kepada penulis.
2. Bapak Prof. Drs. H. Akh. Minhaji, M.A. Ph.D, selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
3. Bapak Agus Mulyanto, M.Kom, selaku ketua Program Studi Teknik Informatika UIN Sunan Kalijaga.
4. Bapak Lukman Heryawan, M.T selaku Dosen Pembimbing I atas bimbingan, arahan dalam penyusunan skripsi.

5. Bapak Bambang Sugiantoro, M.T selaku Dosen Pembimbing II yang telah memberikan saran dan masukkan kepada penulis dalam menyusun skripsi.
6. Para Dosen Teknik Informatika UIN Sunan Kalijaga yang telah memberikan banyak bekal ilmu kepada penulis.
7. Semua pihak yang telah memberikan bantuan dan dukungan kepada penulis dalam penyusunan skripsi yang tidak dapat disebutkan satu per satu.

Akhir kata, semoga Allah *Subhanahu wa ta'ala* memberikan balasan kebaikan atas segala bantuan yang telah diberikan kepada penulis. Amin

Yogyakarta, 20 Juni 2011

Penulis

HALAMAN PERSEMBAHAN

Skripsi ini kupersembahkan untuk :

- Sujud syukurku kepada Allah Swt atas segala kenikmatan, kemudahan, dan hidayah-Nya
- Sholawat serta salam kepada Sayyidina Rasulullah Muhammad Saw dan para keluarga, sahabat dan para pengikutnya
- Ibunda dan ayahanda, adik-adiku zulhin jafar, kasmida, urfiyatul adawiyyah dan keluarga untuk semua kebaikan, doa, motivasi, serta kasih sayang yang tak tergantikan
- Sahabat-sahabatku, baik di organisasi intra kampus BEM-F '10 maupun ekstra kampus PMII Rayon Saintek , seluruh salessrungkku di Asrama Arung Palakka Bone.
- Teman-teman Teknik Informatika 2005, 2006, 2007 yang tidak dapat kusebutkan satu per satu namun tidak mengikiskan terima kasih penulis yang terdalam kepada mereka semua.
- Semua orang yang telah berjasa dalam hidupku, jazakumullah khoiron katsiron untuk segala kebaikannya, semoga Allah *subhanahu wa ta 'ala* membalas kebaikan kalian semua. Amin.

HALAMAN MOTTO

قَالُواْ سُبۡحَٰنَكَ لَا عِلۡمَ لَنَآ إِلَّا مَا عَلَّمۡتَنَآۖ إِنَّكَ أَنتَ ٱلۡعَلِيمُ ٱلۡحَكِيمُ ٣٢

"Mereka menjawab: "Maha Suci Engkau, tidak ada yang kami ketahui selain dari apa yang Telah Engkau ajarkan kepada Kami; Sesungguhnya Engkaulah yang Maha mengetahui lagi Maha Bijaksana" (Al-Baqaroh : 32)

فَكِّرْ مُسْتَقْبَلَكَ العَاجِلَ , وَالأَجِلْ وَحَافِظْ عَلَى أَوْقَاتِكَ , فَإِنَّ ٱلْمَشَقَّةَ فِى البِدَايَةِ خَيْراً مِنَ النَّدَامَةِ فِى النِّهَا يَةِ

"Malam itu Panjang, maka jangan kau persingkat dengan tidurmu, sedangkan siang itu penuh cahaya, maka jangan kau kotori dengan perbuatan-perbuatan dosamu." (yahya bin muadz)

"All things are difficult before they are easy and success doesn't come to you but you go to it, don't ever take off till you get it."

Jangan jadi ikan mati, tapi jadilah seperti ikan yang hidup (KH.Helmi Abdul mubin Lc)

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

PENGEMBANGAN PERANGKAT LUNAK UNTUK SIMULASI
SCHNORR AUTHENTICATION DAN DIGITAL SIGNATURE SCHEME

JUSMAIL
NIM. 06650029

INTISARI

Otentikasi *(authentication)* merupakan identifikasi yang dilakukan oleh masing-masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapatkan oleh satu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian informasi yang diterima. Identifikasi terhadap suatu informasi dapat berupa tanggal pembuatan informasi, isi informasi, waktu kirim dan hal-hal lainnya yang berhubungan dengan informasi tersebut. Tanda tangan digital adalah suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Skema yang dapat digunakan untuk melakukan proses tanda tangan digital terhadap suatu pesan juga bermacam-macam. Salah satunya adalah skema Schnorr Authentication dan Digital Signature. Skema Schnorr Authentication dan Digital Signature merupakan skema tanda tangan digital yang mengambil keamanan dari permasalahan menghitung logaritma diskrit. Skema tanda tangan ini menggunakan bilangan prima dan perpangkatan modulo dalam proses pembentukan kuncinya. Skema otentikasi dapat dimodifikasi menjadi skema tanda tangan digital (*digital signature*). Proses pembentukan kunci privat dan publiknya sama seperti sekema otentikasi, namun pada skema tanda tangan digital ditambahkan sebuah fungsi *hash.*

Pengembangan sistem yang digunakan dalam membangun perangkat lunak ini adalah metode *waterfall* (siklus air terjun). Perangkat lunak untuk simulasi schnorr authentication dan Digital signature scheme ini akan membantu pemahaman kriptografi terutama mengenai Shcnorr Authentication dan Digital Signature Scheme dan perangkat lunak ini juga dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar mencakup input variabel-variabel, kunci privat, kunci public, pesan, pembentukkan digital signature, proses verifikasi dan proses deskripsi.

Software yang digunakan dalam pembuatan perangkat lunak ini adalah Microsoft Visual Basic 6.0. Fitur- fitur yang ada seperti tampilan animasi saat membuka halaman menu, ilustrasi proses pengiriman informasi dan langkah per langkah dari proses perhitungan yang dilakukan.

Kata kunci : Otentikasi, Kriptografi, Schnorr Authentication dan Digital Signature Scheme, Visual Basic 6.0.

DEVELOPMENT OF SOFTWARE FOR THE SIMULATION
SCHNORR AUTHENTICATION AND DIGITAL SIGNATURE SCHEME

JUSMAIL
NIM. 06650029

ABSTRACT

Authentication is an identification made by each party to communicate with each other, meaning several parties communicating must identify each other. The information obtained by one party from another party must be identified to ensure the authenticity of the information received. Identification of the information may include the date of manufacture information, information content, delivery times and other matters relating to such information. Digital signature is an authentication mechanism that allows the manufacturer to add a code message which acts as a signature. Schemes that can be used to make the process of digital signature to a message also varies. One is the scheme of Schnorr Authentication and Digital Signature. Schnorr scheme Authentication and Digital Signature is a digital signature scheme that takes the security of calculating the discrete logarithm problem. This signature scheme using modulo powers of primes and in the process of formation of the key. Authentication scheme can be modified into a scheme of digital signature. The process of forming public and private key as scheme authentication, but in the scheme of digital signatures added to a hash function.

Development of systems used in building this software is a method of waterfall (the waterfall cycle). Schnorr simulation software for authentication and digital signature scheme will help the understanding of cryptography, especially regarding Shcnorr Authentication and Digital Signature Scheme and the software can also be used as support facilities in the learning process includes the input variables, the private key, public key, the message ,the creation of digital signatures, verification processes and process descriptions.

Software used in the manufacture of this software is Microsoft Visual Basic 6.0. Existing features such as view animations when opening menu page, the illustration process of sending information and step by step of the process of calculations performed.

Keywords: Authentication, Cryptography, Schnorr Authentication and Digital Signature Scheme, Visual Basic 6.0.

PENGEMBANGAN PERANGKAT LUNAK UNTUK SIMULASI
SCHNORR AUTHENTICATION DAN DIGITAL SIGNATURE SCHEME

JUSMAIL
NIM. 06650029

INTISARI

Otentikasi *(authentication)* merupakan identifikasi yang dilakukan oleh masing-masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapatkan oleh satu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian informasi yang diterima. Identifikasi terhadap suatu informasi dapat berupa tanggal pembuatan informasi, isi informasi, waktu kirim dan hal-hal lainnya yang berhubungan dengan informasi tersebut. Tanda tangan digital adalah suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Skema yang dapat digunakan untuk melakukan proses tanda tangan digital terhadap suatu pesan juga bermacam-macam. Salah satunya adalah skema Schnorr Authentication dan Digital Signature. Skema Schnorr Authentication dan Digital Signature merupakan skema tanda tangan digital yang mengambil keamanan dari permasalahan menghitung logaritma diskrit. Skema tanda tangan ini menggunakan bilangan prima dan perpangkatan modulo dalam proses pembentukan kuncinya. Skema otentikasi dapat dimodifikasi menjadi skema tanda tangan digital (*digital signature*). Proses pembentukan kunci privat dan publiknya sama seperti sekema otentikasi, namun pada skema tanda tangan digital ditambahkan sebuah fungsi *hash.*

Pengembangan sistem yang digunakan dalam membangun perangkat lunak ini adalah metode *waterfall* (siklus air terjun). Perangkat lunak untuk simulasi schnorr authentication dan Digital signature scheme ini akan membantu pemahaman kriptografi terutama mengenai Shcnorr Authentication dan Digital Signature Scheme dan perangkat lunak ini juga dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar mencakup input variabel-variabel, kunci privat, kunci public, pesan, pembentukkan digital signature, proses verifikasi dan proses deskripsi.

Software yang digunakan dalam pembuatan perangkat lunak ini adalah Microsoft Visual Basic 6.0. Fitur- fitur yang ada seperti tampilan animasi saat membuka halaman menu, ilustrasi proses pengiriman informasi dan langkah per langkah dari proses perhitungan yang dilakukan.

Kata kunci : Otentikasi, Kriptografi, Schnorr Authentication dan Digital Signature Scheme, Visual Basic 6.0.

DEVELOPMENT OF SOFTWARE FOR THE SIMULATION
SCHNORR AUTHENTICATION AND DIGITAL SIGNATURE SCHEME

JUSMAIL
NIM. 06650029

ABSTRACT

Authentication is an identification made by each party to communicate with each other, meaning several parties communicating must identify each other. The information obtained by one party from another party must be identified to ensure the authenticity of the information received. Identification of the information may include the date of manufacture information, information content, delivery times and other matters relating to such information. Digital signature is an authentication mechanism that allows the manufacturer to add a code message which acts as a signature. Schemes that can be used to make the process of digital signature to a message also varies. One is the scheme of Schnorr Authentication and Digital Signature. Schnorr scheme Authentication and Digital Signature is a digital signature scheme that takes the security of calculating the discrete logarithm problem. This signature scheme using modulo powers of primes and in the process of formation of the key. Authentication scheme can be modified into a scheme of digital signature. The process of forming public and private key as scheme authentication, but in the scheme of digital signatures added to a hash function.

Development of systems used in building this software is a method of waterfall (the waterfall cycle). Schnorr simulation software for authentication and digital signature scheme will help the understanding of cryptography, especially regarding Shcnorr Authentication and Digital Signature Scheme and the software can also be used as support facilities in the learning process includes the input variables, the private key, public key, the message ,the creation of digital signatures, verification processes and process descriptions.

Software used in the manufacture of this software is Microsoft Visual Basic 6.0. Existing features such as view animations when opening menu page, the illustration process of sending information and step by step of the process of calculations performed.

Keywords: Authentication, Cryptography, Schnorr Authentication and Digital Signature Scheme, Visual Basic 6.0.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Otentikasi (*authentication*) merupakan identifikasi yang dilakukan oleh masing-masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian dari informasi yang diterima. Identifikasi terhadap suatu informasi dapat berupa tanggal pembuatan informasi, isi informasi, waktu kirim dan hal-hal lainnya yang berhubungan dengan informasi tersebut. Otentikasi pesan memang berhasil melindungi kedua belah pihak yang saling bertukar pesan dari pihak ketiga. Tetapi, otentikasi pesan tidak bisa mencegah kemungkinan kedua belah pihak saling menyerang satu sama lain. Pada situasi dimana tidak ada kepercayaan penuh antara pengirim dan penerima pesan, diperlukan suatu mekanisme yang lebih daripada sekedar otentikasi. Solusi yang paling menarik dari masalah ini adalah tanda tangan digital (*digital signature*). Tanda tangan digital adalah suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tanda tangan tersebut menjamin integritas dan sumber dari sebuah pesan.

Claus Schnorr's *authentication* dan *digital signature scheme* mengambil sekuritas dari permasalahan menghitung logaritma diskrit. Skema ini menggunakan

bilangan prima dan perpangkatan modulo dalam proses pembentukan kuncinya. Skema ini dipatenkan di Amerika Serikat dan berakhir pada tanggal 19 Pebruari 2008. Skema otentikasi dapat dimodifikasi menjadi skema tanda tanda digital (*digital signature scheme*). Proses pembentukan kunci privat dan publiknya sama seperti skema otentikasi, hanya saja pada skema tanda tangan digital ditambahkan sebuah fungsi *hash*.

Prangkat lunak untuk simulasi schnorr authentikasi dan digital signature scheme merupakan pokok dari aplikasi yang penulis kembangkan dan rancang untuk memudakan pemahaman tentang konsep kerja schnorr authentikasi dan digital signature skema. Berdasarkan uraian di atas, penulis bermaksud untuk mengambil tugas akhir (skripsi) dengan judul "*Pengembangan Perangkat Lunak Untuk Simulasi Schnorr Authentication Dan Digital Signature Scheme* ".

1.2 Rumusan Masalah

Yang menjadi rumusan masalah dalam menyusun tugas akhir (skripsi) ini adalah bagaimana mensimulasikan prosedur kerja dari *schnorr authentication* dan *digital signature scheme*.

1.3 Batasan Masalah

Pembatasan permasalahan dalam membuat perangkat lunak simulasi *schnorr authentication* dan *digital signature scheme* adalah sebagai berikut:

1. Perangkat lunak akan menampilkan tahap-tahap perhitungan dalam bentuk desimal.
2. Perangkat lunak menyediakan teori-teori dasar dari schnorr *authentication* dan *digital signature scheme*.
3. Perangkat lunak akan menjelaskan prosedur kerja dengan menggunakan bantuan animasi gambar.
4. Pihak yang berinteraksi adalah 2 orang, yaitu Alice sebagai pihak pertama dan Bob sebagai pihak kedua.
5. Algoritma pendukung yang digunakan dalam skema schnorr adalah:
    a. Untuk menentukan sifat relatif prima, digunakan algoritma *Greatest Common Divisor* (GCD).
    b. Untuk menentukan sifat prima dari sebuah bilangan, digunakan algoritma tes prima Rabin Miller.
    c. Perpangkatan modulo bilangan besar menggunakan algoritma *Fast Exponentiation*.
    d. Operasi inversi modulo menggunakan algoritma *Extended Euclidean*.
    e. Fungsi *hash* yang digunakan adalah fungsi SHA-1.
6. *Input* data berupa:
    a. Pesan (*message*) dengan panjang maksimal 50 karakter (dalam skema tanda tangan digital).
    b. Bilangan prima p, dibatasi maksimal 9 digit *integer* positif.

c. Bilangan prima q (Untuk memenuhi nilai q yang sesuai dengan syarat skema Schnorr, maka panjang bit variabel q harus sekitar $^1/_3$ dari panjang bit variabel p), dibatasi maksimal 3 digit *integer* positif.

d. Nilai a (harus memenuhi syarat: a^q mod p = 1), dibatasi maksimal 5 digit *integer* positif.

e. Nilai s (harus lebih kecil dari q), dibatasi maksimal 3 digit *integer* positif.

f. Nilai r (harus lebih kecil dari q), dibatasi maksimal 3 digit *integer* positif.

g. Nilai e, dibatasi maksimal 9 digit *integer* positif.

1.4 Tujuan

Tujuan penyusunan tugas akhir (skripsi) ini adalah memahami *Schnorr Authentication* dan *Digital Signature Scheme*, serta membuat suatu perangkat lunak untuk membantu proses pemahaman terhadap *Schnorr Authentication* dan *Digital Signature Scheme*.

1.5 Manfaat

Manfaat dari penyusunan tugas akhir (skripsi) ini yaitu :

1. Bagi penulis sendiri, dapat membantu pemahaman terhadap *Schnorr Authentication* dan *Digital Signature Scheme*, serta dapat meningkatkan kemampuan pembuatan perangkat lunak dengan menggunakan bahasa pemrograman *Visual Basic* 6.0.

2. Bagi pembaca, dapat digunakan sebagai alat bantu dalam memahami *Schnorr Authentication* dan *Digital Signature Scheme* serta dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar.

1.6 Keaslian Penelitian.

Penelitian ini menitik beratkan pada bagaimana perangkat lunak ini mensimulasikan konsep kerja dari *Schnorr Authentication* dan *Digital Signature Scheme*. Perangkat Lunak ini dikembangkan dengan mengunakan bahasa pemograman *Visual Basic* 6.0.

Pada alur kerja pengembangan perangkat lunak, perancangan tampilan animasi, proses pembentukan kunci, proses kerja skema otentikasi (*authentication*), proses kerja skema tanda tangan digital (*digital signature scheme*) dan penjelasan terhadap *form-form* yang terdapat di dalam perangkat lunak.

Pada arus kerja secara keseluruhan dari sistem dalam perangkat lunak untuk simulasi *schnorr authentication dan digital signature Scheme* ini menggunakan bagan alir sistem (*system flowchart*). Bagan ini menjelaskan urut- urutan dari prosedur-prosedur yang ada di dalam sistem. Diagram alir ini akan menjelaskan proses dan prosedur yang terjadi pada aplikasi dengan simbol-simbol tertentu sehingga dapat menggambarkan algoritma yang terjadi. Dengan penggunaan *flowchart* memungkinkan penggambaran keseluruhan dari pengambilan data awal hingga dihasilkan keluaran yang diinginkan. Sehingga sangat membantu dalam

mengetahui jalan sistem dari proses awal hingga akhir dan mempermudah bagi orang untuk memahami alur data yang berjalan dalam sistem.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah menyelesaikan perangkat lunak untuk simulasi *Schnorr Authentication* dan *Digital Signature Scheme*, penulis menarik kesimpulan sebagai berikut:

a. Hasil rancangan perangkat lunak dapat membantu pemahaman terhadap skema Schnorr, baik skema otentikasi maupun skema tanda tangan digital. Perangkat lunak dapat digunakan untuk mendukung kegiatan belajar mengajar, terutama dalam mata kuliah Kriptografi.

b. Perangkat lunak juga menyediakan layar teori yang berisi dasar-dasar teori dari algoritma-algoritma yang berada di dalam kedua skema schnorr tersebut. Berdasarkan hasil pengujian *usabilitas* perangkat lunak untuk *simulasi schnorr authentication dan digital signature scheme,* diperoleh kesimpulan bahwa perangkat lunak tersebut menurut sebagian besar pengguna telah bekerja sesuai harapan, sehingga dapat membantu pemahaman terhadap konsep *schnorr authenticatation dan digital signature.*

5.2 Saran

Penulis ingin memberikan beberapa saran yang mungkin dapat membantu dalam pengembangan perangkat lunak ini yaitu :

a. Perangkat lunak dapat dikembangkan menjadi sebuah aplikasi *text editor* yang memberikan fasilitas tanda tangan digital (*digital signature*), sehingga diharapkan dapat digunakan oleh *user* dalam kehidupan sehari-hari.

b. Perangkat lunak dapat dikembangkan dengan menambahkan kriptanalisis terhadap skema Schnorr yang dibahas, sehingga dapat memberikan gambaran mengenai keamanan yang diberikan oleh Schnorr. Sekuritas skema Schnorr berada pada permasalahan mencari logaritma diskrit. Pada proses pembentukan kunci, kunci publik (v) dihasilkan dengan rumus: $v = a^{-s} \bmod p$. Untuk mendapatkan kunci privat (s), maka penyerang (*attacker*) harus mampu menghitung $a^{-s} \equiv v \pmod p$. Ini merupakan permasalahan yang sulit dipecahkan.

DAFTAR PUSTAKA

Agustia, Paul L. 2005, *Perancangan Perangkat Lunak Bantu Pemahaman Masalah Faktorisasi, Perpangkatan Modulo dan Bilangan Prima,* Tugas Akhir STMIK-Mikroskil, Medan.

Cormen, Thomas H. 2004, *Introduction to Algorithms Second Edition*, The Massachusetts Intitute of Technology, North America.

Hafid, Ahmad. 2011, "Aplikasi Bantu Pembelajaran *Digital Signature* dengan Metode *Ong-Schnorr-Shamir*", Skripsi, Universitas Pembangunan Nasional "Veteran" Yogyakarta, Yogyakarta.

Kurniawan, Jusuf. 2004, *Kriptografi, Keamanan Internet dan Jaringan Komunikasi*, Penerbit Informatika Bandung.

Kurniasari, Amy. 2010, *Authentikasi User dalam Sistem Informasi Berbasis WEB.http://blog.unsri.ac.id/userfiles/Autentifikasi%20user(1).doc* Akses pada tanggal 02 Juni 2010.

Kurniawan, Agus, 2008. *Konsep dan Implementasi Cryptography dengan .NET*, Dian Rakyat, Jakarta.

Nugroho, Adi, 2005, "*Analisis dan Perancangan Sistem Informasi dengan Metodologi Berorientasi Obyek*", Informatika, Bandung.

Pandia, Henry, 2002. *Visual Basic 6 Tingkat Lanjut,* Andi Yogyakarta.

Pramono, Djoko. 2002, *Mudah menguasai Visual Basic 6,* PT. Elex Media Komputindo.

Presman, Roger S., Ph.D, 2002, *Rekayasa Perangkat Lunak: Pendekatan Praktisi*, Andi Offset, Yogyakarta.

Rahmayanti, Desi. 2007, Aplikasi digital signature sebagai autentikasi Pada kartu tanda penduduk (Ktp), Institut Teknologi Bandun, Bandung.

Schneier, Bruce.1996, *Applied Crytography*, *Second Edition*. United States of America.

Sugiyono, 2010. Metode Penelitian Pendidikan. Pendekatan Kuantitatif, Kualitatif dan R&D. Alfabeta Bandung.

Stallings, William. 2003, *Cryptography and Network Security*, *Third Edition*. United States of America.

LAMPIRAN A

Source Code

Form frmSplash.frm

```
Option Explicit
Private Sub Command1_Click()
Unload Me
Screen.MousePointer = vbDefault
 frmMenu.Show
End Sub

Private Sub cmdOK_Click(Index As Integer)
Unload Me
Screen.MousePointer = vbDefault
 frmMenu.Show
End Sub

Private Sub Form_KeyPress(KeyAscii As Integer)
    Unload Me
End Sub

Private Sub Frame1_Click()
    Unload Me
End Sub

Private Sub lblPlatform_Click()

End Sub

Private Sub Text1_Change()

End Sub

Private Sub Label1_Click()

End Sub

Private Sub Picture1_Click()

End Sub

Private Sub Image1_Click()

End Sub
```

Form frmMenu.frm

```
Option Explicit
Const LOrange = &H80C0FF
Const DOrange = &H80FF&
```

```
Private Sub cmdAbout_Click()
    frmAbout.Show vbModal
End Sub

Private Sub cmdAbout_MouseMove(Button As Integer, Shift As Integer,
X As Single, Y As Single)
    If lblInfo.Tag <> "5" Then
        'Keterangan
        lblInfo.Caption =
     "Informasi mengenai pembuat pengembangan perangkat lunak " & _
     "untuk simulasi schnorr authentikasi digital signeture scheme
dan sekaligus " & _
     "penyusun tugas akhir skripsi Strata-1 jurusan Teknik
Informatika " & _
     "Universitas Islam Negeri Sunan Kalijaga Yogyakarta."
        lblInfo.Tag = "5"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = DOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdAuthentication_Click()
    If P = 0 Or Q = 0 Or A = 0 Or S = 0 Or V = 0 Then
        MsgBox "Proses pembentukan kunci harus dijalankan sebelum
skema otentikasi.", vbCritical
    Else
        Me.Hide
        frmAuthentication.Show
    End If
End Sub

Private Sub cmdAuthentication_MouseMove(Button As Integer, Shift As
Integer, X As Single, Y As Single)
    If lblInfo.Tag <> "2" Then
        'Keterangan
        lblInfo.Caption =
        "Otentikasi (authentication) adalah layanan " & _
        "yang berhubungan dengan identifikasi, baik " & _
        "mengidentifikasi kebenaran pihak-pihak yang " & _
        "berkomunikasi (user authentication atau entity " & _
     "authentication) maupun mengidentifikasi kebenaran sumber " & _
    "pesan (data origin authentication). Dua pihak yang saling " & _
    "berkomunikasi harus dapat mengotentikasi satu sama lain
sehingga " & _
     "ia dapat memastikan sumber pesan."
        lblInfo.Tag = "2"
       'Warna tombol
```

```
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = DOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdDigitalSignature_Click()
    If P = 0 Or Q = 0 Or A = 0 Or S = 0 Or V = 0 Then
        MsgBox "Proses pembentukan kunci harus dijalankan sebelum
skema tanda tangan digital.",   vbCritical
    Else
        Me.Hide
        frmDigitalSign.Show
    End If
End Sub

Private Sub cmdDigitalSignature_MouseMove(Button As Integer, Shift
As Integer, X As Single, Y As Single)
    If lblInfo.Tag <> "3" Then
        'Keterangan
        lblInfo.Caption =
 "Tanda tangan digital adalah suatu mekanisme otentikasi " & _
 "yang memungkinkan pembuat pesan menambahkan sebuah kode " & _
 "yang bertindak sebagai tanda tangannya. Tanda tangan tersebut "& _
"menjamin integritas dan sumber dari sebuah pesan. Penandatanganan
digital " & _
 "terhadap suatu dokumen adalah sidik jari dari dokumen tersebut
yang dibentuk " & _
  "dengan menggunakan kunci privat pihak yang menandatangani. Tanda
tangan digital " & _
    "akan berbeda untuk dokumen yang berbeda."
        lblInfo.Tag = "3"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = DOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdKeluar_Click()
    End
End Sub

Private Sub cmdKeluar_MouseMove(Button As Integer, Shift As Integer,
X As Single, Y As Single)
    If lblInfo.Tag <> "6" Then
```

```
        'Keterangan
        lblInfo.Caption = "Keluar dari program."
        lblInfo.Tag = "6"

        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = DOrange
    End If
End Sub

Private Sub cmdKeyGeneration_Click()
    Me.Hide
    frmKeyGeneration.Show
End Sub

Private Sub cmdKeyGeneration_MouseMove(Button As Integer, Shift As
Integer, X As Single, Y As Single)
    If lblInfo.Tag <> "1" Then
        'Keterangan
        lblInfo.Caption =
      "Pembentukan kunci (key generation) merupakan proses " & _
       "pembentukan kunci privat dan kunci publik yang akan " & _
      "digunakan pada skema otentikasi (authentication) dan " & _
 "skema tanda tangan digital (digital signature). Kunci privat " & _
     "diketahui oleh pihak pertama (yang akan diverifikasi atau
diperiksa keabsahannya " & _
       "pada kedua skema tersebut) sedangkan kunci publik disebarkan
dan " & _
       "diketahui oleh pihak-pihak lain yang akan memeriksa keaslian
atau keabsahan " & _
           "data dari pihak pertama."
        lblInfo.Tag = "1"
        'Warna tombol
        cmdKeyGeneration.BackColor = DOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdTeori_Click()
    Me.Hide
    frmTeori.Show
End Sub

Private Sub cmdTeori_MouseMove(Button As Integer, Shift As Integer,
```

```
X As Single, Y As Single)
    If lblInfo.Tag <> "4" Then
        lblInfo.Caption = "Teori - Teori mengenai Skema Schnorr."
        lblInfo.Tag = "4"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = DOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub Picture1_MouseMove(Button As Integer, Shift As Integer,
X As Single, Y As Single)
    If lblInfo.Tag <> "0" Then
        'Keterangan
        lblInfo.Caption =
"PERHATIAN Dalam Menjalankan Perangkat Lunak Ini Seorang User" & _
"Harus Mengikuti Tahapan-tahapan dalam Prangkat Lunak " & _
   "Untuk Simulasi Schnorr Authentikasi dan Digital Signature" & _
  "Tahapan Pertama : KEY - GENERATION, Kedua : AUTHENTICATION" & _
                   "KeTiga : DIGIAL-SIGNATURE dan yang TEORI,
ABOUT, KELUAR " & _
 "Merupakan Menu Tambahan. Seorang User Tidak Bisa Langsung Ke
Tahapan Kedua tanpa melewati" & _
           "Tahapan Pertama, Jadi Seorang User Harus mengikuti
Tahapan-tahapan pada MENU"
        lblInfo.Tag = "0"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub
```

Form Key-Generation.frm

```
Option Explicit
Private Const nDelay = 800
Private I As Integer
Private Langkah As Integer
Private nAlice As Integer
Private Sub cmdKeluar_Click()
   Unload Me
End Sub
Private Sub cmdNext_Click()
```

```
    'Langkah algoritma berikutnya
    Langkah = Langkah + 1
    Call EksekusiAlgo(Langkah, True)
End Sub

Private Sub cmdPrev_Click()
    'Langkah algoritma sebelumnya
    Langkah = Langkah - 1
    Call EksekusiAlgo(Langkah, False)
End Sub

Private Sub cmdUlang_Click()
    MSFlexGrid1.Rows = 1
    MSFlexGrid2.Rows = 1
    Call ResetAlgo
End Sub

Private Sub Form_Load()
    'Ulang algoritma
    Call ResetAlgo
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub

Private Sub Text1_Change()
    Text1.SelStart = Len(Text1.Text)
End Sub

Private Sub TmrAlice_Timer()
    nAlice = nAlice + 1
    If nAlice = 5 Then nAlice = 1
    PicBoxAlice.Picture = LoadPicture(App.Path & "\Gambar\AliceB-" &
nAlice & ".bmp")
End Sub

Private Sub ResetAlgo()
    lblHeader = "ALICE SEBAGAI PIHAK PERTAMA YANG MEMBENTUK KUNCI"
    'Pasangan kunci
    P = 0
    A = 0
    Q = 0
    S = 0
    V = 0

    'Langkah algoritma
    Langkah = 0
    'TABEL VARIABEL
    With MSFlexGrid1
        .Cols = 2
        .Rows = 6
```

```
        .ColWidth(0) = 2000
        .ColAlignment(0) = 4

        .ColWidth(1) = 2500
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 6

        .TextMatrix(0, 0) = "VARIABEL"
        .TextMatrix(0, 1) = "NILAI"
        .TextMatrix(1, 0) = "p"
        .TextMatrix(2, 0) = "q"
        .TextMatrix(3, 0) = "a"
        .TextMatrix(4, 0) = "s (privat)"
        .TextMatrix(5, 0) = "v (publik)"
    End With

    'TABEL ALGORITMA
    With MSFlexGrid2
        .Cols = 2
        .Rows = 9
        .ColWidth(0) = 750
        .ColAlignment(0) = 4
        .ColWidth(1) = 5490
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 1

        .TextMatrix(0, 0) = "No."
        .TextMatrix(0, 1) = "Algoritma"
        .TextMatrix(1, 0) = "1."
        .TextMatrix(1, 1) = " Pilih 2 buah bilangan prima p dan q,"
        .TextMatrix(2, 1) = " dan sebuah nilai a, dimana "
        .TextMatrix(3, 1) = " GCD(q, p-1) <> 1 dan (a^q) mod p = 1."
        .TextMatrix(4, 0) = "2."
        .TextMatrix(4, 1) = " Pilih sebuah nilai s, dimana s < q."
        .TextMatrix(5, 1) = " (s adalah kunci privat)"
        .TextMatrix(6, 0) = "3."
        .TextMatrix(6, 1) = " Hitung nilai v dengan rumus berikut:"
        .TextMatrix(7, 1) = "     v = a^(-s) mod p"
        .TextMatrix(8, 1) = " (v adalah kunci publik)"
    End With

    'Keterangan proses
    Text1.Text = ""
    cmdNext.Enabled = True
    cmdPrev.Enabled = False
End Sub

Private Sub EksekusiAlgo(nBaris As Integer, bNext As Boolean)
    cmdPrev.Enabled = False
    cmdNext.Enabled = False
    cmdUlang.Enabled = False
    cmdKeluar.Enabled = False
```

```
    Select Case nBaris
        Case 0
                lblHeader = "Alice SEBAGAI PIHAK PERTAMA YANG
MEMBENTUK KUNCI"
                'Hapus warna hijau dari semua baris algo
                With MSFlexGrid2
                    'Hapus warna hijau pada baris algo-2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        .CellBackColor = White
                        .CellForeColor = 0
                    Next I
                End With
                Text1.Text = ""
                MSFlexGrid1.TextMatrix(1, 1) = ""
                MSFlexGrid1.TextMatrix(2, 1) = ""
                MSFlexGrid1.TextMatrix(3, 1) = ""

        Case 1
                lblHeader = "1. Alice memilih 2 buah bilangan prima
p dan q serta nilai a"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I <= 3 Then
                            'Warna hijau pada baris algo-1
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With
                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form p, q dan a
                    frmInputPQA.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = "1. Alice memilih nilai p, q dan a
sebagai berikut:"
                    'Isi nilai p
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                     "      p = " & P
                    MSFlexGrid1.TextMatrix(1, 1) = P
                    'Isi nilai q
                    Delay nDelay
```

```
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      q = " & Q
                    MSFlexGrid1.TextMatrix(2, 1) = Q
                    'Isi nilai a
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      a = " & A
                    MSFlexGrid1.TextMatrix(3, 1) = A
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Nilai tersebut memenuhi ketentuan bahwa:" &
vbCrLf & _
                    "   - p dan q adalah bilangan prima," & vbCrLf &
_
                    "   - GCD(q, p-1) tidak boleh bernilai 1," &
vbCrLf & _
                    "   - Nilai dari operasi (a^q) mod p harus
bernilai 1."
                    TmrAlice.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(4, 1) = ""
                    'hapus nomor 2.
                    Temp1 = InStr(1, Text1.Text, "2.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 2
                lblHeader = "2. Alice memilih nilai s (s < q)
sebagai kunci privat"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 4 Or I = 5 Then
                            'Warna hijau pada baris algo-2
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form s
                    frmInputS.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
```

```
                                "2. Alice memilih nilai s (s < q)."
                    'tampilkan nilai s
                    Delay nDelay
                    MSFlexGrid1.TextMatrix(4, 1) = S
                    Text1.Text = Text1.Text & vbCrLf & _
                                "      s = " & S & " (s adalah
kunci privat)"

                    TmrAlice.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(5, 1) = ""
                    'hapus nomor 3.
                    Temp1 = InStr(1, Text1.Text, "3.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 3
                lblHeader = "3. Alice menghitung nilai v sebagai
kunci publik"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I >= 6 Then
                            'Warna hijau pada baris algo-3
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Hitung nilai v
                    Temp1 = ExtendedEuclidean(A, P)
                    V = FastExp(Temp1, S, P)
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                "3. Alice menghitung nilai v dengan
rumus berikut:"
                    'rumus v
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                "      v = a^(-s) mod p"
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                "      v = " & A & "^(-" & S & ")
```

```
mod " & P
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      v = ((" & A & "^(-1) mod " & P & ")^" & S
& ") mod " & P

                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                  "   Selesaikan operasi (" & A & "^(-1) mod " & P &
                  ") dengan algoritma                      extended
                  euclidean"

                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      (" & A & "^(-1) mod " & P & ") = " &
Temp1

                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "      v = (" & Temp1 & "^" & S & ") mod " & P &
                  " (selesaikan   dengan fast exponentiation)"

                    Delay nDelay
                    MSFlexGrid1.TextMatrix(5, 1) = V
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      v = " & V & " (v adalah kunci publik)"

                TmrAlice.Enabled = False
                End If
    End Select
    cmdPrev.Enabled = (Langkah > 0)
    cmdNext.Enabled = (Langkah < 3)
    cmdUlang.Enabled = True
    cmdKeluar.Enabled = True
End Sub
```

Form frmInputPQA.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Dim iTemp1 As Integer
    Dim iTemp2 As Integer
    Dim iTemp3 As Integer
    Dim nLoop As Integer
    Dim bFound As Boolean

    cmdOK.Enabled = False
```

```
    cmdAcak.Enabled = False

    'Tes untuk setiap p dan q sebanyak 20000 kali
    ProgressBar1.value = 0
    ProgressBar1.Max = 20000
    ProgressBar1.Visible = True
    bFound = False
    While bFound = False
        lblInfo = "Membangkitkan pasangan nilai p dan q yang sesuai
dengan syarat no.1 dan no.2 ..."
        ProgressBar1.value = 0

        Randomize Timer
        iTemp3 = Int(Rnd * 2)

        'Syarat GCD <> 1
        nLoop = 0
        Do
            'Generate p -> prima
            Randomize Timer
            iTemp1 = 6 + iTemp3
            P = GeneratePrimeNumber(iTemp1)
            'Generate q -> prima
            Randomize Timer
            iTemp2 = 2 + iTemp3
            Q = GeneratePrimeNumber(iTemp2)
            nLoop = nLoop + 1
            If nLoop >= 10000 Then
                nLoop = 0
                'Acak ulang iTemp3
                Randomize Timer
                iTemp3 = Int(Rnd * 2)
            End If
        Loop Until GCD(Q, P - 1) <> 1
        'Syarat nilai a
        lblInfo = "Membangkitkan nilai variabel a yang sesuai dengan
syarat no.3 ..."
        nLoop = 0
        Do
            'Bangkitkan nilai a baru
            Randomize Timer
            A = Int(Rnd * 100000) + 2
            'Jalankan progress bar
            nLoop = nLoop + 1
            ProgressBar1.value = nLoop
            DoEvents
            If nLoop = 20000 Then Exit Do
        Loop Until (FastExp(A, Q, P) = 1)
        bFound = (FastExp(A, Q, P) = 1)
    Wend
    txtP.Text = P
    txtQ.Text = Q
```

```
    txtA.Text = A

    lblInfo = ""
    ProgressBar1.Visible = False

    cmdOK.Enabled = True
    cmdAcak.Enabled = True
End Sub

Private Sub cmdOK_Click()
    P = Val(txtP.Text)
    Q = Val(txtQ.Text)
    A = Val(txtA.Text)
    If P = 0 Then
        MsgBox "Nilai variabel p belum diisi !", vbCritical
        Exit Sub
    ElseIf Q = 0 Then
        MsgBox "Nilai variabel q belum diisi !", vbCritical
        Exit Sub
    ElseIf A = 0 Then
        MsgBox "Nilai variabel a belum diisi !", vbCritical
        Exit Sub
    ElseIf TestPrima(P, 3) = False Then
        MsgBox "Nilai variabel p harus merupakan bilangan prima !",
vbCritical
        Exit Sub
    ElseIf TestPrima(Q, 3) = False Then
        MsgBox "Nilai variabel q harus merupakan bilangan prima !",
vbCritical
        Exit Sub
    ElseIf GCD(Q, P - 1) = 1 Then
        MsgBox "Operasi dari GCD(q, p-1) tidak boleh bernilai 1 !",
vbCritical
        Exit Sub
    ElseIf FastExp(A, Q, P) <> 1 Then
        MsgBox "Nilai dari operasi (a^q) mod p harus bernilai 1 !",
vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub cmdTestGCD_Click()

    If Val(txtQ) = 0 Or Val(txtP) - 1 = 0 Then
        MsgBox "Nilai q dan (p - 1) harus lebih besar dari 0",
vbCritical, "GCD"
        Exit Sub
    End If

    frmTestGCD.iA = txtQ.Text
    frmTestGCD.iB = Val(txtP.Text) - 1
```

```
    frmTestGCD.Show vbModal
End Sub

Private Sub Form_Load()
    Delay 800
    txtP = P
    txtQ = Q
    txtA = A
End Sub

Private Sub txtA_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub

Private Sub txtP_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub

Private Sub txtQ_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frmTestGCD.frm

```
Option Explicit
Public iA As Long
Public iB As Long
Private Sub cmdKeluar_Click()
    Unload Me
End Sub

Private Sub Form_Load()
    'Nilai awal
    txtA = iA
    txtB = iB
    'Analisis algoritma GCD
    Call AnalisisGCD(iA, iB)
End Sub

'Analisis Algoritma GCD
Private Sub AnalisisGCD(ByVal A As Double, ByVal B As Double)
    Dim X As Double
```

```
    Dim Y As Double
    Dim Z As Double
    X = A
    Y = B
    txtE = txtE & "X = " & A
    txtE = txtE & vbCrLf & "Y = " & B

    While Y <> 0
        txtE = txtE & vbCrLf & vbCrLf & _
               "WHILE " & Y & " <> 0  (TRUE)"
        Z = FModulus(X, Y)
        txtE = txtE & vbCrLf & _
               "Z = " & X & " mod " & Y & " = " & Z
        X = Y
        txtE = txtE & vbCrLf & _
               "X = " & Y
        Y = Z
        txtE = txtE & vbCrLf & _
               "Y = " & Z
    Wend
    txtE = txtE & vbCrLf & vbCrLf & _
               "WHILE " & Y & " <> 0  (FALSE)"
    txtGCD.Text = X
    txtE = txtE & vbCrLf & vbCrLf & _
               "Hasil Fungsi GCD(" & A & ", " & B & ") = " & X
End Sub
```

Form frmInputR.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Randomize Timer
    R = 1 + Int(Rnd * (Q - 1))
    txtR = R
End Sub

Private Sub cmdOK_Click()
    R = Val(txtR.Text)
    If R = 0 Then
        MsgBox "Nilai variabel r belum diisi !", vbCritical
        Exit Sub
    ElseIf R >= Q Then
        MsgBox "Nilai variabel r harus lebih kecil dari q !",
vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub Form_Load()
    Delay 800
    txtR = R
```

```
    Text1.Text = Text1.Text & vbCrLf & _
                 "- Nilai q = " & Q
End Sub

Private Sub txtR_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frmInputS.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Randomize Timer
    S = 1 + Int(Rnd * (Q - 1))
    txtS = S
End Sub

Private Sub cmdOK_Click()
    S = Val(txtS.Text)
    If S = 0 Then
        MsgBox "Nilai variabel s belum diisi !", vbCritical
        Exit Sub
    ElseIf S >= Q Then
        MsgBox "Nilai variabel s harus lebih kecil dari q !",
vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub Form_Load()
    Delay 800
    txtS = S
    Text1.Text = Text1.Text & vbCrLf & _
                 "- Nilai q = " & Q
End Sub

Private Sub txtS_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frminputE.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Randomize Timer
    E = 100 + Int(Rnd * 100000000)
```

```
    txtE = E
End Sub

Private Sub cmdOK_Click()
    E = Val(txtE.Text)
    If E = 0 Then
        MsgBox "Nilai variabel e belum diisi !", vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub Form_Load()
    Delay 800
    txtE = E
End Sub

Private Sub txtE_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frmAuthentication.frm

```
Option Explicit
Private Const nDelay = 800
Private I As Integer
Private Langkah As Integer
Private nAlice As Integer
Private nBob As Integer
Private Sub cmdKeluar_Click()
    Unload Me
End Sub

Private Sub cmdNext_Click()
    'Langkah algoritma berikutnya
    Langkah = Langkah + 1
    Call EksekusiAlgo(Langkah, True)
End Sub

Private Sub cmdPrev_Click()
    'Langkah algoritma sebelumnya
    Langkah = Langkah - 1
    Call EksekusiAlgo(Langkah, False)
End Sub

Private Sub cmdUlang_Click()
    MSFlexGrid1.Rows = 6
    MSFlexGrid2.Rows = 1
    Call ResetAlgo
End Sub
```

```
Private Sub Form_Load()
    MSFlexGrid1.TextMatrix(1, 1) = P
    MSFlexGrid1.TextMatrix(2, 1) = Q
    MSFlexGrid1.TextMatrix(3, 1) = A
    MSFlexGrid1.TextMatrix(4, 1) = S
    MSFlexGrid1.TextMatrix(5, 1) = V
    'Ulang algoritma
    Call ResetAlgo
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub

Private Sub Text1_Change()
    Text1.SelStart = Len(Text1.Text)
End Sub

Private Sub TmrAlice_Timer()
    nAlice = nAlice + 1
    If nAlice = 5 Then nAlice = 1
    PicBoxAlice.Picture = LoadPicture(App.Path & "\Gambar\Alice-" &
nAlice & ".bmp")
End Sub

Private Sub TmrBob_Timer()
    nBob = nBob + 1
    If nBob = 8 Then nBob = 1
    PicBoxBob.Picture = LoadPicture(App.Path & "\Gambar\Bob-" & nBob
& ".bmp")
End Sub

Private Sub ResetAlgo()
    lblHeader = "SKEMA OTENTIKASI ANTARA Alice DAN Bob"
    'Pasangan kunci
    R = 0
    X = 0
    t = 0
    E = 0
    Y = 0
    'Langkah algoritma
    Langkah = 0
    'TABEL VARIABEL
    With MSFlexGrid1
        .Cols = 2
        .Rows = 10
        .ColWidth(0) = 2000
        .ColAlignment(0) = 4
        .ColWidth(1) = 2250
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 6
```

```
        .TextMatrix(0, 0) = "VARIABEL"
        .TextMatrix(0, 1) = "NILAI"
        .TextMatrix(1, 0) = "p"
        .TextMatrix(2, 0) = "q"
        .TextMatrix(3, 0) = "a"
        .TextMatrix(4, 0) = "s (privat)"
        .TextMatrix(5, 0) = "v (publik)"
        .TextMatrix(6, 0) = "r"
        .TextMatrix(7, 0) = "x"
        .TextMatrix(8, 0) = "e"
        .TextMatrix(9, 0) = "y"
    End With

    'TABEL ALGORITMA
    With MSFlexGrid2
        .Cols = 2
        .Rows = 15
        .ColWidth(0) = 750
        .ColAlignment(0) = 4
        .ColWidth(1) = 5490
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 1
        .TextMatrix(0, 0) = "No."
        .TextMatrix(0, 1) = "Algoritma"
        .TextMatrix(1, 0) = "1."
        .TextMatrix(1, 1) = " Alice memilih sebuah nilai r (r < q)."
        .TextMatrix(2, 0) = "2."
        .TextMatrix(2, 1) = " Alice menghitung: "
        .TextMatrix(3, 1) = "    x = a^r mod p"
        .TextMatrix(4, 1) = " dan mengirim x kepada Bob."
        .TextMatrix(5, 0) = "3."
        .TextMatrix(5, 1) = " Bob memilih sebuah nilai e "
        .TextMatrix(6, 1) = " (e diantara 0 sampai (2^t-1))"
        .TextMatrix(7, 1) = " dan mengirim e kepada Alice "
        .TextMatrix(8, 0) = "4."
        .TextMatrix(8, 1) = " Alice menghitung:"
        .TextMatrix(9, 1) = "    y = (r + se) mod q"
        .TextMatrix(10, 1) = " dan mengirim y kepada Bob."
        .TextMatrix(11, 0) = "5."
        .TextMatrix(11, 1) = " Bob melakukan verifikasi berikut:"
        .TextMatrix(12, 1) = "    x = ((a^y).(v^e)) mod p"
        .TextMatrix(13, 1) = " Jika nilai x sesuai, maka verifikasi"
        .TextMatrix(14, 1) = " dan otentikasi berhasil."
    End With

    'Keterangan proses
    Text1.Text = ""
    cmdNext.Enabled = True
    cmdPrev.Enabled = False
End Sub
```

```
Private Sub EksekusiAlgo(nBaris As Integer, bNext As Boolean)
    cmdPrev.Enabled = False
    cmdNext.Enabled = False
    cmdUlang.Enabled = False
    cmdKeluar.Enabled = False
    Select Case nBaris
        Case 0
                'Header
                lblHeader = "SKEMA OTENTIKASI ANTARA Alice DAN Bob"
                'Hapus warna hijau dari semua baris algo
                With MSFlexGrid2
                    'Hapus warna hijau pada baris algo-2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        .CellBackColor = White
                        .CellForeColor = 0
                    Next I
                End With

                Text1.Text = ""
                'Hapus semua nilai variabel
                For I = 6 To MSFlexGrid1.Rows - 1
                    MSFlexGrid1.TextMatrix(I, 1) = ""
                Next I
        Case 1
                'Header
                lblHeader = "1. Alice memilih nilai r (r < q)"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I <= 1 Then
                            'Warna hijau pada baris algo-1
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form r
                    frmInputR.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = "1. Alice memilih nilai r sebagai
berikut:"
```

```
                    'Isi nilai r
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                     "      r = " & R
                    MSFlexGrid1.TextMatrix(6, 1) = R
                    TmrAlice.Enabled = False
               Else
                    MSFlexGrid1.TextMatrix(7, 1) = ""
                    'hapus nomor 2.
                    Temp1 = InStr(1, Text1.Text, "2.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 2
                'Header
                lblHeader = "2. Alice menghitung: x = a^r mod p dan
mengirimkan x kepada Bob"
                With MSFlexGrid2
                    .Col = 1
                For I = 1 To .Rows - 1
                        .Row = I
                        If I = 2 Or I = 3 Or I = 4 Then
                            'Warna hijau pada baris algo-2
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                'Perhitungan
                    X = FastExp(A, R, P)
                'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "2. Alice menghitung nilai x"
                'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                      "      x = a^r mod p (selesaikan dengan fast"
& vbCrLf & _
                      "                     exponentiation)"
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & A & "^" & R & " mod " & P
                    'tampilkan nilai x
```

```
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & X
                    MSFlexGrid1.TextMatrix(7, 1) = X
                    'kirimkan nilai x kepada Bob
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Alice mengirimkan x kepada Bob"
                    'Kirimkan
                    Call SendTo("Bob", "x")
                    TmrAlice.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(8, 1) = ""
                    'hapus nomor 3.
                    Temp1 = InStr(1, Text1.Text, "3.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 3
                'Header
                lblHeader = "3. Bob memilih sebuah nilai e dan
mengirimkan e kepada Alice"
                With MSFlexGrid2
                    .Col = 1
                For I = 1 To .Rows - 1
                        .Row = I
                        If I = 5 Or I = 6 Or I = 7 Then
                            'Warna hijau pada baris algo-3
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True
                'Show input form e
                    frmInputE.Show vbModal
                'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "3. Bob memilih nilai e sebagai berikut:"
                    'Isi nilai e
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      e = " & E
                    MSFlexGrid1.TextMatrix(8, 1) = E
                    'kirimkan nilai e kepada Alice
```

```
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Bob mengirimkan e kepada Alice"
                    'Kirimkan
                    Call SendTo("Alice", "e")
                    TmrBob.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(9, 1) = ""
                    'hapus nomor 4.
                    Temp1 = InStr(1, Text1.Text, "4.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 4
                'Header
                lblHeader = "4. Alice menghitung: y = (r + se) mod q
dan mengirim y kepada Bob"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 8 Or I = 9 Or I = 10 Then
                            'Warna hijau pada baris algo-4
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True

                    'Perhitungan
                    Y = FModulus((R + (S * E)), Q)

                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "4. Alice menghitung nilai y
sebagai berikut:"
                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      y = (r + se) mod q"
                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      y = (" & R & " + " & S & " . " & E & ")
```

```
mod " & Q
                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      y = " & Y
                    MSFlexGrid1.TopRow = 9
                    MSFlexGrid1.TextMatrix(9, 1) = Y

                    'kirimkan nilai y kepada Bob
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Alice mengirimkan y kepada Bob"

                    'Kirimkan
                    Call SendTo("Bob", "y")
                    TmrAlice.Enabled = False
                Else
                    'hapus nomor 5.
                    Temp1 = InStr(1, Text1.Text, "5.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 5
                'Header
                lblHeader = "5. Bob melakukan verifikasi x =
((a^y).(v^e)) mod p"
                With MSFlexGrid2
                    .Col = 1
                For I = 1 To .Rows - 1
                        .Row = I
                        If I >= 11 Then
                            'Warna hijau pada baris algo-4
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True
                    'Perhitungan
                    Temp2 = FastExp(A, Y, P)
                    Temp3 = FastExp(V, E, P)
                    Temp1 = FModulus(Temp2 * Temp3, P)
                    bVerifikasi = (X = Temp1)

                    'header
                    Delay nDelay
```

```
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "5. Bob melakukan verifikasi sebagai berikut:"

                    'Rumus verifikasi
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = ((a^y).(v^e)) mod p"

                    'Rumus dipecah
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = ((a^y) mod p . (v^e) mod p) mod p"

                    'Rumus dipecah
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = (" & A & "^" & Y & " mod " & P & ") .
" & vbCrLf & _
                    "(" & V & "^" & E & " mod " & P & ") " & vbCrLf
& "  mod " & P

                    'hasil-1
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                 "      x = (" & Temp2 & _
                                 " . " & Temp3 & ") mod " & P

                    'hasil-2
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                     "      " & X & " = " & Temp1 & " (" &
UCase(Format(bVerifikasi)) & ")"

                    If bVerifikasi Then
                        'Tambahan informasi u/ verifikasi
                        Text1.Text = Text1.Text & vbCrLf & _
                        "Hasil perhitungan operasi (((a^y).(v^e))
mod p) " & _
                        "sama dengan nilai x. Proses otentikasi
berhasil."

                        MsgBox "Proses verifikasi berhasil !",
vbInformation
                    Else
                        MsgBox "Proses verifikasi gagal !",
vbCritical
                    End If
            TmrBob.Enabled = False
                 End If
        End Select

    cmdPrev.Enabled = (Langkah > 0)
```

```
    cmdNext.Enabled = (Langkah < 5)
    cmdUlang.Enabled = True
    cmdKeluar.Enabled = True
End Sub

Private Sub SendTo(Receiver As String, Var As String)
    TmrAlice.Enabled = True
    TmrBob.Enabled = True

    lblVar.Caption = Var
    PicMail.Visible = True

    If Receiver = "Bob" Then
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Alice.gif")
        PicMail.Left = 2325
        While PicMail.Left < 7305
            PicMail.Left = PicMail.Left + 30
            Delay 20
        Wend
    Else
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Bob.gif")
        PicMail.Left = 7305
        While PicMail.Left > 2325
            PicMail.Left = PicMail.Left - 30
            Delay 20
        Wend
    End If

    PicMail.Visible = False

    TmrAlice.Enabled = False
    TmrBob.Enabled = False
End Sub
```

Form frmDigitalSign.frm

```
Option Explicit
Private Const nDelay = 800
Private I As Integer
Private J As Integer

Private Langkah As Integer

Private nAlice As Integer
Private nBob As Integer

Private sTemp1 As String
Private sTemp2 As String
Private sTemp3 As String
```

```
Private sTemp4 As String

Private E1() As Double
Private E2() As Double
Private Y1() As Double

Private Sub cmdKeluar_Click()
    Unload Me
End Sub

Private Sub cmdNext_Click()
    'Cek pesan
    If Langkah = 0 And txtPesan = "" Then
        MsgBox "Pesan masih kosong !", vbCritical
        Exit Sub
    End If

    'Langkah algoritma berikutnya
    Langkah = Langkah + 1
    Call EksekusiAlgo(Langkah, True)
End Sub

Private Sub cmdPrev_Click()
    'Langkah algoritma sebelumnya
    Langkah = Langkah - 1
    Call EksekusiAlgo(Langkah, False)
End Sub

Private Sub cmdUlang_Click()
    MSFlexGrid1.Rows = 6
    MSFlexGrid2.Rows = 1
    Call ResetAlgo
End Sub

Private Sub Form_Load()
    MSFlexGrid1.TextMatrix(1, 1) = P
    MSFlexGrid1.TextMatrix(2, 1) = Q
    MSFlexGrid1.TextMatrix(3, 1) = A
    MSFlexGrid1.TextMatrix(4, 1) = S
    MSFlexGrid1.TextMatrix(5, 1) = V

    'Ulang algoritma
    Call ResetAlgo
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub

Private Sub Text1_Change()
    Text1.SelStart = Len(Text1.Text)
End Sub
```

```
Private Sub TmrAlice_Timer()
    nAlice = nAlice + 1
    If nAlice = 5 Then nAlice = 1

    PicBoxAlice.Picture = LoadPicture(App.Path & "\Gambar\Alice-" &
nAlice & ".bmp")
End Sub

Private Sub TmrBob_Timer()
    nBob = nBob + 1
    If nBob = 8 Then nBob = 1

    PicBoxBob.Picture = LoadPicture(App.Path & "\Gambar\Bob-" & nBob
& ".bmp")
End Sub

Private Sub ResetAlgo()
    lblHeader = "SKEMA TANDA TANGAN DIGITAL ANTARA ALICE DAN BOB"
    'Pasangan kunci
    R = 0
    X = 0
    E = 0
    Y = 0
    'Langkah algoritma
    Langkah = 0
    'TABEL VARIABEL
    With MSFlexGrid1
        .Cols = 2
        .Rows = 8
        .ColWidth(0) = 2000
        .ColAlignment(0) = 4
        .ColWidth(1) = 2500
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 6
        .TextMatrix(0, 0) = "VARIABEL"
        .TextMatrix(0, 1) = "NILAI"
        .TextMatrix(1, 0) = "p"
        .TextMatrix(2, 0) = "q"
        .TextMatrix(3, 0) = "a"
        .TextMatrix(4, 0) = "s (privat)"
        .TextMatrix(5, 0) = "v (publik)"
        .TextMatrix(6, 0) = "r"
        .TextMatrix(7, 0) = "x"
    End With

    'TABEL ALGORITMA
    With MSFlexGrid2
        .Cols = 2
        .Rows = 15
        .ColWidth(0) = 750
        .ColAlignment(0) = 4
```

```
        .ColWidth(1) = 5490
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 1
        .TextMatrix(0, 0) = "No."
        .TextMatrix(0, 1) = "Algoritma"
        .TextMatrix(1, 0) = "1."
        .TextMatrix(1, 1) = " Alice memilih sebuah nilai r (r < q)"
        .TextMatrix(2, 1) = " dan menghitung:   x = a^r mod p"
        .TextMatrix(3, 0) = "2."
        .TextMatrix(3, 1) = " Alice menggabungkan M dan x dan  "
        .TextMatrix(4, 1) = " menghitung nilai hash:"
        .TextMatrix(5, 1) = "    e = H(M, x)"
        .TextMatrix(6, 0) = "3."
        .TextMatrix(6, 1) = " Alice menghitung:"
        .TextMatrix(7, 1) = "    y = (r + se) mod q"
        .TextMatrix(8, 1) = " Tanda tangan adalah e dan y."
        .TextMatrix(9, 1) = " Alice mengirimkannya bersama pesan."
        .TextMatrix(10, 0) = "4."
        .TextMatrix(10, 1) = " Bob menghitung x':"
        .TextMatrix(11, 1) = "    x' = ((a^y).(v^e)) mod p"
        .TextMatrix(12, 0) = "5."
        .TextMatrix(12, 1) = " Bob menggabungkan M dan x' dan"
        .TextMatrix(13, 1) = " melakukan verifikasi berikut:"
        .TextMatrix(14, 1) = "    e = H(M, x')"
    End With

    'Keterangan proses
    Text1.Text = ""
    txtDigiSign.Text = ""

    cmdNext.Enabled = True
    cmdPrev.Enabled = False

End Sub

Private Sub EksekusiAlgo(nBaris As Integer, bNext As Boolean)
    cmdPrev.Enabled = False
    cmdNext.Enabled = False
    cmdUlang.Enabled = False
    cmdKeluar.Enabled = False

    Select Case nBaris
        Case 0
                txtPesan.Locked = False
                'Header
                lblHeader = "SKEMA TANDA TANGAN DIGITAL ANTARA Alice
DAN Bob"

                'Hapus warna hijau dari semua baris algo
                With MSFlexGrid2
                    'Hapus warna hijau pada baris algo-2
                    .Col = 1
```

```
                    For I = 1 To .Rows - 1
                        .Row = I
                        .CellBackColor = White
                        .CellForeColor = 0
                    Next I
                End With

                Text1.Text = ""
                'Hapus semua nilai variabel
                For I = 6 To MSFlexGrid1.Rows - 1
                    MSFlexGrid1.TextMatrix(I, 1) = ""
                Next I
        Case 1
                txtPesan.Locked = True
                'Header
                lblHeader = "1. Alice memilih nilai r (r < q) dan
menghitung: x = a^r mod p"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I <= 2 Then
                            'Warna hijau pada baris algo-1
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form r
                    frmInputR.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = "1. Alice memilih nilai r sebagai
berikut:"
                    'Isi nilai r
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      r = " & R
                    MSFlexGrid1.TextMatrix(6, 1) = R

                    'Perhitungan Fast Exponentiation
                    X = FastExp(A, R, P)
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
```

```
                                  "   Alice menghitung nilai x"
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = a^r mod p (selesaikan dengan fast" &
vbCrLf & _
                    "                     exponentiation)"
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & A & "^" & R & " mod " & P
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & X
                    MSFlexGrid1.TextMatrix(7, 1) = X

                    TmrAlice.Enabled = False
                 Else
                    'hapus nomor 2.
                    Temp1 = InStr(1, Text1.Text, "2.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 2
             'Header
             lblHeader = "2. Alice menggabungkan M dan x dan
menghitung nilai hash: e = H(M, x)"
             With MSFlexGrid2
                    .Col = 1
            For I = 1 To .Rows - 1
                        .Row = I
                        If I = 3 Or I = 4 Or I = 5 Then
                            'Warna hijau pada baris algo-2
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
            'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                     "2. Alice menggabungkan M dan x dan " & vbCrLf
& _
                     "   menghitung nilai hash:  e = H(M, x)"
```

```
                    '----------------------
                    ReDim E1(Len(txtPesan.Text))
                    For I = 1 To Len(txtPesan.Text)
                        Delay nDelay

                        'Karakter ke-i
                        sTemp1 = Mid(txtPesan.Text, I, 1)
                        M = Asc(sTemp1)                     'Nilai
message per huruf
                        sTemp2 = Format(M) & Format(X)      'Hasil
gabung
                        sTemp3 = Left(SHA.SHA1(sTemp2), 4)  'Ambil 4
karakter dari nilai hash

                        'Hasil hash dalam bentuk angka
                        sTemp4 = ""
                        For J = 1 To Len(sTemp3)
                            sTemp4 = sTemp4 & Format(Asc(Mid(sTemp3,
J, 1)))
                        Next J
                        E1(I) = Val(sTemp4)

                        Text1.Text = Text1.Text & vbCrLf & vbCrLf &
_
                      "   M(" & I & ") = ascii dari '" & sTemp1 & "'
= " & M & vbCrLf & _
                      "   (M(" & I & "),x) = M(" & I & ") digabung
dengan x " & vbCrLf & _
                      "   (M(" & I & "),x) = " & sTemp2 & vbCrLf & _
                      "   e(" & I & ") = H(" & sTemp2 & ") " &
vbCrLf & _
                      "   e(" & I & ") = " & E1(I)
                    Next I
                    '----------------------

                    TmrAlice.Enabled = False
                Else
                    'hapus nomor 3.
                    Temp1 = InStr(1, Text1.Text, "3.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                    txtDigiSign.Text = ""
                End If
            Case 3
              'Header
              lblHeader = "3. Alice menghitung: y = (r + se) mod q.
Tanda tangan adalah e dan y."
            With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 6 Or I = 7 Or I = 8 Or I = 9 Then
```

```
                            'Warna hijau pada baris algo-3
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True

                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "3. Alice menghitung nilai y
sebagai berikut:"

                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                 "      y = (r + se) mod q"

                    '----------------------
                    txtDigiSign.Text = ""
                    ReDim Y1(Len(txtPesan.Text))
                    For I = 1 To Len(txtPesan.Text)
                        Delay nDelay

                        'Hitung Y(I)
                        Y1(I) = FModulus(R + (S * E1(I)), Q)

                        Text1.Text = Text1.Text & vbCrLf & vbCrLf &
_
        "   y(" & I & ") = (r + (s . e(" & I & "))) mod q" & vbCrLf
& _
        "   y(" & I & ") = (" & R & " + (" & S & " . " & E1(I) & "))
mod " & Q & vbCrLf & _
        "   y(" & I & ") = " & Y1(I)
        'Tanda tangan
                        txtDigiSign.Text = txtDigiSign.Text & "|" &
E1(I) & "," & Y1(I)
                    Next I
                    '----------------------
        'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "   Tanda tangan digital adalah e
dan y."
        'Kirimkan
```

```
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
               "   Alice mengirimkan pesan dan tanda tangan digital"
& vbCrLf & "   kepada Bob."
               Call SendTo("Bob")
                Else
                    'hapus nomor 4.
                    Temp1 = InStr(1, Text1.Text, "4.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 4
                'Header
                lblHeader = "4. Bob menghitung x' = ((a^y).(v^e))
mod p"
               With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 10 Or I = 11 Then
                            'Warna hijau pada baris algo-4
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True

                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "4. Bob melakukan perhitungan sebagai berikut:"

                    'Rumus verifikasi
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x' = ((a^y).(v^e)) mod p"

                    ReDim Xa(Len(txtPesan.Text))

                    For I = 1 To Len(txtPesan.Text)
                        'Perhitungan
                        Temp2 = FastExp(A, Y1(I), P)
                        Temp3 = FastExp(V, E1(I), P)
                        Xa(I) = FModulus(Temp2 * Temp3, P)
```

```
                        'Rumus dipecah
                        Delay nDelay
                        Text1.Text = Text1.Text & vbCrLf & vbCrLf &
_
                  "   x'(" & I & ") = ((a^y(" & I & ")) mod p .
(v^e(" & I & ")) mod p) mod p"

                        'Rumus dipecah
                        Text1.Text = Text1.Text & vbCrLf & _
                 " x'(" & I & ") = (" & A & "^" & Y1(I) & " mod " &
P & ") . " & vbCrLf & _
                 " (" & V & "^" & E1(I) & " mod " & P & ") " &
vbCrLf & _
                 "  mod " & P

                        'hasil-2
                        Text1.Text = Text1.Text & vbCrLf & _
                   "   x'(" & I & ") = " & Xa(I)
                    Next I
                   TmrBob.Enabled = False
                Else
                    'hapus nomor 5.
                    Temp1 = InStr(1, Text1.Text, "5.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 5
         'Header
         lblHeader = "5. Bob menggabungkan M dan x' dan melakukan
verifikasi berikut: e = H(M, x')"
         With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I >= 12 Then
                            'Warna hijau pada baris algo-5
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "5. Bob menggabungkan M dan x' dan
```

```
" & vbCrLf & _
                                "   melakukan verifikasi:  e = H(M,
x')"
                    '----------------------
                    ReDim E2(Len(txtPesan.Text))
                    For I = 1 To Len(txtPesan.Text)
                        Delay nDelay

                        'Karakter ke-i
                        sTemp1 = Mid(txtPesan.Text, I, 1)
                        M = Asc(sTemp1)                     'Nilai
message per huruf
                        sTemp2 = Format(M) & Format(Xa(I))
'Hasil gabung
                        sTemp3 = Left(SHA.SHA1(sTemp2), 4)  'Ambil 4
karakter dari nilai hash

                        'Hasil hash dalam bentuk angka
                        sTemp4 = ""
                        For J = 1 To Len(sTemp3)
                            sTemp4 = sTemp4 & Format(Asc(Mid(sTemp3,
J, 1)))
                        Next J
                        E2(I) = Val(sTemp4)
                        bVerifikasi = (E1(I) = E2(I))

         Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
         " M(" & I & ") = ascii dari '" & sTemp1 & "' = " & M &
vbCrLf & _
         " (M(" & I & "),x'(" & I & ")) = M(" & I & ") digabung
dengan x'(" & I & ")" & vbCrLf & _
         "   (M(" & I & "),x'(" & I & ")) = " & sTemp2 & vbCrLf & _
         "   e(" & I & ") = H(" & sTemp2 & ")" & vbCrLf & _
         "   " & E1(I) & " = " & E2(I) & " (" &
UCase(Format(bVerifikasi)) & ")"

                        If bVerifikasi = False Then
                            MsgBox "Proses verifikasi gagal !",
vbCritical
                            Exit For
                        End If
                    Next I
                    '----------------------
                    If bVerifikasi Then
                        'Tambahan informasi u/ verifikasi
                        Text1.Text = Text1.Text & vbCrLf & _
                        "Hasil perhitungan operasi H(M, x') sama
dengan nilai e " & _
                        "sehingga proses verifikasi tanda tangan
digital berhasil."

                        MsgBox "Proses verifikasi berhasil !",
```

```
vbInformation
                    End If
                  TmrBob.Enabled = False
                End If
        End Select

    cmdPrev.Enabled = (Langkah > 0)
    cmdNext.Enabled = (Langkah < 5)
    cmdUlang.Enabled = True
    cmdKeluar.Enabled = True
End Sub

Private Sub SendTo(Receiver As String)
    TmrAlice.Enabled = True
    TmrBob.Enabled = True
PicMail.Visible = True
If Receiver = "Bob" Then
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Alice.gif")
        PicMail.Left = 2325
        While PicMail.Left < 7305
            PicMail.Left = PicMail.Left + 30
            Delay 20
        Wend
    Else
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Bob.gif")
        PicMail.Left = 7305
        While PicMail.Left > 2325
            PicMail.Left = PicMail.Left - 30
            Delay 20
        Wend
    End If

    PicMail.Visible = False
TmrAlice.Enabled = False
    TmrBob.Enabled = False
End Sub

Private Sub txtPesan_KeyPress(KeyAscii As Integer)
    If KeyAscii = 13 Then KeyAscii = 0
End Sub
```

Form frmTeori.frm

```
Option Explicit
Private Langkah As Integer

Private Sub cmdKeluar_Click()
    Unload Me
```

```
End Sub

Private Sub cmdNext_Click()
    Langkah = Langkah + 1
    Call EksekusiLangkah
End Sub

Private Sub cmdPrev_Click()
    Langkah = Langkah - 1
    Call EksekusiLangkah
End Sub

Private Sub Form_Load()
    Langkah = 1
    Call EksekusiLangkah
End Sub

Private Sub EksekusiLangkah()
    Picture1.Picture = LoadPicture(App.Path & "\Gambar\Teori-" &
Langkah & ".gif")
    cmdNext.Enabled = (Langkah < 12)
    cmdPrev.Enabled = (Langkah > 1)
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub
```

Form frmAbout.frm

```
Private Sub cmdOK_Click()
    Unload Me
End Sub
```

LAMPIRAN B

Daftar Penguji Dan Kuisioner

Tabel 5.1 Daftar Penguji

NO	Nama Penguji	Pekerjaan	Instansi
1	Achmad Jiswan	Mahasiswa	Teknik Informatika Multimedia STMIK AMIKOM Yogyakarta
2	Andhika Danawiputra	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
3	Aditya WN	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
4	Ahmad Hafid	Mahasiswa	Prodi Teknik Informatika, Universitas Pembangunan Nasional "Veteran" Yogyakarta
5	Agung Rahmawan	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
6	Ahmad Ashar Aras	Mahasiswa	Prodi Seni Teater ISI Yogyakarta
7	Ahmad Athaullah	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
8	Hafidz Syabiq	Mahasiswa	Prodi Pendidikan Bahasa Arab, Fak Tarbiyah UIN Sunan Kalijaga.
9	Healdy	Mahasiswa	Teknik Informatika Jaringan Komputer STMIK AMIKOM Yogyakarta
10	Irvan Arifin	Wiraswasta	-
11	Luthfi Noor Ichsan	Mahasiswa	Prodi Bimbingan dan Penyuluhan Islam, Fak Dakwah UIN Sunan Kalijaga
12	Irwan Saputra	Mahasiswa	Sistem Informasi, Broadcasting TV STMIK AMIKOM Yogyakarta
13	Kamaruddin	Mahasiswa	Sistem Komputer, Universitas Teknologi Yogyakarta
14	Kadir	Mahasiswa	Prodi Komunikasi dan Penyiaran Islam, Fak Dakwah UIN Sunan Kalijaga
15	Muhammad Tahir	Mahasiswa	Teknik Informatika, Jaringan Komputer STMIK AMIKOM Yogyakarta

16	Marta Ika Wijayati	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
17	Muhammad Tasdik	Mahasiswa	Prodi Pendidikan Agama Islam, Fak Tarbiyah UIN Sunan Kalijaga
18	Muhammad Zaenudin Latief	Mahasiswa	Prodi Pendidikan Agama Islam, Fak Tarbiyah UIN Sunan Kalijaga
19	Muhammad Aras	Swasta	CV.Multivisindo Yogyakarta
20	Maulana Ashar Sakti	Mahasiswa	Teknik Industri, Universitas Teknologi Yogyakarta
21	M Aslam S	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
22	Nursyam Fahrurozie	Mahasiswa	Prodi Fisika, Fak Saintek UIN Sunan Kalijaga.
23	Qori Ulvi	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
24	Restu Umar Singgih	Mahasiswa	Teknik Pertambangan, Universitas Pembangunan Nasional "Veteran" Yogyakarta
25	Ryan Adi Putra	Mahasiswa	Teknik Komputer AKAKOM
26	Sarbunis	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
27	Syifa Q.A	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
28	Sutrisno	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
29	Syamsuddin	Mahasiswa	Prodi Keuangan Islam, Fak Syariah UIN Sunan Kalijaga.
30	Susi Susanti	Mahasiswa	Psikologi, Universitas Ahmad Dahlan Yogyakarta

LAMPIRAN C

Daftar Kuisioner

ANGKET PENGUJIAN SISTEM

Nama : Achmad Jiswan

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.				
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.				
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.				
4	Sistem ini memberikan Form Input Variabel r dengan jelas.				
5	Sistem ini memberikan Form Input Variabel e dengan jelas.				
6	Sistem ini menampilkan Form Digital Signature dengan jelas.				
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.				

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.				
2	Interface menarik.				
3	Animasi yang cukup menarik.				
4	Waktu Loading system relative cepat.				
5	Menu pada sistem sudah berfungsi dengan baik.				

ANGKET PENGUJIAN SISTEM

Nama : Andhika Danawiputra

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Aditya WN

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Ahmad Hafid

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Agung Rahmawan

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.			✓	
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Ahmad Ashar Aras

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Ahmad Athaullah

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.			✓	
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Hafidz Syabiq

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Healdy

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Irvan Arifin

Pekerjaan : Wiraswasta

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.			✓	
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.			✓	
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.			✓	
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.			✓	

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Luthfi Noor Ichsan

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Irwan Saputra

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Kamaruddin

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Kadir

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Tahir

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Marta Ika Wijayanti

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Tasdik

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Zaenudin Latief

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Aras

Pekerjaan : Swasta

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Maulana Ashar Sakti

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : M Aslam S

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Nursyam Fahrurozie

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Qori Ulvi

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.			✓	

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Restu Umar Singgih

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Ryan Adi Putra

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.			✓	
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.			✓	
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.			✓	
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.			✓	

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Sarbunis

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Syifa Q.A

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Sutrisno

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Syamsuddin

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Susi Susanti

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

CURRICULUM VITAE

Nama	: Jusmail
Tempat, tanggal lahir	: Jambi, 06 Juli 1986
Jenis Kelamin	: Laki – Laki
Agama	: Islam
Alamat Asal	: Jln.Harapan No.48 Desa Simbur Naik, Dusun Karya Kec.Muara Sabak, Kab. Tanjung Jabung Timur Jambi.
No.Ho	: +6281215763612
Email	: jusmailelbugisy@yahoo.co.id/jusmbugis@gmail.com

Riwayat Pendidikan :

1. TK Dharma Wanita (1992)
2. SD Negeri 67 Simbur Naik (1993-1999)
3. MTS Pondok Pesantren Al-Busyra Jambi (1999-2002)
4. MA Pondok Pesantren Ummul Quro Al-Islamy Bogor (2002-2006)
5. S1 Teknik Informatika UIN Sunan Kalijaga Yogyakarta (2006-2011)

Pengalaman Organisasi :

1. Ketua ISPA Pon-Pes UQI Bogor	Jabatan Ketua Umum (2004-2005)
2. PMII Rayon Fakultas Saintek	Jabatan Dev. Pengkaderan (2008-2009)
3. KAPEMA Tanjabtim Jambi	Jabatan Dev. Intelektualitas (2008-2009)
4. BEM-F Sains & Teknologi	Jabatan Dev. Advokasi (2009-2010)
5. FKM Bone Yogyakarta	Jabatan Sekjen (2010-2011)

DAFTAR PUSTAKA

Agustia, Paul L. 2005, *Perancangan Perangkat Lunak Bantu Pemahaman Masalah Faktorisasi, Perpangkatan Modulo dan Bilangan Prima,* Tugas Akhir STMIK-Mikroskil, Medan.

Cormen, Thomas H. 2004, *Introduction to Algorithms Second Edition*, The Massachusetts Intitute of Technology, North America.

Hafid, Ahmad. 2011, "Aplikasi Bantu Pembelajaran *Digital Signature* dengan Metode *Ong-Schnorr-Shamir*", Skripsi, Universitas Pembangunan Nasional "Veteran" Yogyakarta, Yogyakarta.

Kurniawan, Jusuf. 2004, *Kriptografi, Keamanan Internet dan Jaringan Komunikasi*, Penerbit Informatika Bandung.

Kurniasari, Amy. 2010, *Authentikasi User dalam Sistem Informasi Berbasis WEB.http://blog.unsri.ac.id/userfiles/Autentifikasi%20user(1).doc* Akses pada tanggal 02 Juni 2010.

Kurniawan, Agus, 2008. *Konsep dan Implementasi Cryptography dengan .NET*, Dian Rakyat, Jakarta.

Nugroho, Adi, 2005, "*Analisis dan Perancangan Sistem Informasi dengan Metodologi Berorientasi Obyek*", Informatika, Bandung.

Pandia, Henry, 2002. *Visual Basic 6 Tingkat Lanjut,* Andi Yogyakarta.

Pramono, Djoko. 2002, *Mudah menguasai Visual Basic 6,* PT. Elex Media Komputindo.

Presman, Roger S., Ph.D, 2002, *Rekayasa Perangkat Lunak: Pendekatan Praktisi*, Andi Offset, Yogyakarta.

Rahmayanti, Desi. 2007, Aplikasi digital signature sebagai autentikasi Pada kartu tanda penduduk (Ktp), Institut Teknologi Bandun, Bandung.

Schneier, Bruce.1996, *Applied Crytography*, *Second Edition*. United States of America.

Sugiyono, 2010. Metode Penelitian Pendidikan. Pendekatan Kuantitatif, Kualitatif dan R&D. Alfabeta Bandung.

Stallings, William. 2003, *Cryptography and Network Security*, *Third Edition*. United States of America.

LAMPIRAN A

Source Code

Form frmSplash.frm

```
Option Explicit
Private Sub Command1_Click()
Unload Me
Screen.MousePointer = vbDefault
 frmMenu.Show
End Sub

Private Sub cmdOK_Click(Index As Integer)
Unload Me
Screen.MousePointer = vbDefault
 frmMenu.Show
End Sub

Private Sub Form_KeyPress(KeyAscii As Integer)
    Unload Me
End Sub

Private Sub Frame1_Click()
    Unload Me
End Sub

Private Sub lblPlatform_Click()

End Sub

Private Sub Text1_Change()

End Sub

Private Sub Label1_Click()

End Sub

Private Sub Picture1_Click()

End Sub

Private Sub Image1_Click()

End Sub
```

Form frmMenu.frm

```
Option Explicit
Const LOrange = &H80C0FF
Const DOrange = &H80FF&
```

```
Private Sub cmdAbout_Click()
    frmAbout.Show vbModal
End Sub

Private Sub cmdAbout_MouseMove(Button As Integer, Shift As Integer,
X As Single, Y As Single)
    If lblInfo.Tag <> "5" Then
        'Keterangan
        lblInfo.Caption =
     "Informasi mengenai pembuat pengembangan perangkat lunak " & _
     "untuk simulasi schnorr authentikasi digital signeture scheme
dan sekaligus " & _
     "penyusun tugas akhir skripsi Strata-1 jurusan Teknik
Informatika " & _
     "Universitas Islam Negeri Sunan Kalijaga Yogyakarta."
        lblInfo.Tag = "5"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = DOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdAuthentication_Click()
    If P = 0 Or Q = 0 Or A = 0 Or S = 0 Or V = 0 Then
        MsgBox "Proses pembentukan kunci harus dijalankan sebelum
skema otentikasi.", vbCritical
    Else
        Me.Hide
        frmAuthentication.Show
    End If
End Sub

Private Sub cmdAuthentication_MouseMove(Button As Integer, Shift As
Integer, X As Single, Y As Single)
    If lblInfo.Tag <> "2" Then
        'Keterangan
        lblInfo.Caption =
        "Otentikasi (authentication) adalah layanan " & _
        "yang berhubungan dengan identifikasi, baik " & _
        "mengidentifikasi kebenaran pihak-pihak yang " & _
        "berkomunikasi (user authentication atau entity " & _
     "authentication) maupun mengidentifikasi kebenaran sumber " & _
    "pesan (data origin authentication). Dua pihak yang saling " & _
    "berkomunikasi harus dapat mengotentikasi satu sama lain
sehingga " & _
     "ia dapat memastikan sumber pesan."
        lblInfo.Tag = "2"
       'Warna tombol
```

```
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = DOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdDigitalSignature_Click()
    If P = 0 Or Q = 0 Or A = 0 Or S = 0 Or V = 0 Then
        MsgBox "Proses pembentukan kunci harus dijalankan sebelum
skema tanda tangan digital.",   vbCritical
    Else
        Me.Hide
        frmDigitalSign.Show
    End If
End Sub

Private Sub cmdDigitalSignature_MouseMove(Button As Integer, Shift
As Integer, X As Single, Y As Single)
    If lblInfo.Tag <> "3" Then
        'Keterangan
        lblInfo.Caption =
 "Tanda tangan digital adalah suatu mekanisme otentikasi " & _
 "yang memungkinkan pembuat pesan menambahkan sebuah kode " & _
 "yang bertindak sebagai tanda tangannya. Tanda tangan tersebut "& _
"menjamin integritas dan sumber dari sebuah pesan. Penandatanganan
digital " & _
 "terhadap suatu dokumen adalah sidik jari dari dokumen tersebut
yang dibentuk " & _
  "dengan menggunakan kunci privat pihak yang menandatangani. Tanda
tangan digital " & _
    "akan berbeda untuk dokumen yang berbeda."
        lblInfo.Tag = "3"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = DOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdKeluar_Click()
    End
End Sub

Private Sub cmdKeluar_MouseMove(Button As Integer, Shift As Integer,
X As Single, Y As Single)
    If lblInfo.Tag <> "6" Then
```

```
        'Keterangan
        lblInfo.Caption = "Keluar dari program."
        lblInfo.Tag = "6"

        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = DOrange
    End If
End Sub

Private Sub cmdKeyGeneration_Click()
    Me.Hide
    frmKeyGeneration.Show
End Sub

Private Sub cmdKeyGeneration_MouseMove(Button As Integer, Shift As
Integer, X As Single, Y As Single)
    If lblInfo.Tag <> "1" Then
        'Keterangan
        lblInfo.Caption =
      "Pembentukan kunci (key generation) merupakan proses " & _
       "pembentukan kunci privat dan kunci publik yang akan " & _
      "digunakan pada skema otentikasi (authentication) dan " & _
 "skema tanda tangan digital (digital signature). Kunci privat " & _
     "diketahui oleh pihak pertama (yang akan diverifikasi atau
diperiksa keabsahannya " & _
       "pada kedua skema tersebut) sedangkan kunci publik disebarkan
dan " & _
       "diketahui oleh pihak-pihak lain yang akan memeriksa keaslian
atau keabsahan " & _
           "data dari pihak pertama."
        lblInfo.Tag = "1"
        'Warna tombol
        cmdKeyGeneration.BackColor = DOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub cmdTeori_Click()
    Me.Hide
    frmTeori.Show
End Sub

Private Sub cmdTeori_MouseMove(Button As Integer, Shift As Integer,
```

```
X As Single, Y As Single)
    If lblInfo.Tag <> "4" Then
        lblInfo.Caption = "Teori - Teori mengenai Skema Schnorr."
        lblInfo.Tag = "4"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = DOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub

Private Sub Picture1_MouseMove(Button As Integer, Shift As Integer,
X As Single, Y As Single)
    If lblInfo.Tag <> "0" Then
        'Keterangan
        lblInfo.Caption =
"PERHATIAN Dalam Menjalankan Perangkat Lunak Ini Seorang User" & _
"Harus Mengikuti Tahapan-tahapan dalam Prangkat Lunak " & _
   "Untuk Simulasi Schnorr Authentikasi dan Digital Signature" & _
  "Tahapan Pertama : KEY - GENERATION, Kedua : AUTHENTICATION" & _
                   "KeTiga : DIGIAL-SIGNATURE dan yang TEORI,
ABOUT, KELUAR " & _
 "Merupakan Menu Tambahan. Seorang User Tidak Bisa Langsung Ke
Tahapan Kedua tanpa melewati" & _
           "Tahapan Pertama, Jadi Seorang User Harus mengikuti
Tahapan-tahapan pada MENU"
        lblInfo.Tag = "0"
        'Warna tombol
        cmdKeyGeneration.BackColor = LOrange
        cmdAuthentication.BackColor = LOrange
        cmdDigitalSignature.BackColor = LOrange
        cmdTeori.BackColor = LOrange
        cmdAbout.BackColor = LOrange
        cmdKeluar.BackColor = LOrange
    End If
End Sub
```

Form Key-Generation.frm

```
Option Explicit
Private Const nDelay = 800
Private I As Integer
Private Langkah As Integer
Private nAlice As Integer
Private Sub cmdKeluar_Click()
   Unload Me
End Sub
Private Sub cmdNext_Click()
```

```
    'Langkah algoritma berikutnya
    Langkah = Langkah + 1
    Call EksekusiAlgo(Langkah, True)
End Sub

Private Sub cmdPrev_Click()
    'Langkah algoritma sebelumnya
    Langkah = Langkah - 1
    Call EksekusiAlgo(Langkah, False)
End Sub

Private Sub cmdUlang_Click()
    MSFlexGrid1.Rows = 1
    MSFlexGrid2.Rows = 1
    Call ResetAlgo
End Sub

Private Sub Form_Load()
    'Ulang algoritma
    Call ResetAlgo
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub

Private Sub Text1_Change()
    Text1.SelStart = Len(Text1.Text)
End Sub

Private Sub TmrAlice_Timer()
    nAlice = nAlice + 1
    If nAlice = 5 Then nAlice = 1
    PicBoxAlice.Picture = LoadPicture(App.Path & "\Gambar\AliceB-" &
nAlice & ".bmp")
End Sub

Private Sub ResetAlgo()
    lblHeader = "ALICE SEBAGAI PIHAK PERTAMA YANG MEMBENTUK KUNCI"
    'Pasangan kunci
    P = 0
    A = 0
    Q = 0
    S = 0
    V = 0

    'Langkah algoritma
    Langkah = 0
    'TABEL VARIABEL
    With MSFlexGrid1
        .Cols = 2
        .Rows = 6
```

```
        .ColWidth(0) = 2000
        .ColAlignment(0) = 4

        .ColWidth(1) = 2500
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 6

        .TextMatrix(0, 0) = "VARIABEL"
        .TextMatrix(0, 1) = "NILAI"
        .TextMatrix(1, 0) = "p"
        .TextMatrix(2, 0) = "q"
        .TextMatrix(3, 0) = "a"
        .TextMatrix(4, 0) = "s (privat)"
        .TextMatrix(5, 0) = "v (publik)"
    End With

    'TABEL ALGORITMA
    With MSFlexGrid2
        .Cols = 2
        .Rows = 9
        .ColWidth(0) = 750
        .ColAlignment(0) = 4
        .ColWidth(1) = 5490
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 1

        .TextMatrix(0, 0) = "No."
        .TextMatrix(0, 1) = "Algoritma"
        .TextMatrix(1, 0) = "1."
        .TextMatrix(1, 1) = " Pilih 2 buah bilangan prima p dan q,"
        .TextMatrix(2, 1) = " dan sebuah nilai a, dimana "
        .TextMatrix(3, 1) = " GCD(q, p-1) <> 1 dan (a^q) mod p = 1."
        .TextMatrix(4, 0) = "2."
        .TextMatrix(4, 1) = " Pilih sebuah nilai s, dimana s < q."
        .TextMatrix(5, 1) = " (s adalah kunci privat)"
        .TextMatrix(6, 0) = "3."
        .TextMatrix(6, 1) = " Hitung nilai v dengan rumus berikut:"
        .TextMatrix(7, 1) = "     v = a^(-s) mod p"
        .TextMatrix(8, 1) = " (v adalah kunci publik)"
    End With

    'Keterangan proses
    Text1.Text = ""
    cmdNext.Enabled = True
    cmdPrev.Enabled = False
End Sub

Private Sub EksekusiAlgo(nBaris As Integer, bNext As Boolean)
    cmdPrev.Enabled = False
    cmdNext.Enabled = False
    cmdUlang.Enabled = False
    cmdKeluar.Enabled = False
```

```
    Select Case nBaris
        Case 0
                lblHeader = "Alice SEBAGAI PIHAK PERTAMA YANG
MEMBENTUK KUNCI"
                'Hapus warna hijau dari semua baris algo
                With MSFlexGrid2
                    'Hapus warna hijau pada baris algo-2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        .CellBackColor = White
                        .CellForeColor = 0
                    Next I
                End With
                Text1.Text = ""
                MSFlexGrid1.TextMatrix(1, 1) = ""
                MSFlexGrid1.TextMatrix(2, 1) = ""
                MSFlexGrid1.TextMatrix(3, 1) = ""

        Case 1
                lblHeader = "1. Alice memilih 2 buah bilangan prima
p dan q serta nilai a"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I <= 3 Then
                            'Warna hijau pada baris algo-1
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With
                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form p, q dan a
                    frmInputPQA.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = "1. Alice memilih nilai p, q dan a
sebagai berikut:"
                    'Isi nilai p
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                     "      p = " & P
                    MSFlexGrid1.TextMatrix(1, 1) = P
                    'Isi nilai q
                    Delay nDelay
```

```
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      q = " & Q
                    MSFlexGrid1.TextMatrix(2, 1) = Q
                    'Isi nilai a
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      a = " & A
                    MSFlexGrid1.TextMatrix(3, 1) = A
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Nilai tersebut memenuhi ketentuan bahwa:" &
vbCrLf & _
                    "   - p dan q adalah bilangan prima," & vbCrLf &
_
                    "   - GCD(q, p-1) tidak boleh bernilai 1," &
vbCrLf & _
                    "   - Nilai dari operasi (a^q) mod p harus
bernilai 1."
                    TmrAlice.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(4, 1) = ""
                    'hapus nomor 2.
                    Temp1 = InStr(1, Text1.Text, "2.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 2
                lblHeader = "2. Alice memilih nilai s (s < q)
sebagai kunci privat"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 4 Or I = 5 Then
                            'Warna hijau pada baris algo-2
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form s
                    frmInputS.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
```

```
                                "2. Alice memilih nilai s (s < q)."
                    'tampilkan nilai s
                    Delay nDelay
                    MSFlexGrid1.TextMatrix(4, 1) = S
                    Text1.Text = Text1.Text & vbCrLf & _
                                "      s = " & S & " (s adalah
kunci privat)"

                    TmrAlice.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(5, 1) = ""
                    'hapus nomor 3.
                    Temp1 = InStr(1, Text1.Text, "3.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 3
                lblHeader = "3. Alice menghitung nilai v sebagai
kunci publik"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I >= 6 Then
                            'Warna hijau pada baris algo-3
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Hitung nilai v
                    Temp1 = ExtendedEuclidean(A, P)
                    V = FastExp(Temp1, S, P)
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                "3. Alice menghitung nilai v dengan
rumus berikut:"
                    'rumus v
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                "      v = a^(-s) mod p"
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                "      v = " & A & "^(-" & S & ")
```

```
mod " & P
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      v = ((" & A & "^(-1) mod " & P & ")^" & S
& ") mod " & P

                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                  "   Selesaikan operasi (" & A & "^(-1) mod " & P &
                  ") dengan algoritma                      extended
                  euclidean"

                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      (" & A & "^(-1) mod " & P & ") = " &
Temp1

                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "      v = (" & Temp1 & "^" & S & ") mod " & P &
                  " (selesaikan   dengan fast exponentiation)"

                    Delay nDelay
                    MSFlexGrid1.TextMatrix(5, 1) = V
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      v = " & V & " (v adalah kunci publik)"

                TmrAlice.Enabled = False
                End If
    End Select
    cmdPrev.Enabled = (Langkah > 0)
    cmdNext.Enabled = (Langkah < 3)
    cmdUlang.Enabled = True
    cmdKeluar.Enabled = True
End Sub
```

Form frmInputPQA.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Dim iTemp1 As Integer
    Dim iTemp2 As Integer
    Dim iTemp3 As Integer
    Dim nLoop As Integer
    Dim bFound As Boolean

    cmdOK.Enabled = False
```

```
    cmdAcak.Enabled = False

    'Tes untuk setiap p dan q sebanyak 20000 kali
    ProgressBar1.value = 0
    ProgressBar1.Max = 20000
    ProgressBar1.Visible = True
    bFound = False
    While bFound = False
        lblInfo = "Membangkitkan pasangan nilai p dan q yang sesuai
dengan syarat no.1 dan no.2 ..."
        ProgressBar1.value = 0

        Randomize Timer
        iTemp3 = Int(Rnd * 2)

        'Syarat GCD <> 1
        nLoop = 0
        Do
            'Generate p -> prima
            Randomize Timer
            iTemp1 = 6 + iTemp3
            P = GeneratePrimeNumber(iTemp1)
            'Generate q -> prima
            Randomize Timer
            iTemp2 = 2 + iTemp3
            Q = GeneratePrimeNumber(iTemp2)
            nLoop = nLoop + 1
            If nLoop >= 10000 Then
                nLoop = 0
                'Acak ulang iTemp3
                Randomize Timer
                iTemp3 = Int(Rnd * 2)
            End If
        Loop Until GCD(Q, P - 1) <> 1
        'Syarat nilai a
        lblInfo = "Membangkitkan nilai variabel a yang sesuai dengan
syarat no.3 ..."
        nLoop = 0
        Do
            'Bangkitkan nilai a baru
            Randomize Timer
            A = Int(Rnd * 100000) + 2
            'Jalankan progress bar
            nLoop = nLoop + 1
            ProgressBar1.value = nLoop
            DoEvents
            If nLoop = 20000 Then Exit Do
        Loop Until (FastExp(A, Q, P) = 1)
        bFound = (FastExp(A, Q, P) = 1)
    Wend
    txtP.Text = P
    txtQ.Text = Q
```

```
    txtA.Text = A

    lblInfo = ""
    ProgressBar1.Visible = False

    cmdOK.Enabled = True
    cmdAcak.Enabled = True
End Sub

Private Sub cmdOK_Click()
    P = Val(txtP.Text)
    Q = Val(txtQ.Text)
    A = Val(txtA.Text)
    If P = 0 Then
        MsgBox "Nilai variabel p belum diisi !", vbCritical
        Exit Sub
    ElseIf Q = 0 Then
        MsgBox "Nilai variabel q belum diisi !", vbCritical
        Exit Sub
    ElseIf A = 0 Then
        MsgBox "Nilai variabel a belum diisi !", vbCritical
        Exit Sub
    ElseIf TestPrima(P, 3) = False Then
        MsgBox "Nilai variabel p harus merupakan bilangan prima !",
vbCritical
        Exit Sub
    ElseIf TestPrima(Q, 3) = False Then
        MsgBox "Nilai variabel q harus merupakan bilangan prima !",
vbCritical
        Exit Sub
    ElseIf GCD(Q, P - 1) = 1 Then
        MsgBox "Operasi dari GCD(q, p-1) tidak boleh bernilai 1 !",
vbCritical
        Exit Sub
    ElseIf FastExp(A, Q, P) <> 1 Then
        MsgBox "Nilai dari operasi (a^q) mod p harus bernilai 1 !",
vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub cmdTestGCD_Click()

    If Val(txtQ) = 0 Or Val(txtP) - 1 = 0 Then
        MsgBox "Nilai q dan (p - 1) harus lebih besar dari 0",
vbCritical, "GCD"
        Exit Sub
    End If

    frmTestGCD.iA = txtQ.Text
    frmTestGCD.iB = Val(txtP.Text) - 1
```

```
    frmTestGCD.Show vbModal
End Sub

Private Sub Form_Load()
    Delay 800
    txtP = P
    txtQ = Q
    txtA = A
End Sub

Private Sub txtA_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub

Private Sub txtP_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub

Private Sub txtQ_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frmTestGCD.frm

```
Option Explicit
Public iA As Long
Public iB As Long
Private Sub cmdKeluar_Click()
    Unload Me
End Sub

Private Sub Form_Load()
    'Nilai awal
    txtA = iA
    txtB = iB
    'Analisis algoritma GCD
    Call AnalisisGCD(iA, iB)
End Sub

'Analisis Algoritma GCD
Private Sub AnalisisGCD(ByVal A As Double, ByVal B As Double)
    Dim X As Double
```

```
    Dim Y As Double
    Dim Z As Double
    X = A
    Y = B
    txtE = txtE & "X = " & A
    txtE = txtE & vbCrLf & "Y = " & B

    While Y <> 0
        txtE = txtE & vbCrLf & vbCrLf & _
               "WHILE " & Y & " <> 0  (TRUE)"
        Z = FModulus(X, Y)
        txtE = txtE & vbCrLf & _
               "Z = " & X & " mod " & Y & " = " & Z
        X = Y
        txtE = txtE & vbCrLf & _
               "X = " & Y
        Y = Z
        txtE = txtE & vbCrLf & _
               "Y = " & Z
    Wend
    txtE = txtE & vbCrLf & vbCrLf & _
               "WHILE " & Y & " <> 0  (FALSE)"
    txtGCD.Text = X
    txtE = txtE & vbCrLf & vbCrLf & _
               "Hasil Fungsi GCD(" & A & ", " & B & ") = " & X
End Sub
```

Form frmInputR.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Randomize Timer
    R = 1 + Int(Rnd * (Q - 1))
    txtR = R
End Sub

Private Sub cmdOK_Click()
    R = Val(txtR.Text)
    If R = 0 Then
        MsgBox "Nilai variabel r belum diisi !", vbCritical
        Exit Sub
    ElseIf R >= Q Then
        MsgBox "Nilai variabel r harus lebih kecil dari q !",
vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub Form_Load()
    Delay 800
    txtR = R
```

```
    Text1.Text = Text1.Text & vbCrLf & _
                 "- Nilai q = " & Q
End Sub

Private Sub txtR_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frmInputS.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Randomize Timer
    S = 1 + Int(Rnd * (Q - 1))
    txtS = S
End Sub

Private Sub cmdOK_Click()
    S = Val(txtS.Text)
    If S = 0 Then
        MsgBox "Nilai variabel s belum diisi !", vbCritical
        Exit Sub
    ElseIf S >= Q Then
        MsgBox "Nilai variabel s harus lebih kecil dari q !",
vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub Form_Load()
    Delay 800
    txtS = S
    Text1.Text = Text1.Text & vbCrLf & _
                 "- Nilai q = " & Q
End Sub

Private Sub txtS_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frminputE.frm

```
Option Explicit
Private Sub cmdAcak_Click()
    Randomize Timer
    E = 100 + Int(Rnd * 100000000)
```

```
    txtE = E
End Sub

Private Sub cmdOK_Click()
    E = Val(txtE.Text)
    If E = 0 Then
        MsgBox "Nilai variabel e belum diisi !", vbCritical
        Exit Sub
    End If
    Unload Me
End Sub

Private Sub Form_Load()
    Delay 800
    txtE = E
End Sub

Private Sub txtE_KeyPress(KeyAscii As Integer)
    If KeyAscii <> vbKeyBack And IsNumeric(Chr(KeyAscii)) = False
Then
        KeyAscii = 0
    End If
End Sub
```

Form frmAuthentication.frm

```
Option Explicit
Private Const nDelay = 800
Private I As Integer
Private Langkah As Integer
Private nAlice As Integer
Private nBob As Integer
Private Sub cmdKeluar_Click()
    Unload Me
End Sub

Private Sub cmdNext_Click()
    'Langkah algoritma berikutnya
    Langkah = Langkah + 1
    Call EksekusiAlgo(Langkah, True)
End Sub

Private Sub cmdPrev_Click()
    'Langkah algoritma sebelumnya
    Langkah = Langkah - 1
    Call EksekusiAlgo(Langkah, False)
End Sub

Private Sub cmdUlang_Click()
    MSFlexGrid1.Rows = 6
    MSFlexGrid2.Rows = 1
    Call ResetAlgo
End Sub
```

```
Private Sub Form_Load()
    MSFlexGrid1.TextMatrix(1, 1) = P
    MSFlexGrid1.TextMatrix(2, 1) = Q
    MSFlexGrid1.TextMatrix(3, 1) = A
    MSFlexGrid1.TextMatrix(4, 1) = S
    MSFlexGrid1.TextMatrix(5, 1) = V
    'Ulang algoritma
    Call ResetAlgo
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub

Private Sub Text1_Change()
    Text1.SelStart = Len(Text1.Text)
End Sub

Private Sub TmrAlice_Timer()
    nAlice = nAlice + 1
    If nAlice = 5 Then nAlice = 1
    PicBoxAlice.Picture = LoadPicture(App.Path & "\Gambar\Alice-" &
nAlice & ".bmp")
End Sub

Private Sub TmrBob_Timer()
    nBob = nBob + 1
    If nBob = 8 Then nBob = 1
    PicBoxBob.Picture = LoadPicture(App.Path & "\Gambar\Bob-" & nBob
& ".bmp")
End Sub

Private Sub ResetAlgo()
    lblHeader = "SKEMA OTENTIKASI ANTARA Alice DAN Bob"
    'Pasangan kunci
    R = 0
    X = 0
    t = 0
    E = 0
    Y = 0
    'Langkah algoritma
    Langkah = 0
    'TABEL VARIABEL
    With MSFlexGrid1
        .Cols = 2
        .Rows = 10
        .ColWidth(0) = 2000
        .ColAlignment(0) = 4
        .ColWidth(1) = 2250
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 6
```

```
        .TextMatrix(0, 0) = "VARIABEL"
        .TextMatrix(0, 1) = "NILAI"
        .TextMatrix(1, 0) = "p"
        .TextMatrix(2, 0) = "q"
        .TextMatrix(3, 0) = "a"
        .TextMatrix(4, 0) = "s (privat)"
        .TextMatrix(5, 0) = "v (publik)"
        .TextMatrix(6, 0) = "r"
        .TextMatrix(7, 0) = "x"
        .TextMatrix(8, 0) = "e"
        .TextMatrix(9, 0) = "y"
    End With

    'TABEL ALGORITMA
    With MSFlexGrid2
        .Cols = 2
        .Rows = 15
        .ColWidth(0) = 750
        .ColAlignment(0) = 4
        .ColWidth(1) = 5490
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 1
        .TextMatrix(0, 0) = "No."
        .TextMatrix(0, 1) = "Algoritma"
        .TextMatrix(1, 0) = "1."
        .TextMatrix(1, 1) = " Alice memilih sebuah nilai r (r < q)."
        .TextMatrix(2, 0) = "2."
        .TextMatrix(2, 1) = " Alice menghitung: "
        .TextMatrix(3, 1) = "    x = a^r mod p"
        .TextMatrix(4, 1) = " dan mengirim x kepada Bob."
        .TextMatrix(5, 0) = "3."
        .TextMatrix(5, 1) = " Bob memilih sebuah nilai e "
        .TextMatrix(6, 1) = " (e diantara 0 sampai (2^t-1))"
        .TextMatrix(7, 1) = " dan mengirim e kepada Alice "
        .TextMatrix(8, 0) = "4."
        .TextMatrix(8, 1) = " Alice menghitung:"
        .TextMatrix(9, 1) = "    y = (r + se) mod q"
        .TextMatrix(10, 1) = " dan mengirim y kepada Bob."
        .TextMatrix(11, 0) = "5."
        .TextMatrix(11, 1) = " Bob melakukan verifikasi berikut:"
        .TextMatrix(12, 1) = "    x = ((a^y).(v^e)) mod p"
        .TextMatrix(13, 1) = " Jika nilai x sesuai, maka verifikasi"
        .TextMatrix(14, 1) = " dan otentikasi berhasil."
    End With

    'Keterangan proses
    Text1.Text = ""
    cmdNext.Enabled = True
    cmdPrev.Enabled = False
End Sub
```

```
Private Sub EksekusiAlgo(nBaris As Integer, bNext As Boolean)
    cmdPrev.Enabled = False
    cmdNext.Enabled = False
    cmdUlang.Enabled = False
    cmdKeluar.Enabled = False
    Select Case nBaris
        Case 0
                'Header
                lblHeader = "SKEMA OTENTIKASI ANTARA Alice DAN Bob"
                'Hapus warna hijau dari semua baris algo
                With MSFlexGrid2
                    'Hapus warna hijau pada baris algo-2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        .CellBackColor = White
                        .CellForeColor = 0
                    Next I
                End With

                Text1.Text = ""
                'Hapus semua nilai variabel
                For I = 6 To MSFlexGrid1.Rows - 1
                    MSFlexGrid1.TextMatrix(I, 1) = ""
                Next I
        Case 1
                'Header
                lblHeader = "1. Alice memilih nilai r (r < q)"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I <= 1 Then
                            'Warna hijau pada baris algo-1
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form r
                    frmInputR.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = "1. Alice memilih nilai r sebagai
berikut:"
```

```
                    'Isi nilai r
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                     "      r = " & R
                    MSFlexGrid1.TextMatrix(6, 1) = R
                    TmrAlice.Enabled = False
               Else
                    MSFlexGrid1.TextMatrix(7, 1) = ""
                    'hapus nomor 2.
                    Temp1 = InStr(1, Text1.Text, "2.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 2
                'Header
                lblHeader = "2. Alice menghitung: x = a^r mod p dan
mengirimkan x kepada Bob"
                With MSFlexGrid2
                    .Col = 1
                For I = 1 To .Rows - 1
                        .Row = I
                        If I = 2 Or I = 3 Or I = 4 Then
                            'Warna hijau pada baris algo-2
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                'Perhitungan
                    X = FastExp(A, R, P)
                'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "2. Alice menghitung nilai x"
                'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                      "      x = a^r mod p (selesaikan dengan fast"
& vbCrLf & _
                      "                     exponentiation)"
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & A & "^" & R & " mod " & P
                    'tampilkan nilai x
```

```
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & X
                    MSFlexGrid1.TextMatrix(7, 1) = X
                    'kirimkan nilai x kepada Bob
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Alice mengirimkan x kepada Bob"
                    'Kirimkan
                    Call SendTo("Bob", "x")
                    TmrAlice.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(8, 1) = ""
                    'hapus nomor 3.
                    Temp1 = InStr(1, Text1.Text, "3.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 3
                'Header
                lblHeader = "3. Bob memilih sebuah nilai e dan
mengirimkan e kepada Alice"
                With MSFlexGrid2
                    .Col = 1
                For I = 1 To .Rows - 1
                        .Row = I
                        If I = 5 Or I = 6 Or I = 7 Then
                            'Warna hijau pada baris algo-3
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True
                'Show input form e
                    frmInputE.Show vbModal
                'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "3. Bob memilih nilai e sebagai berikut:"
                    'Isi nilai e
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      e = " & E
                    MSFlexGrid1.TextMatrix(8, 1) = E
                    'kirimkan nilai e kepada Alice
```

```
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Bob mengirimkan e kepada Alice"
                    'Kirimkan
                    Call SendTo("Alice", "e")
                    TmrBob.Enabled = False
                Else
                    MSFlexGrid1.TextMatrix(9, 1) = ""
                    'hapus nomor 4.
                    Temp1 = InStr(1, Text1.Text, "4.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 4
                'Header
                lblHeader = "4. Alice menghitung: y = (r + se) mod q
dan mengirim y kepada Bob"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 8 Or I = 9 Or I = 10 Then
                            'Warna hijau pada baris algo-4
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True

                    'Perhitungan
                    Y = FModulus((R + (S * E)), Q)

                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "4. Alice menghitung nilai y
sebagai berikut:"
                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      y = (r + se) mod q"
                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      y = (" & R & " + " & S & " . " & E & ")
```

```
mod " & Q
                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      y = " & Y
                    MSFlexGrid1.TopRow = 9
                    MSFlexGrid1.TextMatrix(9, 1) = Y

                    'kirimkan nilai y kepada Bob
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "   Alice mengirimkan y kepada Bob"

                    'Kirimkan
                    Call SendTo("Bob", "y")
                    TmrAlice.Enabled = False
                Else
                    'hapus nomor 5.
                    Temp1 = InStr(1, Text1.Text, "5.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 5
                'Header
                lblHeader = "5. Bob melakukan verifikasi x =
((a^y).(v^e)) mod p"
                With MSFlexGrid2
                    .Col = 1
                For I = 1 To .Rows - 1
                        .Row = I
                        If I >= 11 Then
                            'Warna hijau pada baris algo-4
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True
                    'Perhitungan
                    Temp2 = FastExp(A, Y, P)
                    Temp3 = FastExp(V, E, P)
                    Temp1 = FModulus(Temp2 * Temp3, P)
                    bVerifikasi = (X = Temp1)

                    'header
                    Delay nDelay
```

```
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "5. Bob melakukan verifikasi sebagai berikut:"

                    'Rumus verifikasi
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = ((a^y).(v^e)) mod p"

                    'Rumus dipecah
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = ((a^y) mod p . (v^e) mod p) mod p"

                    'Rumus dipecah
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = (" & A & "^" & Y & " mod " & P & ") .
" & vbCrLf & _
                    "(" & V & "^" & E & " mod " & P & ") " & vbCrLf
& "  mod " & P

                    'hasil-1
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                 "      x = (" & Temp2 & _
                                 " . " & Temp3 & ") mod " & P

                    'hasil-2
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                     "      " & X & " = " & Temp1 & " (" &
UCase(Format(bVerifikasi)) & ")"

                    If bVerifikasi Then
                        'Tambahan informasi u/ verifikasi
                        Text1.Text = Text1.Text & vbCrLf & _
                        "Hasil perhitungan operasi (((a^y).(v^e))
mod p) " & _
                        "sama dengan nilai x. Proses otentikasi
berhasil."

                        MsgBox "Proses verifikasi berhasil !",
vbInformation
                    Else
                        MsgBox "Proses verifikasi gagal !",
vbCritical
                    End If
            TmrBob.Enabled = False
                 End If
        End Select

    cmdPrev.Enabled = (Langkah > 0)
```

```
    cmdNext.Enabled = (Langkah < 5)
    cmdUlang.Enabled = True
    cmdKeluar.Enabled = True
End Sub

Private Sub SendTo(Receiver As String, Var As String)
    TmrAlice.Enabled = True
    TmrBob.Enabled = True

    lblVar.Caption = Var
    PicMail.Visible = True

    If Receiver = "Bob" Then
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Alice.gif")
        PicMail.Left = 2325
        While PicMail.Left < 7305
            PicMail.Left = PicMail.Left + 30
            Delay 20
        Wend
    Else
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Bob.gif")
        PicMail.Left = 7305
        While PicMail.Left > 2325
            PicMail.Left = PicMail.Left - 30
            Delay 20
        Wend
    End If

    PicMail.Visible = False

    TmrAlice.Enabled = False
    TmrBob.Enabled = False
End Sub
```

Form frmDigitalSign.frm

```
Option Explicit
Private Const nDelay = 800
Private I As Integer
Private J As Integer

Private Langkah As Integer

Private nAlice As Integer
Private nBob As Integer

Private sTemp1 As String
Private sTemp2 As String
Private sTemp3 As String
```

```
Private sTemp4 As String

Private E1() As Double
Private E2() As Double
Private Y1() As Double

Private Sub cmdKeluar_Click()
    Unload Me
End Sub

Private Sub cmdNext_Click()
    'Cek pesan
    If Langkah = 0 And txtPesan = "" Then
        MsgBox "Pesan masih kosong !", vbCritical
        Exit Sub
    End If

    'Langkah algoritma berikutnya
    Langkah = Langkah + 1
    Call EksekusiAlgo(Langkah, True)
End Sub

Private Sub cmdPrev_Click()
    'Langkah algoritma sebelumnya
    Langkah = Langkah - 1
    Call EksekusiAlgo(Langkah, False)
End Sub

Private Sub cmdUlang_Click()
    MSFlexGrid1.Rows = 6
    MSFlexGrid2.Rows = 1
    Call ResetAlgo
End Sub

Private Sub Form_Load()
    MSFlexGrid1.TextMatrix(1, 1) = P
    MSFlexGrid1.TextMatrix(2, 1) = Q
    MSFlexGrid1.TextMatrix(3, 1) = A
    MSFlexGrid1.TextMatrix(4, 1) = S
    MSFlexGrid1.TextMatrix(5, 1) = V

    'Ulang algoritma
    Call ResetAlgo
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub

Private Sub Text1_Change()
    Text1.SelStart = Len(Text1.Text)
End Sub
```

```
Private Sub TmrAlice_Timer()
    nAlice = nAlice + 1
    If nAlice = 5 Then nAlice = 1

    PicBoxAlice.Picture = LoadPicture(App.Path & "\Gambar\Alice-" &
nAlice & ".bmp")
End Sub

Private Sub TmrBob_Timer()
    nBob = nBob + 1
    If nBob = 8 Then nBob = 1

    PicBoxBob.Picture = LoadPicture(App.Path & "\Gambar\Bob-" & nBob
& ".bmp")
End Sub

Private Sub ResetAlgo()
    lblHeader = "SKEMA TANDA TANGAN DIGITAL ANTARA ALICE DAN BOB"
    'Pasangan kunci
    R = 0
    X = 0
    E = 0
    Y = 0
    'Langkah algoritma
    Langkah = 0
    'TABEL VARIABEL
    With MSFlexGrid1
        .Cols = 2
        .Rows = 8
        .ColWidth(0) = 2000
        .ColAlignment(0) = 4
        .ColWidth(1) = 2500
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 6
        .TextMatrix(0, 0) = "VARIABEL"
        .TextMatrix(0, 1) = "NILAI"
        .TextMatrix(1, 0) = "p"
        .TextMatrix(2, 0) = "q"
        .TextMatrix(3, 0) = "a"
        .TextMatrix(4, 0) = "s (privat)"
        .TextMatrix(5, 0) = "v (publik)"
        .TextMatrix(6, 0) = "r"
        .TextMatrix(7, 0) = "x"
    End With

    'TABEL ALGORITMA
    With MSFlexGrid2
        .Cols = 2
        .Rows = 15
        .ColWidth(0) = 750
        .ColAlignment(0) = 4
```

```
        .ColWidth(1) = 5490
        .FixedAlignment(1) = 4
        .ColAlignment(1) = 1
        .TextMatrix(0, 0) = "No."
        .TextMatrix(0, 1) = "Algoritma"
        .TextMatrix(1, 0) = "1."
        .TextMatrix(1, 1) = " Alice memilih sebuah nilai r (r < q)"
        .TextMatrix(2, 1) = " dan menghitung:   x = a^r mod p"
        .TextMatrix(3, 0) = "2."
        .TextMatrix(3, 1) = " Alice menggabungkan M dan x dan  "
        .TextMatrix(4, 1) = " menghitung nilai hash:"
        .TextMatrix(5, 1) = "    e = H(M, x)"
        .TextMatrix(6, 0) = "3."
        .TextMatrix(6, 1) = " Alice menghitung:"
        .TextMatrix(7, 1) = "    y = (r + se) mod q"
        .TextMatrix(8, 1) = " Tanda tangan adalah e dan y."
        .TextMatrix(9, 1) = " Alice mengirimkannya bersama pesan."
        .TextMatrix(10, 0) = "4."
        .TextMatrix(10, 1) = " Bob menghitung x':"
        .TextMatrix(11, 1) = "    x' = ((a^y).(v^e)) mod p"
        .TextMatrix(12, 0) = "5."
        .TextMatrix(12, 1) = " Bob menggabungkan M dan x' dan"
        .TextMatrix(13, 1) = " melakukan verifikasi berikut:"
        .TextMatrix(14, 1) = "    e = H(M, x')"
    End With

    'Keterangan proses
    Text1.Text = ""
    txtDigiSign.Text = ""

    cmdNext.Enabled = True
    cmdPrev.Enabled = False

End Sub

Private Sub EksekusiAlgo(nBaris As Integer, bNext As Boolean)
    cmdPrev.Enabled = False
    cmdNext.Enabled = False
    cmdUlang.Enabled = False
    cmdKeluar.Enabled = False

    Select Case nBaris
        Case 0
                txtPesan.Locked = False
                'Header
                lblHeader = "SKEMA TANDA TANGAN DIGITAL ANTARA Alice
DAN Bob"

                'Hapus warna hijau dari semua baris algo
                With MSFlexGrid2
                    'Hapus warna hijau pada baris algo-2
                    .Col = 1
```

```
                    For I = 1 To .Rows - 1
                        .Row = I
                        .CellBackColor = White
                        .CellForeColor = 0
                    Next I
                End With

                Text1.Text = ""
                'Hapus semua nilai variabel
                For I = 6 To MSFlexGrid1.Rows - 1
                    MSFlexGrid1.TextMatrix(I, 1) = ""
                Next I
        Case 1
                txtPesan.Locked = True
                'Header
                lblHeader = "1. Alice memilih nilai r (r < q) dan
menghitung: x = a^r mod p"
                With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I <= 2 Then
                            'Warna hijau pada baris algo-1
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
                    'Show input form r
                    frmInputR.Show vbModal
                    'header
                    Delay nDelay
                    Text1.Text = "1. Alice memilih nilai r sebagai
berikut:"
                    'Isi nilai r
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      r = " & R
                    MSFlexGrid1.TextMatrix(6, 1) = R

                    'Perhitungan Fast Exponentiation
                    X = FastExp(A, R, P)
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
```

```
                                  "   Alice menghitung nilai x"
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = a^r mod p (selesaikan dengan fast" &
vbCrLf & _
                    "                     exponentiation)"
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & A & "^" & R & " mod " & P
                    'tampilkan nilai x
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x = " & X
                    MSFlexGrid1.TextMatrix(7, 1) = X

                    TmrAlice.Enabled = False
                 Else
                    'hapus nomor 2.
                    Temp1 = InStr(1, Text1.Text, "2.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 2
             'Header
             lblHeader = "2. Alice menggabungkan M dan x dan
menghitung nilai hash: e = H(M, x)"
             With MSFlexGrid2
                    .Col = 1
            For I = 1 To .Rows - 1
                        .Row = I
                        If I = 3 Or I = 4 Or I = 5 Then
                            'Warna hijau pada baris algo-2
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True
            'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                     "2. Alice menggabungkan M dan x dan " & vbCrLf
& _
                     "   menghitung nilai hash:  e = H(M, x)"
```

```
                    '----------------------
                    ReDim E1(Len(txtPesan.Text))
                    For I = 1 To Len(txtPesan.Text)
                        Delay nDelay

                        'Karakter ke-i
                        sTemp1 = Mid(txtPesan.Text, I, 1)
                        M = Asc(sTemp1)                     'Nilai
message per huruf
                        sTemp2 = Format(M) & Format(X)      'Hasil
gabung
                        sTemp3 = Left(SHA.SHA1(sTemp2), 4)  'Ambil 4
karakter dari nilai hash

                        'Hasil hash dalam bentuk angka
                        sTemp4 = ""
                        For J = 1 To Len(sTemp3)
                            sTemp4 = sTemp4 & Format(Asc(Mid(sTemp3,
J, 1)))
                        Next J
                        E1(I) = Val(sTemp4)

                        Text1.Text = Text1.Text & vbCrLf & vbCrLf &
_
                      "   M(" & I & ") = ascii dari '" & sTemp1 & "'
= " & M & vbCrLf & _
                      "   (M(" & I & "),x) = M(" & I & ") digabung
dengan x " & vbCrLf & _
                      "   (M(" & I & "),x) = " & sTemp2 & vbCrLf & _
                      "   e(" & I & ") = H(" & sTemp2 & ") " &
vbCrLf & _
                      "   e(" & I & ") = " & E1(I)
                    Next I
                    '----------------------

                    TmrAlice.Enabled = False
                Else
                    'hapus nomor 3.
                    Temp1 = InStr(1, Text1.Text, "3.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                    txtDigiSign.Text = ""
                End If
            Case 3
              'Header
              lblHeader = "3. Alice menghitung: y = (r + se) mod q.
Tanda tangan adalah e dan y."
            With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 6 Or I = 7 Or I = 8 Or I = 9 Then
```

```
                            'Warna hijau pada baris algo-3
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrAlice.Enabled = True

                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "3. Alice menghitung nilai y
sebagai berikut:"

                    'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                                 "      y = (r + se) mod q"

                    '----------------------
                    txtDigiSign.Text = ""
                    ReDim Y1(Len(txtPesan.Text))
                    For I = 1 To Len(txtPesan.Text)
                        Delay nDelay

                        'Hitung Y(I)
                        Y1(I) = FModulus(R + (S * E1(I)), Q)

                        Text1.Text = Text1.Text & vbCrLf & vbCrLf &
_
        "   y(" & I & ") = (r + (s . e(" & I & "))) mod q" & vbCrLf
& _
        "   y(" & I & ") = (" & R & " + (" & S & " . " & E1(I) & "))
mod " & Q & vbCrLf & _
        "   y(" & I & ") = " & Y1(I)
        'Tanda tangan
                        txtDigiSign.Text = txtDigiSign.Text & "|" &
E1(I) & "," & Y1(I)
                    Next I
                    '----------------------
        'Rumus y
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "   Tanda tangan digital adalah e
dan y."
        'Kirimkan
```

```
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
               "   Alice mengirimkan pesan dan tanda tangan digital"
& vbCrLf & "   kepada Bob."
               Call SendTo("Bob")
                Else
                    'hapus nomor 4.
                    Temp1 = InStr(1, Text1.Text, "4.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 4
                'Header
                lblHeader = "4. Bob menghitung x' = ((a^y).(v^e))
mod p"
               With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I = 10 Or I = 11 Then
                            'Warna hijau pada baris algo-4
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True

                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                    "4. Bob melakukan perhitungan sebagai berikut:"

                    'Rumus verifikasi
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & _
                    "      x' = ((a^y).(v^e)) mod p"

                    ReDim Xa(Len(txtPesan.Text))

                    For I = 1 To Len(txtPesan.Text)
                        'Perhitungan
                        Temp2 = FastExp(A, Y1(I), P)
                        Temp3 = FastExp(V, E1(I), P)
                        Xa(I) = FModulus(Temp2 * Temp3, P)
```

```
                        'Rumus dipecah
                        Delay nDelay
                        Text1.Text = Text1.Text & vbCrLf & vbCrLf &
_
                  "   x'(" & I & ") = ((a^y(" & I & ")) mod p .
(v^e(" & I & ")) mod p) mod p"

                        'Rumus dipecah
                        Text1.Text = Text1.Text & vbCrLf & _
                 " x'(" & I & ") = (" & A & "^" & Y1(I) & " mod " &
P & ") . " & vbCrLf & _
                 " (" & V & "^" & E1(I) & " mod " & P & ") " &
vbCrLf & _
                 "  mod " & P

                        'hasil-2
                        Text1.Text = Text1.Text & vbCrLf & _
                   "   x'(" & I & ") = " & Xa(I)
                    Next I
                   TmrBob.Enabled = False
                Else
                    'hapus nomor 5.
                    Temp1 = InStr(1, Text1.Text, "5.")
                    Text1.Text = Left(Text1.Text, Temp1 - 5)
                End If

        Case 5
         'Header
         lblHeader = "5. Bob menggabungkan M dan x' dan melakukan
verifikasi berikut: e = H(M, x')"
         With MSFlexGrid2
                    .Col = 1
                    For I = 1 To .Rows - 1
                        .Row = I
                        If I >= 12 Then
                            'Warna hijau pada baris algo-5
                            .CellBackColor = DGreen
                            .CellForeColor = White
                        Else
                            'Warna putih pada baris algo lainnya
                            .CellBackColor = White
                            .CellForeColor = 0
                        End If
                    Next I
                End With

                If bNext Then
                    TmrBob.Enabled = True
                    'header
                    Delay nDelay
                    Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
                                 "5. Bob menggabungkan M dan x' dan
```

```
" & vbCrLf & _
                                "   melakukan verifikasi:  e = H(M,
x')"
                    '----------------------
                    ReDim E2(Len(txtPesan.Text))
                    For I = 1 To Len(txtPesan.Text)
                        Delay nDelay

                        'Karakter ke-i
                        sTemp1 = Mid(txtPesan.Text, I, 1)
                        M = Asc(sTemp1)                     'Nilai
message per huruf
                        sTemp2 = Format(M) & Format(Xa(I))
'Hasil gabung
                        sTemp3 = Left(SHA.SHA1(sTemp2), 4)  'Ambil 4
karakter dari nilai hash

                        'Hasil hash dalam bentuk angka
                        sTemp4 = ""
                        For J = 1 To Len(sTemp3)
                            sTemp4 = sTemp4 & Format(Asc(Mid(sTemp3,
J, 1)))
                        Next J
                        E2(I) = Val(sTemp4)
                        bVerifikasi = (E1(I) = E2(I))

         Text1.Text = Text1.Text & vbCrLf & vbCrLf & _
         " M(" & I & ") = ascii dari '" & sTemp1 & "' = " & M &
vbCrLf & _
         " (M(" & I & "),x'(" & I & ")) = M(" & I & ") digabung
dengan x'(" & I & ")" & vbCrLf & _
         "   (M(" & I & "),x'(" & I & ")) = " & sTemp2 & vbCrLf & _
         "   e(" & I & ") = H(" & sTemp2 & ")" & vbCrLf & _
         "   " & E1(I) & " = " & E2(I) & " (" &
UCase(Format(bVerifikasi)) & ")"

                        If bVerifikasi = False Then
                            MsgBox "Proses verifikasi gagal !",
vbCritical
                            Exit For
                        End If
                    Next I
                    '----------------------
                    If bVerifikasi Then
                        'Tambahan informasi u/ verifikasi
                        Text1.Text = Text1.Text & vbCrLf & _
                        "Hasil perhitungan operasi H(M, x') sama
dengan nilai e " & _
                        "sehingga proses verifikasi tanda tangan
digital berhasil."

                        MsgBox "Proses verifikasi berhasil !",
```

```
vbInformation
                    End If
                  TmrBob.Enabled = False
                End If
        End Select

    cmdPrev.Enabled = (Langkah > 0)
    cmdNext.Enabled = (Langkah < 5)
    cmdUlang.Enabled = True
    cmdKeluar.Enabled = True
End Sub

Private Sub SendTo(Receiver As String)
    TmrAlice.Enabled = True
    TmrBob.Enabled = True
PicMail.Visible = True
If Receiver = "Bob" Then
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Alice.gif")
        PicMail.Left = 2325
        While PicMail.Left < 7305
            PicMail.Left = PicMail.Left + 30
            Delay 20
        Wend
    Else
        PicMail.Picture = LoadPicture(App.Path & "\Gambar\Mail-
Bob.gif")
        PicMail.Left = 7305
        While PicMail.Left > 2325
            PicMail.Left = PicMail.Left - 30
            Delay 20
        Wend
    End If

    PicMail.Visible = False
TmrAlice.Enabled = False
    TmrBob.Enabled = False
End Sub

Private Sub txtPesan_KeyPress(KeyAscii As Integer)
    If KeyAscii = 13 Then KeyAscii = 0
End Sub
```

Form frmTeori.frm

```
Option Explicit
Private Langkah As Integer

Private Sub cmdKeluar_Click()
    Unload Me
```

```
End Sub

Private Sub cmdNext_Click()
    Langkah = Langkah + 1
    Call EksekusiLangkah
End Sub

Private Sub cmdPrev_Click()
    Langkah = Langkah - 1
    Call EksekusiLangkah
End Sub

Private Sub Form_Load()
    Langkah = 1
    Call EksekusiLangkah
End Sub

Private Sub EksekusiLangkah()
    Picture1.Picture = LoadPicture(App.Path & "\Gambar\Teori-" &
Langkah & ".gif")
    cmdNext.Enabled = (Langkah < 12)
    cmdPrev.Enabled = (Langkah > 1)
End Sub

Private Sub Form_Unload(Cancel As Integer)
    frmMenu.Show
End Sub
```

Form frmAbout.frm

```
Private Sub cmdOK_Click()
    Unload Me
End Sub
```

LAMPIRAN B

Daftar Penguji Dan Kuisioner

Tabel 5.1 Daftar Penguji

NO	Nama Penguji	Pekerjaan	Instansi
1	Achmad Jiswan	Mahasiswa	Teknik Informatika Multimedia STMIK AMIKOM Yogyakarta
2	Andhika Danawiputra	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
3	Aditya WN	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
4	Ahmad Hafid	Mahasiswa	Prodi Teknik Informatika, Universitas Pembangunan Nasional "Veteran" Yogyakarta
5	Agung Rahmawan	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
6	Ahmad Ashar Aras	Mahasiswa	Prodi Seni Teater ISI Yogyakarta
7	Ahmad Athaullah	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
8	Hafidz Syabiq	Mahasiswa	Prodi Pendidikan Bahasa Arab, Fak Tarbiyah UIN Sunan Kalijaga.
9	Healdy	Mahasiswa	Teknik Informatika Jaringan Komputer STMIK AMIKOM Yogyakarta
10	Irvan Arifin	Wiraswasta	-
11	Luthfi Noor Ichsan	Mahasiswa	Prodi Bimbingan dan Penyuluhan Islam, Fak Dakwah UIN Sunan Kalijaga
12	Irwan Saputra	Mahasiswa	Sistem Informasi, Broadcasting TV STMIK AMIKOM Yogyakarta
13	Kamaruddin	Mahasiswa	Sistem Komputer, Universitas Teknologi Yogyakarta
14	Kadir	Mahasiswa	Prodi Komunikasi dan Penyiaran Islam, Fak Dakwah UIN Sunan Kalijaga
15	Muhammad Tahir	Mahasiswa	Teknik Informatika, Jaringan Komputer STMIK AMIKOM Yogyakarta

16	Marta Ika Wijayati	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
17	Muhammad Tasdik	Mahasiswa	Prodi Pendidikan Agama Islam, Fak Tarbiyah UIN Sunan Kalijaga
18	Muhammad Zaenudin Latief	Mahasiswa	Prodi Pendidikan Agama Islam, Fak Tarbiyah UIN Sunan Kalijaga
19	Muhammad Aras	Swasta	CV.Multivisindo Yogyakarta
20	Maulana Ashar Sakti	Mahasiswa	Teknik Industri, Universitas Teknologi Yogyakarta
21	M Aslam S	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
22	Nursyam Fahrurozie	Mahasiswa	Prodi Fisika, Fak Saintek UIN Sunan Kalijaga.
23	Qori Ulvi	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
24	Restu Umar Singgih	Mahasiswa	Teknik Pertambangan, Universitas Pembangunan Nasional "Veteran" Yogyakarta
25	Ryan Adi Putra	Mahasiswa	Teknik Komputer AKAKOM
26	Sarbunis	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
27	Syifa Q.A	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
28	Sutrisno	Mahasiswa	Prodi Teknik Informatika, Fak Saintek UIN Sunan Kalijaga.
29	Syamsuddin	Mahasiswa	Prodi Keuangan Islam, Fak Syariah UIN Sunan Kalijaga.
30	Susi Susanti	Mahasiswa	Psikologi, Universitas Ahmad Dahlan Yogyakarta

LAMPIRAN C

Daftar Kuisioner

ANGKET PENGUJIAN SISTEM

Nama : Achmad Jiswan

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.				
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.				
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.				
4	Sistem ini memberikan Form Input Variabel r dengan jelas.				
5	Sistem ini memberikan Form Input Variabel e dengan jelas.				
6	Sistem ini menampilkan Form Digital Signature dengan jelas.				
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.				

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.				
2	Interface menarik.				
3	Animasi yang cukup menarik.				
4	Waktu Loading system relative cepat.				
5	Menu pada sistem sudah berfungsi dengan baik.				

ANGKET PENGUJIAN SISTEM

Nama : Andhika Danawiputra

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Aditya WN

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Ahmad Hafid

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Agung Rahmawan

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.			✓	
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Ahmad Ashar Aras

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Ahmad Athaullah

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.			✓	
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Hafidz Syabiq

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Healdy

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Irvan Arifin

Pekerjaan : Wiraswasta

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.			✓	
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.			✓	
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.			✓	
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.			✓	

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Luthfi Noor Ichsan

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Irwan Saputra

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Kamaruddin

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Kadir

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Tahir

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Marta Ika Wijayanti

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Tasdik

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Zaenudin Latief

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Muhammad Aras

Pekerjaan : Swasta

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Maulana Ashar Sakti

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : M Aslam S

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Nursyam Fahrurozie

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Qori Ulvi

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.			✓	

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.		✓		
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Restu Umar Singgih

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Ryan Adi Putra

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.			✓	
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.			✓	
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.			✓	
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.			✓	

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.			✓	
2	Interface menarik.			✓	
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Sarbunis

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.	✓			
5	Sistem ini memberikan Form Input Variabel e dengan jelas.	✓			
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Syifa Q.A

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Sutrisno

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.	✓			

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.	✓			

ANGKET PENGUJIAN SISTEM

Nama : Syamsuddin

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.		✓		
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.		✓		
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.	✓			
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.		✓		
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.		✓		
3	Animasi yang cukup menarik.		✓		
4	Waktu Loading system relative cepat.	✓			
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

ANGKET PENGUJIAN SISTEM

Nama : Susi Susanti

Pekerjaan : Mahasiswa

Pengujian Fungsionalitas Sistem

No	Pernyataan	SS	S	TS	STS
1	Sistem ini memberikan Form Input variabel q, p dan a dengan jelas.	✓			
2	Sistem ini memberikan penjelasan tentang Test GCD dengan jelas.	✓			
3	Sistem ini memberikan penjelasan tentang Konsep Digital Signature dengan jelas.		✓		
4	Sistem ini memberikan Form Input Variabel r dengan jelas.		✓		
5	Sistem ini memberikan Form Input Variabel e dengan jelas.		✓		
6	Sistem ini menampilkan Form Digital Signature dengan jelas.	✓			
7	Sistem ini memberikan penjelasan algoritma Authentication dengan jelas.		✓		

Pengujian *Interface* dan Pengaksesan

No	Pernyataan	SS	S	TS	STS
1	Konten yang disediakan sederhana sehingga memudahkan bagi pengguna.	✓			
2	Interface menarik.	✓			
3	Animasi yang cukup menarik.	✓			
4	Waktu Loading system relative cepat.		✓		
5	Menu pada sistem sudah berfungsi dengan baik.		✓		

CURRICULUM VITAE

Nama	: Jusmail
Tempat, tanggal lahir	: Jambi, 06 Juli 1986
Jenis Kelamin	: Laki – Laki
Agama	: Islam
Alamat Asal	: Jln.Harapan No.48 Desa Simbur Naik, Dusun Karya Kec.Muara Sabak, Kab. Tanjung Jabung Timur Jambi.
No.Ho	: +6281215763612
Email	: jusmailelbugisy@yahoo.co.id/jusmbugis@gmail.com

Riwayat Pendidikan :

1. TK Dharma Wanita (1992)
2. SD Negeri 67 Simbur Naik (1993-1999)
3. MTS Pondok Pesantren Al-Busyra Jambi (1999-2002)
4. MA Pondok Pesantren Ummul Quro Al-Islamy Bogor (2002-2006)
5. S1 Teknik Informatika UIN Sunan Kalijaga Yogyakarta (2006-2011)

Pengalaman Organisasi :

1. Ketua ISPA Pon-Pes UQI Bogor	Jabatan Ketua Umum (2004-2005)
2. PMII Rayon Fakultas Saintek	Jabatan Dev. Pengkaderan (2008-2009)
3. KAPEMA Tanjabtim Jambi	Jabatan Dev. Intelektualitas (2008-2009)
4. BEM-F Sains & Teknologi	Jabatan Dev. Advokasi (2009-2010)
5. FKM Bone Yogyakarta	Jabatan Sekjen (2010-2011)