

**PEMBENTUKAN KATA SANDI MENGGUNAKAN
PERTUKARAN KUNCI STICKEL ATAS ALJABAR
MIN-PLUS UNTUK MENGAMANAKAN INFORMASI
RAHASIA**

SKRIPSI

Untuk memenuhi sebagian persyaratan mencapai derajat Sarjana S-1

Program Studi Matematika



MAHENDRA FAKHRUL FATHAN

13610007

**STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA**

KEPADA

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2017



SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :

Lamp :

Kepada

Yth. Dekan Fakultas Sains dan 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 : Mahendra Fakhru Fathan
NIM : 13610007
Judul Skripsi : Pembentukan Kata Sandi Menggunakan Pertukaran Kunci Stickel Atas Aljabar Min-Plus untuk Mengamankan Informasi Rahasia

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Bidang Matematika.

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

Wassalamu'alaikum wr. wb.

Pembimbing I

Dr. M. Wakhid Musthofa, M.Si.
NIP. 19800402 200501 1 003

Yogyakarta, 23 Mei 2017

Pembimbing II

Muhamad Zaki Riyanto, M.Sc
NIP. 19840113 201503 1 001



PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B- 1847/Un.02/DST/PP.05.3/06/ 2017

Skripsi/Tugas Akhir dengan judul : Pembentukan Kata Sandi Menggunakan Pertukaran Kunci Stickel Atas Aljabar Min – Plus untuk Mengamankan Informasi Rahasia

Yang dipersiapkan dan disusun oleh :
Nama : Mahendra Fakhrul Fathan
NIM : 13610007
Telah dimunaqasyahkan pada : 30 Mei 2017
Nilai Munaqasyah : A

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

TIM MUNAQASYAH :

Ketua Sidang

Dr. Muhammad Wakhid Musthofa, M.Si
NIP. 19800402 200501 1 003

Penguji I

M. Zaki Riyanto, M.Sc
NIP.19840113 201503 1 001

Penguji II

Malahayati, M.Sc
NIP.19840412 201101 2 010

Yogyakarta, 6 Juni 2017
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi

Dekan



Dr. Murtono, M.Si
NIP. 19691212 200003 1 001

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini

Nama : Mahendra Fakhrol Fathan

NIM : 13610007

Program Studi : Matematika

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 23 Mei 2017



Mahendra Fakhrol Fathan

NIM. 13610007

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

HALAMAN PERSEMBAHAN

Karya ini penulis persembahkan untuk bapak dan ibu tercinta yang telah membesarkan, mendoakan dan selalu memberikanku semangat. Berkat doa dan kerja keras kalian tugas ini dapat terselesaikan.

Kepada saudara-saudaraku yang senantiasa menjadi motivasi penulis untuk menyelesaikan tugas akhir ini. Kepada keluarga besar matematika angkatan 2013 dan kampusku tercinta UIN Sunan Kalijaga Yogyakarta.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

HALAMAN MOTTO

”Kami telah turunkan kepadamu Al-Dzikir (Al-Quran) untuk kamu terangkan kepada manusia apa-apa yang diturunkan kepada mereka agar mereka berpikir”

(Q.S Al An’am : 44)

”Sesungguhnya bersama kesukaran itu ada keringanan. Karena itu bila kau sudah selesai (mengerjakan yang lain). Dan berharaplah kepada Tuhanmu”

(Q.S Al Insyirah : 6-8)

”Allah mencintai pekerjaan yang apabila bekerja ia menyelesaikannya dengan baik”

(HR. Thabrani)

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

KATA PENGANTAR

Assalamualaikum Wr Wb

Puji syukur kehadirat Allah yang telah memberikan limpahan rahmat, taufik dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi yang berjudul "*Pembentukan Kata Sandi Menggunakan Pertukaran Kunci SticKel untuk Mengamankan Informasi Rahasia*" ini dengan semaksimal mungkin. Shalawat dan salam senantiasa tercurah kepada baginda Muhammad SAW, teladan bagi seluruh umat manusia.

Penulis menyadari bahwa proses penulisan skripsi ini tidak terlepas dari dukungan, motivasi, dan bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Ibu Dr. Murtono, M.Si selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
2. Bapak Dr. M. Wakhid Musthofa, M.Si selaku Ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga, dan juga pembimbing skripsi yang telah berkenan memberikan bimbingan serta arahan sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
3. Bapak M. Zaki Riyanto, M.Sc selaku pembimbing skripsi yang telah berkenan memberikan bimbingan serta arahan sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
4. Bapak M. Farhan Qudratullah, M.Si selaku dosen pembimbing akademik yang telah memberikan pengarahan kepada penulis selama kuliah.

5. Bapak/Ibu Dosen dan Staf Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta atas ilmu, bimbingan dan pelayanan selama perkuliahan dan penyusunan skripsi ini selesai.
6. Bapak dan Ibuku tercinta, serta kakak dan adikku tersayang yang selalu memberikan semangat, nasehat dan do'a-do'anya yang tiada henti, sehingga penulis termotivasi untuk mengerjakan skripsi ini dengan giat.
7. Teman-teman matematika angkatan 2013 atas kebersamaan yang tak mudah dilupakan dan semua pihak yang turut membantu hingga selesainya skripsi ini yang tidak dapat penulis sebutkan satu persatu, terima kasih.

Penulis menyadari masih banyak kesalahan dan kekurangan dalam penulisan skripsi ini, untuk itu diharapkan saran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini. Namun demikian, penulis tetap berharap semoga skripsi ini dapat bermanfaat dan dapat membantu memberi suatu informasi yang baru bagi semua orang yang membacanya.

Wassalamualaikum Wr Wb

Yogyakarta, 29 Mei 2017

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Mahendra Fakhru Fathan

DAFTAR ISI

HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTTO	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR TABEL	xiii
DAFTAR LAMBANG	xiv
ABSTRAK	xv
I PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Batasan Masalah	4
1.3. Rumusan Masalah	4
1.4. Tujuan Penulisan	5
1.5. Manfaat Penelitian	5
1.6. Tinjauan Pustaka	6
1.7. Metode Penelitian	8
1.8. Sistematika Penulisan	9
II DASAR TEORI	11
2.1. Semigrup	11
2.2. Semiring	13
2.3. Semifield	15

2.4. Semiring Polinomial	15
2.5. Semimodul	23
III ALJABAR MIN-PLUS	24
3.1. Definisi Aljabar Min Plus	24
3.2. Matriks Atas Aljabar Min-Plus	29
3.3. Polinomial atas Aljabar Min-Plus	38
IV PROTOKOL PERTUKARAN KUNCI STICKEL ATAS ALJABAR MIN-PLUS	47
4.1. Kriptografi	47
4.1.1. Definisi Kriptografi	47
4.1.2. Sejarah Kriptografi	48
4.1.3. Algoritma Kriptografi	49
4.1.4. Sistem Kriptografi	50
4.2. Sejarah Protokol Pertukaran Kunci	51
4.3. Protokol Pertukaran Kunci Atas Aljabar Min-Plus	54
4.4. Perhitungan Protokol Pertukaran Kunci atas Aljabar Min-Plus	56
4.4.1. Sandi Vigenere	63
V IMPLEMENTASI DAN UJI COBA	68
5.1. Sarana Implementasi	68
5.1.1. Perangkat keras (<i>hardware</i>)	68
5.1.2. Perangkat lunak (<i>software</i>)	69
5.2. Pembuatan Program	69
5.3. Uji Coba Program	79
VI PENUTUP	86
6.1. Kesimpulan	86
6.2. Saran	87
DAFTAR PUSTAKA	89

A	SKRIP PROGRAM MATLAB PEMBENTUKAN KATA SANDI MENGGUNAKAN PERTUKARAN KUNCI STICKEL ATAS ALJABAR MINUS PLUS	90
B	SKRIP PROGRAM MATLAB ENKRIPSI DAN DEKRIPSI	115
C	TABEL KODE ASCII 1	124
D	TABEL KODE ASCII 2	125



STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR TABEL

1.1	Tinjauan Pustaka	7
4.1	Skema Protokol Pertukaran Kunci Diffie-Hellman	52
4.2	Skema Protokol Pertukaran Kunci Sticklel	53
4.3	Skema Protokol Pertukaran Kunci Sticklel atas Semiring	54
4.4	Skema Protokol Pertukaran Kunci Sticklel atas Aljabar Min Plus	55
4.5	Skema Pengembangan Protokol Pertukaran Kunci Sticklel atas Al- jabar Min Plus	56
5.1	Spesifikasi perangkat keras	68
5.2	Spesifikasi perangkat lunak	69
5.3	Properti Algoritma Protokol Pertukaran Kunci atas Aljabar Min Plus	70
5.4	Properti Enkripsi dan Dekripsi	72

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR GAMBAR

1.1	Alur Penelitian	9
1.2	Alur Sistematika Penelitian	10
4.1	Skema Sistem Kriptografi Simetris	51
5.1	Desain program Algoritma Protokol Pertukaran Kunci atas Aljabar Min Plus	70
5.2	Desain Program Enkripsi dan Dekripsi	71
5.3	Tampilan Awal Program	79
5.4	Input Data 1	80
5.5	Didapatkan Matriks V	81
5.6	Input Matriks V	82
5.7	Didapatkan Kunci Rahasia Bersama	82
5.8	Desain Program Enkripsi dan Dekripsi	83
5.9	Input Kunci dan Plainteks	84
5.10	Didapatkan Cipherteks	84
5.11	Input Kunci dan Cipherteks	84
5.12	Didapatkan Plainteks	85

DAFTAR LAMBANG

\mathbb{Z}	: Himpunan semua bilangan bulat
\mathbb{R}	: Himpunan semua bilangan real
$\mathbb{R}^+ \cup \{0\}$: Himpunan semua bilangan real non negatif
ε	: Elemen netral terhadap operasi minimum ($\varepsilon := +\infty$)
\mathbb{Z}_ε	: $\mathbb{Z} \cup \{\varepsilon\}$
\otimes	: Operasi perkalian pada aljabar min-plus
\oplus	: Operasi penjumlahan pada aljabar min-plus
■	: akhir suatu bukti
\mathbb{Z}_{min}	: $(\mathbb{Z}_\varepsilon, \oplus, \otimes)$
\rightarrow	: menuju
$\mathbb{Z}_{min}^{n \times n}$: Matriks persegi atas aljabar min-plus
$\mathbb{Z}_{min}[x]$: Polinomial atas aljabar min-plus

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

ABSTRAK

PEMBENTUKAN KATA SANDI MENGGUNAKAN PERTUKARAN KUNCI STICKEL ATAS ALJABAR MIN-PLUS UNTUK MENGAMANANKAN INFORMASI RAHASIA

Oleh

MAHENDRA FAKHRUL FATHAN

13610007

Pesan yang dikirimkan melalui jalur yang tidak aman sangat rentan untuk disadap, maka diperlukan solusi untuk mengamankan informasi. Salah satu cara mengamankan pesan adalah menggunakan kriptografi yaitu dengan menyandikan isi pesan (plainteks) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi, dan untuk memperoleh isi pesan asli dilakukan dekripsi, disertai kunci yang sama. Kesepakatan kunci dapat dikakukan walaupun kedua belah pihak tidak saling bertemu, dengan menggunakan protokol pertukaran kunci.

Protokol pertukaran kunci pertama kali diperkenalkan oleh Diffie-Hellman, protokol ini menggunakan struktur aljabar komutatif dan keamanannya diletakkan pada masalah logaritma diskrit. Adanya ancaman komputer kuantum dimasa depan mengakibatkan protokol dengan struktur aljabar komutatif akan mudah untuk dipecahkan. Pengembangan protokol pertukaran kunci menggunakan struktur aljabar non-komutatif diharapkan mampu meningkatkan keamanan kunci rahasia, salah satunya yaitu protokol pertukaran kunci Stickel dengan menggunakan struktur aljabar non komutatif.

Tugas akhir ini membahas mengenai protokol pertukaran kunci Stickel menggunakan polinomial dan matriks atas aljabar min-plus. Keamanan protokol pertukaran kunci ini diletakkan pada permasalahan dekomposisi. Protokol pertukaran kunci ini menggunakan polinomial dan matriks atas aljabar min-plus. Pihak penyadap akan sulit mengetahui kunci rahasianya karena harus memecahkan fungsi polinomial yang digunakan oleh kedua belah pihak.

Kata Kunci : Kriptografi, Aljabar Min-Plus, Protokol Pertukaran Kunci, Semiring

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Komunikasi adalah hal yang sangat penting dalam kehidupan bersosialisasi, karena dengan berkomunikasi manusia dapat bertukar informasi satu sama lain. Sebagaimana dijelaskan dalam Al-Qur'an surat An-Nissa' ayat 83,

وَإِذَا جَاءَهُمْ أَمْرٌ مِّنَ الْأَمْنِ أَوْ الْخَوْفِ أَذَاعُوا بِهِ ۗ وَلَوْ
رَدُّوهُ إِلَى الرَّسُولِ وَإِلَىٰ أُولِي الْأَمْرِ مِنْهُمْ لَعَلِمَهُ الَّذِينَ يَسْتَنْبِطُونَهُ
مِنْهُمْ ۗ وَلَوْلَا فَضْلُ اللَّهِ عَلَيْكُمْ وَرَحْمَتُهُ لَاتَّبَعْتُمُ الشَّيْطَانَ إِلَّا
قَلِيلًا ﴿٨٣﴾

Artinya, “Dan apabila datang kepada mereka suatu berita tentang keamanan ataupun ketakutan, mereka lalu menyiarkannya. Dan kalau mereka menyerahkan kepada Rasul dan Ulil Amri di antara mereka, tentulah orang-orang yang ingin mengetahui kebenaran (akan dapat) mengetahui dari mereka (Rasul dan Ulil Amri). Kalau tidaklah karena karunia dan rahmat Allah kepada kamu, tentulah kamu mengikuti syaitan, kecuali sebagian kecil saja (di antara kamu)”.

Potongan ayat di atas menunjukkan bahwa Allah telah memerintahkan umatnya untuk saling memberi kabar satu sama lain, cara memberi kabar yaitu dengan saling berkomunikasi. Dahulu manusia berkomunikasi hanya dengan menggunakan lisan dan tulisan tangan (surat) saja. Namun seiring perkembangan teknologi, kini

komunikasi dapat dilakukan dengan berbagai media, seperti *handphone* dan komputer. Salah satu jalur yang saat ini banyak digunakan adalah jalur yang tidak aman yaitu jalur internet. Semua orang dapat menggunakan jalur komunikasi internet secara bebas, baik yang berhak maupun yang tidak berhak memperoleh informasi tersebut. Sehingga rawan terjadi penyadapan dan pengubahan informasi yang akan disampaikan kepada orang yang berhak.

Keamanan informasi sangat dibutuhkan terlebih informasi yang bersifat rahasia. Informasi-informasi yang rahasia banyak dikirimkan melalui jalur yang tidak aman, maka pihak yang tidak berhak dapat menyadap bahkan mengubah informasi tersebut. Dibutuhkan solusi untuk mengamankan informasi tersebut agar pihak yang tidak berhak tidak dapat membaca isi informasi dan menyadapnya.

Kriptografi memberikan solusi terhadap permasalahan keamanan informasi. Konsep kriptografi sudah ditemukan sejak jaman Mesir kuno kira-kira 4.000 tahun yang lalu dan terus berkembang sampai sekarang seiring perkembangan teknologi dalam bidang informasi. Kriptografi sendiri berasal dari bahasa Yunani yaitu *cryptos* dan *graphien*. *Cryptos* berarti rahasia dan *graphien* berarti tulisan. Sehingga menurut bahasa kriptografi berarti tulisan rahasia. Sedangkan menurut istilah kriptografi berarti suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, dan autentikasi data (Menezes, Oorschot, dan Vanstone, 1996). Kriptografi memberikan keamanan terhadap suatu informasi rahasia yang dikirimkan melalui jalur yang tidak aman, sehingga pihak ketiga tidak dapat memahami dan menyadap informasi rahasia tersebut.

Proses utama dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi adalah suatu proses penyandian yang melakukan perubahan suatu pesan yang dapat dimengerti (plaintexts), menjadi kode yang sulit dimengerti (chiphertexts). Sedangkan

proses kebalikannya, untuk mengubah ciphertext menjadi plaintext disebut dekripsi. Enkripsi dan dekripsi memerlukan sebuah kunci yang hanya diketahui oleh pihak yang saling berkomunikasi. Pembentukan kunci rahasia dapat dilakukan dengan bertemu secara langsung. Namun jika kedua belah pihak tidak memungkinkan untuk bertemu, maka diperlukan metode untuk melakukan perjanjian kunci yaitu protokol perjanjian kunci. Metode ini membantu kedua belah pihak yang tidak bertemu untuk melakukan perjanjian kunci rahasia yang sama dengan aman walaupun melalui jalur yang tidak aman. Kunci rahasia tersebut nantinya akan digunakan untuk mengirimkan pesan yang sudah di enkripsi dan untuk dekripsi pesan.

Protokol pertukaran kunci pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman (1976). Selanjutnya protokol ini dinamai dengan protokol Diffie-Hellman sesuai dengan nama penemunya, dalam protokol tersebut mereka menggunakan struktur aljabar komutatif, yaitu grup siklik. Keamanan pada protokol pertukaran kunci Diffie-Helman terletak pada masalah logaritma diskrit. Namun, adanya ancaman komputer kuantum di masa depan membuat masalah logaritma diskrit menjadi mudah untuk dipecahkan (Peter W. Shor, 1997). Sehingga saat ini banyak peneliti yang mengembangkan protokol pertukaran kunci dengan kunci non komutatif yang diharapkan keamanannya lebih tinggi dan sulit untuk dipecahkan, di antaranya adalah :

1. Stickel (2005) memperkenalkan protokol pertukaran kunci menggunakan grup non-komutatif.
2. Dima Grigoriev dan Vladimir Shpilrain (2012) mengembangkan protokol pertukaran kunci Stickel dengan menggunakan semiring non-komutatif aljabar min-plus.
3. Musthofa dan Dwi Lestari (2014) meneliti tentang Metode perjanjian *pass-*

word berdasarkan operasi matriks atas aljabar min-plus untuk keamanan pengiriman informasi rahasia.

Berdasarkan penelitian-penelitian tersebut penulis tertarik meneliti tentang pembentukan sandi menggunakan pertukaran kunci Stickel atas aljabar min-plus untuk mengamankan informasi rahasia.

1.2. Batasan Masalah

Batasan masalah sangat diperlukan untuk memfokuskan sebuah pembahasan guna menghindari meluas dan kesimpangsiuran pembahasan. Berdasarkan latar belakang masalah, penelitian ini difokuskan untuk membahas pembentukan kunci rahasia menggunakan semiring non-komutatif yaitu aljabar min plus. Setelah diperoleh kunci rahasia, penulis akan memberikan contoh proses enkripsi dan dekripsi pesan dengan menggunakan algoritma kriptografi simetris yaitu sandi Vigenere. Diberikan pula program MATLAB perhitungan dalam pembentukan kunci rahasia menggunakan protokol pertukaran kunci Stickel dan proses enkripsi dekripsi menggunakan sandi Vigenere.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang telah diaparkan, maka dirumuskan permasalahan-permasalahan sebagai berikut :

1. Bagaimana konsep matematis yang melandasi prosedur pembentukan sandi pada sistem kriptografi simetris?
2. Bagaimana langkah-langkah yang digunakan untuk memperoleh kunci rahasia menggunakan protokol pertukaran kunci stickel atas semiring aljabar min plus?

3. Bagaimana proses perhitungan enkripsi dan dekripsi menggunakan sistem kriptografi simetris dengan sandi Vigenere?
4. Bagaimana implementasi perhitungan protokol pertukaran kunci Stickel atas semiring aljabar min plus dan proses enkripsi serta dekripsi menggunakan sandi Vigenere pada bahasa pemrograman MATLAB?

1.4. Tujuan Penulisan

Tujuan penulis menyusun tugas akhir ini adalah sebagai berikut :

1. Mengkaji konsep matematis yang melandasi prosedur pertukaran kunci.
2. Mengkaji langkah-langkah yang digunakan untuk memperoleh sandi menggunakan protokol pertukaran kunci stickel atas semiring aljabar min plus.
3. Mengkaji proses perhitungan enkripsi dan dekripsi menggunakan sistem kriptografi simetris dengan sandi Vigenere.
4. Membuat algoritma perhitungan protokol pertukaran kunci atas semiring aljabar min plus dan perhitungan proses enkripsi serta dekripsi menggunakan Sandi Vigenere pada bahasa pemrograman MATLAB.

1.5. Manfaat Penelitian

Beberapa manfaat dari penelitian ini adalah sebagai berikut :

1. Memberikan solusi kepada kedua belah pihak untuk mendapatkan kunci rahasia yang sama.
2. Memberikan kemudahan dalam perhitungan protokol pertukaran kunci atas semiring aljabar min plus dan perhitungan proses enkripsi serta dekripsi menggunakan Sandi Vigenere dengan bahasa pemrograman MATLAB.

3. Sebagai dasar untuk peneliti selanjutnya dalam mengembangkan protokol pertukaran kunci.

1.6. Tinjauan Pustaka

Referensi utama dalam penyusunan tugas akhir ini adalah jurnal dari Dima Grigoriev dan Vladimir Shpilrain (2012) yang berjudul *Tropical Cryptography*. Jurnal tersebut menjelaskan tentang protokol pertukaran kunci dengan skema stickel atas semiring non-komutatif. Contoh semiring komutatif yang digunakan adalah aljabar min-plus. Protokol ini menggunakan penjumlahan dan perkalian atas aljabar min plus.

Peneliti lain yang telah meneliti terkait protokol pertukaran kunci Stickel yaitu Musthofa dan Dwi Lestari (2014) yang berjudul *Metode perjanjian password berdasarkan operasi matriks atas Aljabar Min-Plus untuk keamanan pengiriman informasi rahasia*. Musthofa dan Dewi Lestari menggunakan semiring aljabar min plus, sama seperti penelitian sebelumnya. Perbedaan antara penelitian Dima Grigoriev dan Vladimir Shpilrain dengan Musthofa dan Dwi Lestari terletak pada penggunaan polinomial pada protokol pertukaran kunci. Penulis menggunakan polinomial pada protokol pertukaran kunci dan menambahkan enkripsi dan dekripsi pada penelitian ini.

Perbedaan dan persamaan penelitian yang dilakukan penulis dengan penelitian sebelumnya dapat dilihat pada tabel berikut.

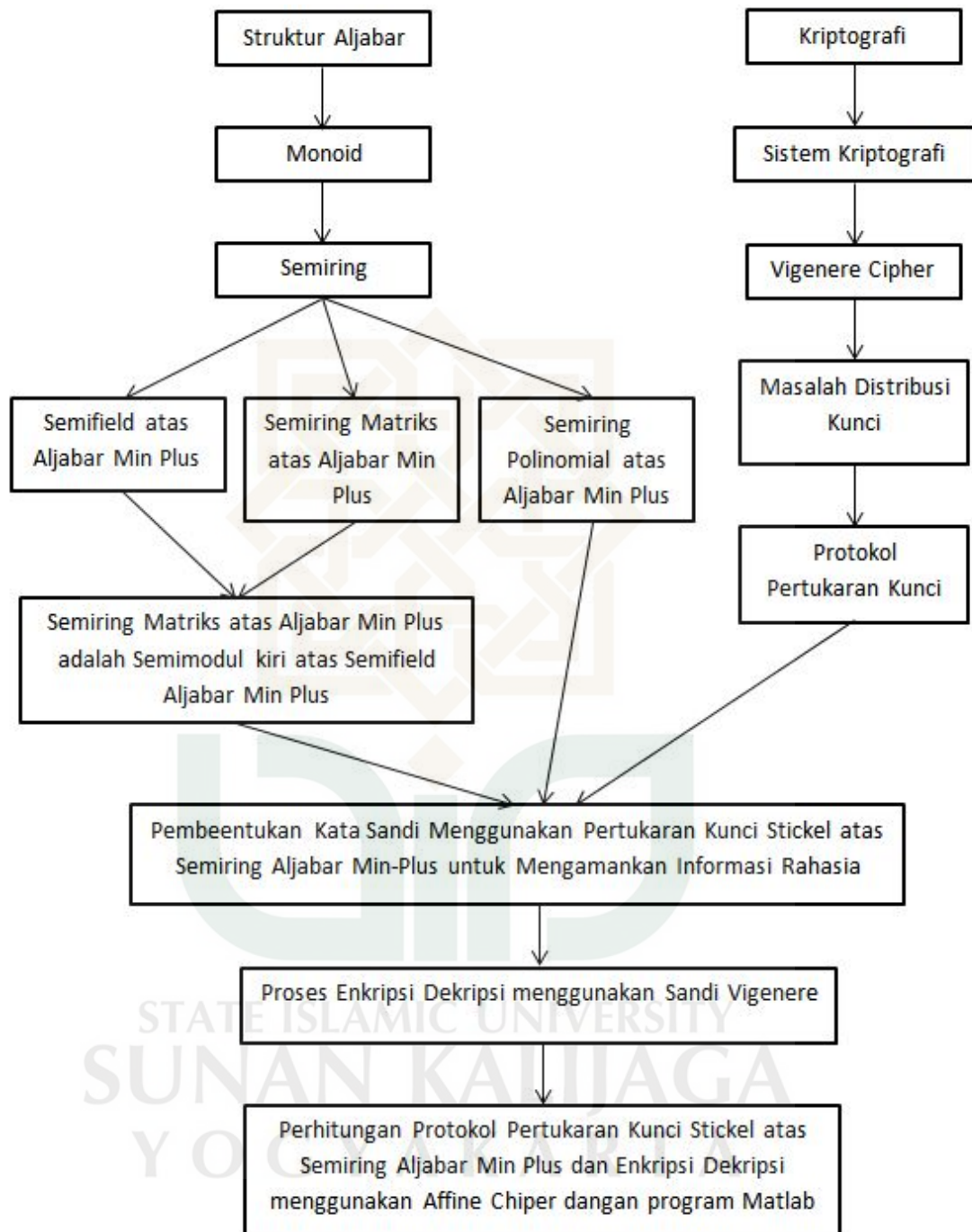
Tabel 1.1 Tinjauan Pustaka

No	Nama Peneliti	Judul Penelitian	Persamaan	Perbedaan
1.	Dima Grigoriev dan Vladimir Shpilrain (2012)	<i>Tropical Cryptography</i>	Menggunakan protokol pertukaran kunci Stickel	Protokol pertukaran kunci Stickel atas Aljabar Min Plus dengan Polinomial
2.	Musthofa dan Dwi Lestari (2014)	<i>Metode perjanjian password berdasarkan operasi matriks atas Aljabar Min-Plus untuk keamanan pengiriman informasi rahasia</i>	Menggunakan protokol pertukaran kunci Stickel	Protokol pertukaran kunci Stickel atas Aljabar Min Plus
3.	Mahendra Fakhrol Fathan (2017)	<i>Pembentukan Kata Sandi Menggunakan Pertukaran Kunci Stickel Atas Aljabar Min-Plus Untuk Mengamankan Informasi Rahasia</i>	Menggunakan protokol pertukaran kunci Stickel	Protokol pertukaran kunci Stickel atas Aljabar Min Plus dengan Polinomial serta pangkat

1.7. Metode Penelitian

Metode yang digunakan dalam penyusunan tugas akhir ini adalah metode studi literatur. Penelitian ini dilakukan dengan cara membahas dan menjabarkan teorema-teorema dan materi yang bersumber pada buku, jurnal maupun catatan kuliah. Secara umum pembahasan dalam penelitian ini terdiri dari dua bagian, yaitu kriptografi dan struktur aljabar.

Pembahasan kriptografi diawali dari sistem kriptografi simetris yaitu sandi Vigenere. Permasalahan distribusi dari sistem kriptografi simetris adalah masalah distribusi kunci antara kedua belah pihak. Solusi untuk permasalahan distribusi kunci yaitu protokol pertukaran kunci. Sedangkan pembahasan mengenai struktur aljabar diawali dari pembahasan operasi biner yang mendukung pembahasan mengenai semigrup dan semiring. Semiring kemudian membentuk struktur aljabar baru yaitu, semifield atas aljabar min plus, semiring matriks atas aljabar min plus, dan semiring polinomial atas aljabar min plus. Semifield atas aljabar min plus dan semiring matriks atas aljabar min plus kemudian membentuk sebuah semimodul. Berdasarkan penjelasan tersebut, maka langkah terakhir dalam melakukan penelitian ini adalah menyelesaikan masalah distribusi kunci dengan protokol pertukaran kunci Stickel atas aljabar min plus. Selanjutnya diberikan proses perhitungan enkripsi dan dekripsi menggunakan sandi Vigenere. Langkah-langkah penulis dalam menyusun tugas akhir ini dapat dijelaskan pada diagram berikut :

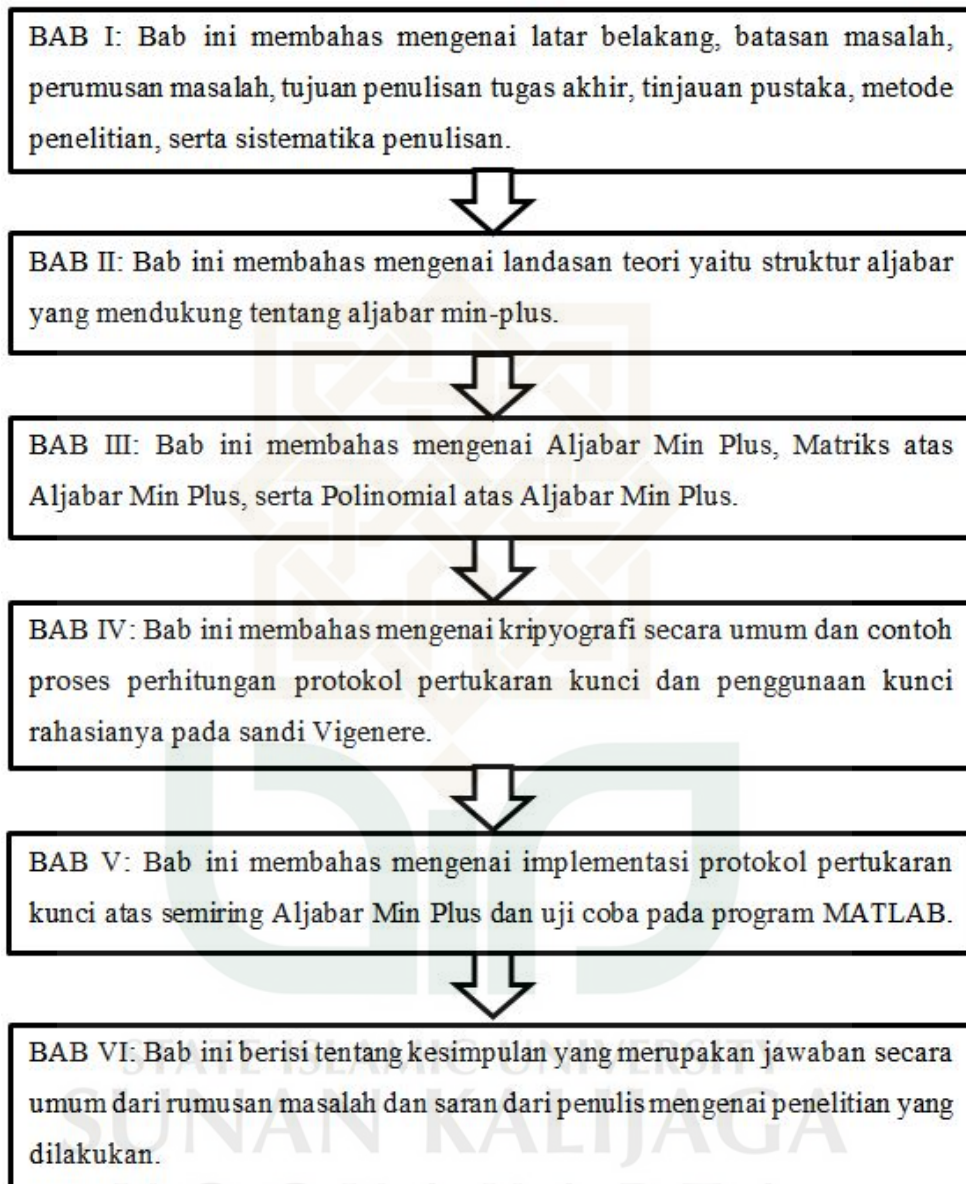


Gambar 1.1 Alur Penelitian

1.8. Sistematika Penulisan

Dalam penyusunan tugas akhir ini, penulis membaginya ke dalam enam bab yang disusun secara runtun dan sistematis dengan rincian masing-masing bab dije-

laskan secara umum oleh penulis yaitu :



Gambar 1.2 Alur Sistematika Penelitian

BAB VI

PENUTUP

Berdasarkan pembahasan mengenai pembuatan sandi menggunakan protokol pertukaran kunci Stickel atas aljabar min-plus, maka dapat diambil beberapa kesimpulan dan saran sebagai berikut :

6.1. Kesimpulan

Kesimpulan yang dapat diambil penulis setelah menyelesaikan pembuatan tugas akhir ini adalah :

1. Prosedur pembuatan sandi menggunakan protokol pertukaran kunci Stickel atas aljabar min-plus untuk mengamankan informasi rahasia ini diperlukan pemahaman tentang kriptografi dan dasar struktur aljabar seperti semigrup, semiring, semifield, serta semimodul.
2. Kunci yang digunakan dalam penelitian ini adalah matriks atas aljabar min-plus dengan strukturnya yaitu semiring non komutatif ($\mathbb{Z}_{min}^{n \times n}$). Adapun skema yang digunakan adalah protokol pertukaran kunci atas aljabar min-plus dengan pembuatan kunci rahasianya adalah, Alice dan Bob menyepakati kunci publik $A, B \in \mathbb{Z}_{min}^{n \times n}$ dengan $A \otimes B \neq B \otimes A$. Kemudian Alice memilih secara rahasia $p_1(x), p_2(x) \in \mathbb{Z}_{min}[x]$ serta $m, n \in \mathbb{N}$ dan Bob memilih secara rahasia $q_1(x), q_2(x) \in \mathbb{Z}_{min}[x]$ serta $r, s \in \mathbb{N}$. Selanjutnya Alice menghitung kunci publiknya $P = p_1(x)^m \otimes p_2(x)^n$ dan mengirimkannya kepada Bob, begitu juga Bob menghitung kunci publiknya $Q = q_1(x)^r \otimes q_2(x)^s$ dan mengirimkannya kepada Alice. Selanjutnya Alice dan Bob menghitung kunci

rahasiannya yaitu $K_1 = p_1(x)^m \otimes Q \otimes p_2(x)^n$ dan $K_2 = q_1(x)^r \otimes P \otimes q_2(x)^s$, diperoleh $K_1 = K_2$.

3. Kunci rahasia yang sudah diperoleh kemudian digunakan untuk menyandikan pesan rahasia yang akan dikirimkan melalui jalur yang tidak aman, penyandian menggunakan sandi Vigenere. Adapun alurnya yaitu, Alice dan Bob menyepakati kunci yang sama yaitu berupa matriks $\mathcal{K} \in M_n(\mathbb{Z}_{256})$. Selanjutnya, plainteks yang akan dikirim diubah menjadi angka sesuai dengan tabel ASCII. Plainteks dibagi menjadi masing masing n huruf dan dikonstruksikan menjadi matriks $n \times n$. Setelah itu Alice melakukan proses enkripsi, yaitu $e_k(x) = (x+k) \bmod 256$ kemudian dikirimkan kepada Bob. Setelah menerima chiperteks, Bob mendekripsi chiperteks yaitu $d_k(y) = (y-k) \bmod 256$ dan mendapatkan plainteksnya.
4. Dalam mempermudah dan mempercepat perhitungan protokol pertukaran kunci Stickel atas aljabar min-plus dan proses enkripsi dekripsi yang cukup rumit dan dibutuhkan ketelitian, dibuat pemrograman dengan MATLAB. Pemrograman ini menggunakan GUI (interface) agar lebih mudah untuk mengedit inputannya. *Script* yang digunakan seperti pada lampiran dan dibahas pada bab V. Program ini sangat memudahkan dan meminimalkan error dari kedua belah pihak untuk menghitung kunci rahasia dan melakukan enkripsi serta dekripsi dengan sandi Vigenere.

6.2. Saran

Setelah membahas dan mengimplementasikan sistem kriptografi Elatrash, penulis ingin menyampaikan beberapa saran.

1. Protokol pertukaran kunci merupakan metode untuk menyelesaikan masalah

kunci, diharapkan ada penelitian selanjutnya yang membahas tentang protokol pertukaran kunci dengan keamanan yang lebih tinggi dan lebih efektif.

2. Proses enkripsi dan dekripsi pada penelitian ini menggunakan sandi Vigenere dengan operasi biasa, diharapkan kepada peneliti selanjutnya untuk mengembangkan proses enkripsi dan dekripsi dengan memanfaatkan operasi aljabar min-plus.
3. Program yang peneliti buat menggunakan MATLAB terbatas hanya maksimal polinomial pangkat 3 saja. Diharapkan kepada peneliti selanjutnya yang berminat meneliti lebih lanjut tentang masalah ini untuk mengembangkan program dengan pangkat polinomialnya diinputkan sendiri oleh *user*, serta menyempurnakan program ini.

DAFTAR PUSTAKA

- Buchmann, J. A., 2000, *Introduction to Cryptography*, Springer-Verlag New York, Inc., USA.
- Farlow, Kasie G, 2009, *Max-Plus Algebra*, Masters Thesis Virginia Polytechnic Institute and State University, Blacksburg, VA.
- Butkovic, Peter, 2010, *Max Linear System: Theory and Algorithm*, Springer, New York.
- Grigoriev, D., dan Shpilrain, V., *Tropical Cryptography*, Federal Agency of the Science and Innovations of Russia, State Contract No. 02.740.11.5192.
- Malik, D.S., Modershon, Jhon N, dan Sen, M.K., *An Indtroduction to Abstract Algebra*, Creighton University, USA.
- Menezes, Oorschot, dan Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, Inc., USA.
- Subiono, 2015, *Aljabar Min-Max Plus dan Terapannya*, Institut Teknologi Sepuluh November, Surabaya.
- Myasnikov, Shpilrain, dan Ushakov, 2008, *Grup Based Cryptography*, Birkhäuser Verlag, Berlin.
- Musthofa, dan Dwi Lestari, 2013, *Metode Perjanjian Password Berdasarkan Operasi Matriks atas Aljabar Min-Plus untuk Keamanan Pengiriman Informasi Rahaasia*, Penelitian, FMIPA, UNY.
- Rudhito MA, 2016, *Aljabar Max-Plus dan Penerapannya*, Universitas Sanata Dharma, Yogyakarta.
- Schneier, Bruce, 1996, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*, Wiley Computer Publishing, John Wiley and Sons, Inc, USA.
- Shor, Peter W., 1997, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, Society for Industrial and Applied Mathematics Philadelphia, PA, USA.

LAMPIRAN A

SKRIP PROGRAM MATLAB PEMBENTUKAN KATA SANDI MENGUNAKAN PERTUKARAN KUNCI STICKEL ATAS ALJABAR MIN-PLUS

```
1 function varargout = pertukaran_kunci(varargin)
2 % PERTUKARAN_KUNCI M-file for pertukaran_kunci.fig
3 %     PERTUKARAN_KUNCI, by itself, creates a new
4 %     PERTUKARAN_KUNCI or raises the existing
5 %     singleton*.
6 %     H = PERTUKARAN_KUNCI returns the handle to a new
7 %     PERTUKARAN_KUNCI or the handle to
8 %     the existing singleton*.
9 %     PERTUKARAN_KUNCI('CALLBACK', hObject, eventData, handles
10 %     ,...) calls the local
11 %     function named CALLBACK in PERTUKARAN_KUNCI.M with the
12 %     given input arguments.
13 %     PERTUKARAN_KUNCI('Property','Value',...) creates a new
14 %     PERTUKARAN_KUNCI or raises the
15 %     existing singleton*. Starting from the left, property
16 %     value pairs are
17 %     applied to the GUI before
18 %     pertukaran_kunci_OpeningFunction gets called. An
```

```

15 % unrecognized property name or invalid value makes
    property application
16 % stop. All inputs are passed to
    pertukaran_kunci_OpeningFcn via varargin.
17 %
18 % *See GUI Options on GUIDE's Tools menu. Choose "GUI
    allows only one
19 % instance to run (singleton)".
20 %
21 % See also: GUIDE, GUIDATA, GUIHANDLES
22
23 % Edit the above text to modify the response to help
    pertukaran_kunci
24
25 % Last Modified by GUIDE v2.5 12-May-2017 20:58:40
26
27 % Begin initialization code - DO NOT EDIT
28 gui_Singleton = 1;
29 gui_State = struct('gui_Name', mfilename, ...
30                   'gui_Singleton', gui_Singleton, ...
31                   'gui_OpeningFcn',
    @pertukaran_kunci_OpeningFcn, ...
32                   'gui_OutputFcn', @pertukaran_kunci_OutputFcn
    , ...
33                   'gui_LayoutFcn', [] , ...
34                   'gui_Callback', []);
35 if nargin && ischar(varargin{1})
36     gui_State.gui_Callback = str2func(varargin{1});
37 end
38
39 if nargin

```

```
40     [varargout{1:nargout}] = gui_mainfcn(gui_State , varargin{:})
        ;
41 else
42     gui_mainfcn(gui_State , varargin{:});
43 end
44 % End initialization code – DO NOT EDIT
45
46
47 % — Executes just before pertukaran_kunci is made visible.
48 function pertukaran_kunci_OpeningFcn(hObject, eventdata, handles
        , varargin)
49 % This function has no output args, see OutputFcn.
50 % hObject    handle to figure
51 % eventdata  reserved – to be defined in a future version of
        MATLAB
52 % handles    structure with handles and user data (see GUIDATA)
53 % varargin   command line arguments to pertukaran_kunci (see
        VARARGIN)
54
55 % Choose default command line output for pertukaran_kunci
56 handles.output = hObject;
57
58 % Update handles structure
59 guidata(hObject, handles);
60
61 % UIWAIT makes pertukaran_kunci wait for user response (see
        UIRESUME)
62 % uiwait(handles.figure1);
63
64
```



```
65 % — Outputs from this function are returned to the command
    line .
66 function varargout = pertukaran_kunci_OutputFcn(hObject ,
    eventdata , handles)
67 % varargout cell array for returning output args (see VARARGOUT
    );
68 % hObject handle to figure
69 % eventdata reserved – to be defined in a future version of
    MATLAB
70 % handles structure with handles and user data (see GUIDATA)
71
72 % Get default command line output from handles structure
73 varargout{1} = handles.output;
74
75
76
77 function X_Callback(hObject , eventdata , handles)
78 % hObject handle to X (see GCBO)
79 % eventdata reserved – to be defined in a future version of
    MATLAB
80 % handles structure with handles and user data (see GUIDATA)
81
82 % Hints: get(hObject,'String') returns contents of X as text
83 % str2double(get(hObject,'String')) returns contents of X
    as a double
84
85
86 % — Executes during object creation , after setting all
    properties .
87 function X_CreateFcn(hObject , eventdata , handles)
88 % hObject handle to X (see GCBO)
```

```
89 % eventdata reserved – to be defined in a future version of
    MATLAB
90 % handles empty – handles not created until after all
    CreateFcns called
91
92 % Hint: edit controls usually have a white background on Windows
    .
93 % See ISPC and COMPUTER.
94 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
    defaultUicontrolBackgroundColor'))
95     set(hObject,'BackgroundColor','white');
96 end
97
98
99
100 function Y_Callback(hObject, eventdata, handles)
101 % hObject handle to Y (see GCBO)
102 % eventdata reserved – to be defined in a future version of
    MATLAB
103 % handles structure with handles and user data (see GUIDATA)
104
105 % Hints: get(hObject,'String') returns contents of Y as text
106 % str2double(get(hObject,'String')) returns contents of Y
    as a double
107
108
109 % — Executes during object creation, after setting all
    properties.
110 function Y_CreateFcn(hObject, eventdata, handles)
111 % hObject handle to Y (see GCBO)
```

```

112 % eventdata reserved – to be defined in a future version of
      MATLAB
113 % handles empty – handles not created until after all
      CreateFcns called
114
115 % Hint: edit controls usually have a white background on Windows
      .
116 % See ISPC and COMPUTER.
117 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
118     set(hObject,'BackgroundColor','white');
119 end
120
121
122
123 function m_Callback(hObject, eventdata, handles)
124 % hObject handle to m (see GCBO)
125 % eventdata reserved – to be defined in a future version of
      MATLAB
126 % handles structure with handles and user data (see GUIDATA)
127
128 % Hints: get(hObject,'String') returns contents of m as text
129 % str2double(get(hObject,'String')) returns contents of m
      as a double
130
131
132 % — Executes during object creation, after setting all
      properties.
133 function m_CreateFcn(hObject, eventdata, handles)
134 % hObject handle to m (see GCBO)

```

```
135 % eventdata reserved – to be defined in a future version of
      MATLAB
136 % handles empty – handles not created until after all
      CreateFcns called
137
138 % Hint: edit controls usually have a white background on Windows
      .
139 % See ISPC and COMPUTER.
140 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
141     set(hObject,'BackgroundColor','white');
142 end
143
144
145
146 function n_Callback(hObject, eventdata, handles)
147 % hObject handle to n (see GCBO)
148 % eventdata reserved – to be defined in a future version of
      MATLAB
149 % handles structure with handles and user data (see GUIDATA)
150
151 % Hints: get(hObject,'String') returns contents of n as text
152 % str2double(get(hObject,'String')) returns contents of n
      as a double
153
154
155 % — Executes during object creation, after setting all
      properties.
156 function n_CreateFcn(hObject, eventdata, handles)
157 % hObject handle to n (see GCBO)
```

```
158 % eventdata reserved – to be defined in a future version of
      MATLAB
159 % handles empty – handles not created until after all
      CreateFcns called
160
161 % Hint: edit controls usually have a white background on Windows
      .
162 % See ISPC and COMPUTER.
163 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
164     set(hObject,'BackgroundColor','white');
165 end
166
167
168
169 function a1_Callback(hObject, eventdata, handles)
170 % hObject handle to a1 (see GCBO)
171 % eventdata reserved – to be defined in a future version of
      MATLAB
172 % handles structure with handles and user data (see GUIDATA)
173
174 % Hints: get(hObject,'String') returns contents of a1 as text
175 % str2double(get(hObject,'String')) returns contents of
      a1 as a double
176
177
178 % — Executes during object creation, after setting all
      properties.
179 function a1_CreateFcn(hObject, eventdata, handles)
180 % hObject handle to a1 (see GCBO)
```

```
181 % eventdata reserved – to be defined in a future version of
    MATLAB
182 % handles empty – handles not created until after all
    CreateFcns called
183
184 % Hint: edit controls usually have a white background on Windows
    .
185 % See ISPC and COMPUTER.
186 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
    defaultUicontrolBackgroundColor'))
187     set(hObject,'BackgroundColor','white');
188 end
189
190
191
192 function b1_Callback(hObject, eventdata, handles)
193 % hObject handle to b1 (see GCBO)
194 % eventdata reserved – to be defined in a future version of
    MATLAB
195 % handles structure with handles and user data (see GUIDATA)
196
197 % Hints: get(hObject,'String') returns contents of b1 as text
198 % str2double(get(hObject,'String')) returns contents of
    b1 as a double
199
200
201 % — Executes during object creation, after setting all
    properties.
202 function b1_CreateFcn(hObject, eventdata, handles)
203 % hObject handle to b1 (see GCBO)
```

```
204 % eventdata reserved – to be defined in a future version of
      MATLAB
205 % handles empty – handles not created until after all
      CreateFcns called
206
207 % Hint: edit controls usually have a white background on Windows
      .
208 % See ISPC and COMPUTER.
209 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
210     set(hObject,'BackgroundColor','white');
211 end
212
213
214
215 function c1_Callback(hObject, eventdata, handles)
216 % hObject handle to c1 (see GCBO)
217 % eventdata reserved – to be defined in a future version of
      MATLAB
218 % handles structure with handles and user data (see GUIDATA)
219
220 % Hints: get(hObject,'String') returns contents of c1 as text
221 % str2double(get(hObject,'String')) returns contents of
      c1 as a double
222
223
224 % — Executes during object creation, after setting all
      properties.
225 function c1_CreateFcn(hObject, eventdata, handles)
226 % hObject handle to c1 (see GCBO)
```

```
227 % eventdata reserved – to be defined in a future version of
      MATLAB
228 % handles empty – handles not created until after all
      CreateFcns called
229
230 % Hint: edit controls usually have a white background on Windows
      .
231 % See ISPC and COMPUTER.
232 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
233     set(hObject,'BackgroundColor','white');
234 end
235
236
237
238 function d1_Callback(hObject, eventdata, handles)
239 % hObject handle to d1 (see GCBO)
240 % eventdata reserved – to be defined in a future version of
      MATLAB
241 % handles structure with handles and user data (see GUIDATA)
242
243 % Hints: get(hObject,'String') returns contents of d1 as text
244 % str2double(get(hObject,'String')) returns contents of
      d1 as a double
245
246
247 % — Executes during object creation, after setting all
      properties.
248 function d1_CreateFcn(hObject, eventdata, handles)
249 % hObject handle to d1 (see GCBO)
```



```
250 % eventdata reserved – to be defined in a future version of
      MATLAB
251 % handles empty – handles not created until after all
      CreateFcns called
252
253 % Hint: edit controls usually have a white background on Windows
      .
254 % See ISPC and COMPUTER.
255 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
256     set(hObject,'BackgroundColor','white');
257 end
258
259
260
261 function a2_Callback(hObject, eventdata, handles)
262 % hObject handle to a2 (see GCBO)
263 % eventdata reserved – to be defined in a future version of
      MATLAB
264 % handles structure with handles and user data (see GUIDATA)
265
266 % Hints: get(hObject,'String') returns contents of a2 as text
267 % str2double(get(hObject,'String')) returns contents of
      a2 as a double
268
269
270 % — Executes during object creation, after setting all
      properties.
271 function a2_CreateFcn(hObject, eventdata, handles)
272 % hObject handle to a2 (see GCBO)
```

```
273 % eventdata reserved – to be defined in a future version of
      MATLAB
274 % handles empty – handles not created until after all
      CreateFcns called
275
276 % Hint: edit controls usually have a white background on Windows
      .
277 % See ISPC and COMPUTER.
278 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
279     set(hObject,'BackgroundColor','white');
280 end
281
282
283
284 function b2_Callback(hObject, eventdata, handles)
285 % hObject handle to b2 (see GCBO)
286 % eventdata reserved – to be defined in a future version of
      MATLAB
287 % handles structure with handles and user data (see GUIDATA)
288
289 % Hints: get(hObject,'String') returns contents of b2 as text
290 % str2double(get(hObject,'String')) returns contents of
      b2 as a double
291
292
293 % — Executes during object creation, after setting all
      properties.
294 function b2_CreateFcn(hObject, eventdata, handles)
295 % hObject handle to b2 (see GCBO)
```

```
296 % eventdata reserved – to be defined in a future version of
      MATLAB
297 % handles empty – handles not created until after all
      CreateFcns called
298
299 % Hint: edit controls usually have a white background on Windows
      .
300 % See ISPC and COMPUTER.
301 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
302     set(hObject,'BackgroundColor','white');
303 end
304
305
306
307 function c2_Callback(hObject, eventdata, handles)
308 % hObject handle to c2 (see GCBO)
309 % eventdata reserved – to be defined in a future version of
      MATLAB
310 % handles structure with handles and user data (see GUIDATA)
311
312 % Hints: get(hObject,'String') returns contents of c2 as text
313 % str2double(get(hObject,'String')) returns contents of
      c2 as a double
314
315
316 % — Executes during object creation, after setting all
      properties.
317 function c2_CreateFcn(hObject, eventdata, handles)
318 % hObject handle to c2 (see GCBO)
```

```
319 % eventdata reserved – to be defined in a future version of
      MATLAB
320 % handles empty – handles not created until after all
      CreateFcns called
321
322 % Hint: edit controls usually have a white background on Windows
      .
323 % See ISPC and COMPUTER.
324 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
325     set(hObject,'BackgroundColor','white');
326 end
327
328
329
330 function d2_Callback(hObject, eventdata, handles)
331 % hObject handle to d2 (see GCBO)
332 % eventdata reserved – to be defined in a future version of
      MATLAB
333 % handles structure with handles and user data (see GUIDATA)
334
335 % Hints: get(hObject,'String') returns contents of d2 as text
336 % str2double(get(hObject,'String')) returns contents of
      d2 as a double
337
338
339 % — Executes during object creation, after setting all
      properties.
340 function d2_CreateFcn(hObject, eventdata, handles)
341 % hObject handle to d2 (see GCBO)
```

```
342 % eventdata reserved – to be defined in a future version of
      MATLAB
343 % handles empty – handles not created until after all
      CreateFcns called
344
345 % Hint: edit controls usually have a white background on Windows
      .
346 % See ISPC and COMPUTER.
347 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
348     set(hObject,'BackgroundColor','white');
349 end
350
351
352
353 function V_Callback(hObject, eventdata, handles)
354 % hObject handle to V (see GCBO)
355 % eventdata reserved – to be defined in a future version of
      MATLAB
356 % handles structure with handles and user data (see GUIDATA)
357
358 % Hints: get(hObject,'String') returns contents of V as text
359 % str2double(get(hObject,'String')) returns contents of V
      as a double
360
361
362 % — Executes during object creation, after setting all
      properties.
363 function V_CreateFcn(hObject, eventdata, handles)
364 % hObject handle to V (see GCBO)
```

```
365 % eventdata reserved – to be defined in a future version of
      MATLAB
366 % handles empty – handles not created until after all
      CreateFens called
367
368 % Hint: edit controls usually have a white background on Windows
      .
369 % See ISPC and COMPUTER.
370 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
      defaultUicontrolBackgroundColor'))
371     set(hObject,'BackgroundColor','white');
372 end
373
374
375 % — Executes on button press in pushbutton1.
376 function pushbutton1_Callback(hObject, eventdata, handles)
377 % hObject handle to pushbutton1 (see GCBO)
378 % eventdata reserved – to be defined in a future version of
      MATLAB
379 % handles structure with handles and user data (see GUIDATA)
380 X=str2num(get(handles.X,'string'));
381 Y=str2num(get(handles.Y,'string'));
382 a1=str2num(get(handles.a1,'string'));
383 b1=str2num(get(handles.b1,'string'));
384 c1=str2num(get(handles.c1,'string'));
385 d1=str2num(get(handles.d1,'string'));
386 a2=str2num(get(handles.a2,'string'));
387 b2=str2num(get(handles.b2,'string'));
388 c2=str2num(get(handles.c2,'string'));
389 d2=str2num(get(handles.d2,'string'));
390 m=str2num(get(handles.m,'string'));
```

```

391 n=str2num(get(handles.n,'string'));
392
393 [p,q]=size(X);
394 [r,s]=size(Y);
395
396 if p==q
397     E1=inf*ones(p,q); E2=inf*ones(p,q);
398     F1=inf*ones(p,q); F2=inf*ones(p,q);
399     G1=inf*ones(p,q); G2=inf*ones(p,q);
400     V1=inf*ones(p,q); V2=inf*ones(p,q);
401     for i=1:p
402         for j=1:q
403             E1(i,j)=min(E1(i,j),(X(i,j)));
404             E2(i,j)=min(E2(i,j),(Y(i,j)));
405             for k=1:q
406                 F1(i,j)=(min(F1(i,j),(X(i,k)+X(k,j))));
407                 F2(i,j)=(min(F2(i,j),(Y(i,k)+Y(k,j))));
408                 for l=1:q
409                     V1(i,l)=(min(V1(i,l),(X(i,k)+X(k,j)+X(j,l)))
410                                 );
411                     V2(i,l)=(min(V2(i,l),(Y(i,k)+Y(k,j)+Y(j,l)))
412                                 );
413                 end
414                 if i==j
415                     G1(i,j)=d1;
416                     G2(i,j)=d2;
417                 end
418             end
419         end
420     end

```

```

420 V1=ones(p,q)*a1+V1;
421 F1=ones(p,q)*b1+F1;
422 E1=ones(p,q)*c1+E1;
423 V2=ones(r,s)*a2+V2;
424 F2=ones(r,s)*b2+F2;
425 E2=ones(r,s)*c2+E2;
426
427 if q==p
428     H1=inf*ones(p,q);
429     H2=inf*ones(p,q);
430     for i=1:p
431         for j=1:q
432             H1(i,j)=min(H1(i,j),min(E1(i,j),min(F1(i,j),min(G1(i
433                 ,j),V1(i,j))))));
434             H2(i,j)=min(H2(i,j),min(E2(i,j),min(F2(i,j),min(G2(i
435                 ,j),V1(i,j))))));
436         end
437     end
438 end
439
440 D1=H1;
441 for l=1:m-1
442     l+1;
443     for i=1:p
444         for j=1:q
445             C1(i,j)=inf;
446             for k=1:q
447                 C1(i,j)=min(C1(i,j),H1(i,k)+D1(k,j));
448             end;
449         end;
450     end;
451 end;

```



```
449     D1=C1;
450 end
451 C1
452 D2=H2;
453 for l=1:n-1
454     l+1;
455     for i=1:p
456         for j=1:q
457             C2(i,j)=inf;
458             for k=1:q
459                 C2(i,j)=min(C2(i,j),H2(i,k)+D2(k,j));
460             end;
461         end;
462     end;
463     D2=C2;
464 end
465 C2
466
467 if q==p
468     U=inf*ones(p,q);
469     for i=1:p
470         for j=1:q
471             for k=1:q
472                 U(i,j)=min(U(i,j),(C1(i,k)+C2(k,j)));
473             end
474         end
475     end
476 end
477 disp('Diperoleh U=')
478 disp(num2str(U))
479
```

```

480 set(handles.hasil , 'string' , num2str(U));
481
482
483 % — Executes on button press in pushbutton2.
484 function pushbutton2_Callback(hObject , eventdata , handles)
485 % hObject     handle to pushbutton2 (see GCBO)
486 % eventdata   reserved – to be defined in a future version of
      MATLAB
487 % handles     structure with handles and user data (see GUIDATA)
488 V=str2num(get(handles.V, 'string'));
489 X=str2num(get(handles.X, 'string'));
490 Y=str2num(get(handles.Y, 'string'));
491 a1=str2num(get(handles.a1, 'string'));
492 b1=str2num(get(handles.b1, 'string'));
493 c1=str2num(get(handles.c1, 'string'));
494 d1=str2num(get(handles.d1, 'string'));
495 a2=str2num(get(handles.a2, 'string'));
496 b2=str2num(get(handles.b2, 'string'));
497 c2=str2num(get(handles.c2, 'string'));
498 d2=str2num(get(handles.d2, 'string'));
499 m=str2num(get(handles.m, 'string'));
500 n=str2num(get(handles.n, 'string'));
501
502 [q , r]= size (V) ;
503 [p , q]= size (X) ;
504 [r , s]= size (Y) ;
505
506
507 if p==q
508     E1=inf*ones(p,q) ; E2=inf*ones(p,q) ;
509     F1=inf*ones(p,q) ; F2=inf*ones(p,q) ;

```

```

510 G1=inf*ones(p,q); G2=inf*ones(p,q);
511 V1=inf*ones(p,q); V2=inf*ones(p,q);
512 for i=1:p
513     for j=1:q
514         E1(i,j)=min(E1(i,j),(X(i,j)));
515         E2(i,j)=min(E2(i,j),(Y(i,j)));
516         for k=1:q
517             F1(i,j)=(min(F1(i,j),(X(i,k)+X(k,j))));
518             F2(i,j)=(min(F2(i,j),(Y(i,k)+Y(k,j))));
519             for l=1:q
520                 V1(i,l)=(min(V1(i,l),(X(i,k)+X(k,j)+X(j,l)))
521                     );
522                 V2(i,l)=(min(V2(i,l),(Y(i,k)+Y(k,j)+Y(j,l)))
523                     );
524             end
525         end
526         if i==j
527             G1(i,j)=d1;
528             G2(i,j)=d2;
529         end
530     end
531 end
532 V1=ones(p,q)*a1+V1;
533 F1=ones(p,q)*b1+F1;
534 E1=ones(p,q)*c1+E1;
535 V2=ones(r,s)*a2+V2;
536 F2=ones(r,s)*b2+F2;
537 E2=ones(r,s)*c2+E2;
538

```

```

539 if q==p
540     H1=inf*ones(p,q);
541     H2=inf*ones(p,q);
542     for i=1:p
543         for j=1:q
544             H1(i,j)=min(H1(i,j),min(E1(i,j),min(F1(i,j),min(G1(i
                    ,j),V1(i,j))))));
545             H2(i,j)=min(H2(i,j),min(E2(i,j),min(F2(i,j),min(G2(i
                    ,j),V1(i,j))))));
546         end
547     end
548 end
549
550 D1=H1;
551 for l=1:m-1
552     l+1;
553     for i=1:p
554         for j=1:q
555             C1(i,j)=inf;
556             for k=1:q
557                 C1(i,j)=min(C1(i,j),H1(i,k)+D1(k,j));
558             end;
559         end;
560     end;
561     D1=C1;
562 end
563 C1
564 D2=H2;
565 for l=1:n-1
566     l+1;
567     for i=1:p

```

```

568     for j=1:q
569         C2(i,j)=inf;
570         for k=1:q
571             C2(i,j)=min(C2(i,j),H2(i,k)+D2(k,j));
572         end;
573     end;
574 end;
575 D2=C2;
576 end
577 C2
578
579 if q==r
580     K1=inf*ones(q,r);
581     for i=1:q
582         for j=1:r
583             for k=1:r
584                 for l=1:r
585                     K1(i,l)=min(K1(i,l),(D1(i,k)+V(k,j)+D2(j,l))
586                                     );
587                 end
588             end
589         end
590     end
591 disp('Diperoleh_K=');
592 disp(num2str(K1));
593 set(handles.rahasia,'string',num2str(K1));
594
595 % — Executes on button press in pushbutton3.
596 function pushbutton3_Callback(hObject, eventdata, handles)
597 % hObject    handle to pushbutton3 (see GCBO)

```

```
598 % eventdata reserved – to be defined in a future version of
      MATLAB
599 % handles structure with handles and user data (see GUIDATA)
600 run enkripsidekripsi;
```



LAMPIRAN B

SKRIP PROGRAM MATLAB ENKRIPSI DAN DEKRIPSI

```
1 function varargout = enkripsidekripsi(varargin)
2 % ENKRIPSIDEKRIPSI M-file for enkripsidekripsi.fig
3 %     ENKRIPSIDEKRIPSI, by itself, creates a new
4 %     ENKRIPSIDEKRIPSI or raises the existing
5 %     singleton*.
6 %     H = ENKRIPSIDEKRIPSI returns the handle to a new
7 %     ENKRIPSIDEKRIPSI or the handle to
8 %     the existing singleton*.
9 %     ENKRIPSIDEKRIPSI('CALLBACK', hObject, eventData, handles
10 %     ,...) calls the local
11 %     function named CALLBACK in ENKRIPSIDEKRIPSI.M with the
12 %     given input arguments.
13 %     ENKRIPSIDEKRIPSI('Property','Value',...) creates a new
14 %     ENKRIPSIDEKRIPSI or raises the
15 %     existing singleton*. Starting from the left, property
16 %     value pairs are
17 %     applied to the GUI before
18 %     enkripsidekripsi_OpeningFunction gets called. An
19 %     unrecognized property name or invalid value makes
20 %     property application
21 %     stop. All inputs are passed to
22 %     enkripsidekripsi_OpeningFcn via varargin.
```

```

17 %
18 %      *See GUI Options on GUIDE's Tools menu.  Choose "GUI
      allows only one
19 %      instance to run (singleton)".
20 %
21 % See also: GUIDE, GUIDATA, GUIHANDLES
22
23 % Edit the above text to modify the response to help
      enkripsidekripsi
24
25 % Last Modified by GUIDE v2.5 12-May-2017 21:46:33
26
27 % Begin initialization code - DO NOT EDIT
28 gui_Singleton = 1;
29 gui_State = struct('gui_Name',       mfilename, ...
30                  'gui_Singleton',   gui_Singleton, ...
31                  'gui_OpeningFcn',
                        @enkripsidekripsi_OpeningFcn, ...
32                  'gui_OutputFcn',   @enkripsidekripsi_OutputFcn
                        , ...
33                  'gui_LayoutFcn',   [], ...
34                  'gui_Callback',    []);
35 if nargin && ischar(varargin{1})
36     gui_State.gui_Callback = str2func(varargin{1});
37 end
38
39 if nargin
40     [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
      ;
41 else
42     gui_mainfcn(gui_State, varargin{:});

```



```
43 end
44 % End initialization code – DO NOT EDIT
45
46
47 % — Executes just before enkripsidekripsi is made visible.
48 function enkripsidekripsi_OpeningFcn(hObject, eventdata, handles
    , varargin)
49 % This function has no output args, see OutputFcn.
50 % hObject    handle to figure
51 % eventdata  reserved – to be defined in a future version of
    MATLAB
52 % handles    structure with handles and user data (see GUIDATA)
53 % varargin   command line arguments to enkripsidekripsi (see
    VARARGIN)
54
55 % Choose default command line output for enkripsidekripsi
56 handles.output = hObject;
57
58 % Update handles structure
59 guidata(hObject, handles);
60
61 % UIWAIT makes enkripsidekripsi wait for user response (see
    UIRESUME)
62 % uiwait(handles.figure1);
63
64
65 % — Outputs from this function are returned to the command
    line.
66 function varargout = enkripsidekripsi_OutputFcn(hObject,
    eventdata, handles)
```

```
67 % varargout    cell array for returning output args (see VARARGOUT
    );
68 % hObject     handle to figure
69 % eventdata   reserved – to be defined in a future version of
    MATLAB
70 % handles     structure with handles and user data (see GUIDATA)
71
72 % Get default command line output from handles structure
73 varargout{1} = handles.output;
74
75
76
77 function kunci_Callback(hObject, eventdata, handles)
78 % hObject     handle to kunci (see GCBO)
79 % eventdata   reserved – to be defined in a future version of
    MATLAB
80 % handles     structure with handles and user data (see GUIDATA)
81
82 % Hints: get(hObject, 'String') returns contents of kunci as text
83 %           str2double(get(hObject, 'String')) returns contents of
    kunci as a double
84
85
86 % — Executes during object creation, after setting all
    properties.
87 function kunci_CreateFcn(hObject, eventdata, handles)
88 % hObject     handle to kunci (see GCBO)
89 % eventdata   reserved – to be defined in a future version of
    MATLAB
90 % handles     empty – handles not created until after all
    CreateFcns called
```

```
91
92 % Hint: edit controls usually have a white background on Windows
93
94 % See ISPC and COMPUTER.
95 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
    defaultUicontrolBackgroundColor'))
96     set(hObject,'BackgroundColor','white');
97 end
98
99
100 function pesan_Callback(hObject, eventdata, handles)
101 % hObject handle to pesan (see GCBO)
102 % eventdata reserved - to be defined in a future version of
    MATLAB
103 % handles structure with handles and user data (see GUIDATA)
104
105 % Hints: get(hObject,'String') returns contents of pesan as text
106 % str2double(get(hObject,'String')) returns contents of
    pesan as a double
107
108 STATE ISLAMIC UNIVERSITY
109 SUNAN KALIJAGA
110 % — Executes during object creation, after setting all
    properties.
111
112 function pesan_CreateFcn(hObject, eventdata, handles)
113 % hObject handle to pesan (see GCBO)
114 % eventdata reserved - to be defined in a future version of
    MATLAB
115 % handles empty - handles not created until after all
    CreateFcns called
```

```
115 % Hint: edit controls usually have a white background on Windows
    .
116 %         See ISPC and COMPUTER.
117 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
    defaultUicontrolBackgroundColor'))
118     set(hObject,'BackgroundColor','white');
119 end
120
121
122
123 function hasil_Callback(hObject, eventdata, handles)
124 % hObject    handle to hasil (see GCBO)
125 % eventdata  reserved – to be defined in a future version of
    MATLAB
126 % handles    structure with handles and user data (see GUIDATA)
127
128 % Hints: get(hObject,'String') returns contents of hasil as text
129 %         str2double(get(hObject,'String')) returns contents of
    hasil as a double
130
131
132 % — Executes during object creation, after setting all
    properties.
133 function hasil_CreateFcn(hObject, eventdata, handles)
134 % hObject    handle to hasil (see GCBO)
135 % eventdata  reserved – to be defined in a future version of
    MATLAB
136 % handles    empty – handles not created until after all
    CreateFcns called
137
```

```
138 % Hint: edit controls usually have a white background on Windows
139
140 % See ISPC and COMPUTER.
141 if ispc && isequal(get(hObject,'BackgroundColor'), get(0,'
    defaultUicontrolBackgroundColor'))
142     set(hObject,'BackgroundColor','white');
143 end
144
145 % — Executes on button press in pushbutton1.
146 function pushbutton1_Callback(hObject, eventdata, handles)
147 % hObject handle to pushbutton1 (see GCBO)
148 % eventdata reserved - to be defined in a future version of
    MATLAB
149 % handles structure with handles and user data (see GUIDATA)
150 kunci=str2num(get(handles.kunci,'string'));
151 m=get(handles.pesan,'String');
152 [p,q]=size(kunci);
153 kunci=mod(kunci,256)
154 z=p*q;
155 n=length(m);
156 o=double(m);
157 B=[];
158 E=[];
159
160 if mod(n,z)~=0
161     for i=1:(z-mod(n,z))
162         o=[o 88];
163     end
164     n=length(o);
165 end
```

```

166
167 for i=1:p
168     A=kunci(i,:);
169     B=[B A];
170 end
171 k=1;
172 t=z;
173 for j=0:((n/z)-1)
174     C=o(k:t);
175     k=k+z;
176     t=t+z;
177     q=mod(C+B,256);
178     E=[E q];
179 end
180 teks=E;
181 set(handles.hasil,'string',num2str(teks))
182
183 % — Executes on button press in pushbutton2.
184 function pushbutton2_Callback(hObject, eventdata, handles)
185 % hObject    handle to pushbutton2 (see GCBO)
186 % eventdata  reserved - to be defined in a future version of
187 %           MATLAB
188 % handles    structure with handles and user data (see GUIDATA)
189 kunci=str2num(get(handles.kunci,'string'));
190 m=get(handles.pesan,'String');
191 [p,q]=size(kunci);
192 kunci=mod(kunci,256)
193 z=p*q;
194 n=length(m);
195 o1=char(str2num(m));
196 o=double(o1);

```

```
196 B=[];
197 E=[];
198
199 if mod(n,z)~=0
200     for i=1:(z-mod(n,z))
201         o=[o 88];
202     end
203     n=length(o);
204 end
205
206 for i=1:p
207     A=kunci(i,:);
208     B=[B A];
209 end
210 k=1;
211 t=z;
212 for j=0:((n/z)-1)
213     C=o(k:t);
214     k=k+z;
215     t=t+z;
216     q=mod(C-B,256);
217     D=char(q);
218     E=[E D];
219 end
220 teks=E;
221 set(handles.hasil,'string',teks)
```

LAMPIRAN C

TABEL KODE ASCII 1

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	\$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(72	48	H	104	68	h
9	09	Horizontal tab	41	29)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	
29	1D	Group separator	61	3D	=	93	5D]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

LAMPIRAN D

TABEL KODE ASCII 2

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	ƒ	224	E0	α
129	81	ü	161	A1	í	193	C1	⊥	225	E1	β
130	82	é	162	A2	ó	194	C2	⌈	226	E2	Γ
131	83	á	163	A3	ú	195	C3	⌋	227	E3	π
132	84	ä	164	A4	ñ	196	C4	—	228	E4	Σ
133	85	à	165	A5	Ñ	197	C5	†	229	E5	σ
134	86	ã	166	A6	ª	198	C6	‡	230	E6	μ
135	87	ç	167	A7	º	199	C7	‡	231	E7	ι
136	88	ê	168	A8	¿	200	C8	ℓ	232	E8	Φ
137	89	ë	169	A9	ƒ	201	C9	ℓ	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	⊥	234	EA	Ω
139	8B	ì	171	AB	½	203	CB	⌈	235	EB	ϛ
140	8C	í	172	AC	¼	204	CC	‡	236	EC	∞
141	8D	î	173	AD	¡	205	CD	=	237	ED	∞
142	8E	Ë	174	AE	«	206	CE	‡	238	EE	ε
143	8F	Ä	175	AF	»	207	CF	⊥	239	EF	∩
144	90	É	176	B0	⋯	208	D0	⊥	240	FO	≡
145	91	æ	177	B1	⋮	209	D1	⌈	241	F1	±
146	92	Æ	178	B2	⋮	210	D2	⌈	242	F2	≥
147	93	ó	179	B3		211	D3	ℓ	243	F3	≤
148	94	ö	180	B4	†	212	D4	ℓ	244	F4	[
149	95	ò	181	B5	‡	213	D5	ℓ	245	F5]
150	96	ù	182	B6	‡	214	D6	⌈	246	F6	÷
151	97	û	183	B7	⌈	215	D7	‡	247	F7	≈
152	98	ÿ	184	B8	‡	216	D8	‡	248	F8	°
153	99	ÿ	185	B9	‡	217	D9	⌋	249	F9	•
154	9A	Û	186	BA		218	DA	ƒ	250	FA	·
155	9B	ø	187	BB	⌈	219	DB	■	251	FB	√
156	9C	£	188	BC	⌋	220	DC	■	252	FC	π
157	9D	¥	189	BD	⌋	221	DD	■	253	FD	z
158	9E	ℳ	190	BE	⌋	222	DE	■	254	FE	■
159	9F	f	191	BF	⌋	223	DF	■	255	FF	□

DAFTAR RIWAYAT HIDUP

Nama : Mahendra Fakhrol Fathan

Tempat tanggal lahir : Klaten, 13 Juni 1995

Alamat : Tegalmulyo, Gergunung, Klaten Utara, Klaten

Hp : 089522826255

Fakultas/Program Studi : Sains dan Teknologi / Matematika

Alamat Email : mahendrafathan@gmail.com

Riwayat Pendidikan : TK PEMBINA (1999 – 2001)

SD Negeri 1 Gergunung (2001 – 2007)

SMP Negeri 1 Ngawen (2007 – 2010)

SMA Negeri 3 Klaten (2010 – 2013)

UIN Sunan Kalijaga (2013 – 2017)



STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA