SKRIPSI

ANALISIS KOMPARASI ALGORITMA KRIPTOGRAFI ANTARA METODE DES (DATA ENCRYPTION SYSTEM) DAN AES (ADVANCED ENCRYPTION SYSTEM)

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik Informatika

Disusun Oleh :

EKO PUJI LAKSONO

09650003

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2014

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

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1846/2014

Skripsi/Tugas Akhir dengan judul	:	Analisis Komparasi Algoritma Kriptografi Antara Metode DES (Data Encryption System) dan AES (Advanced Encryption System)

Yang dipersiapkan dan disusun oleh	:	
Nama	:	Eko Puji Laksono
NIM	:	09650003
Telah dimunaqasyahkan pada	:	Jum'at, 20 Juni 2014
Nilai Munaqasyah	:	A / B

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

TIM MUNAQASYAH :

Ketua Sidang

Arief Ikhwan W, M.Cs
NIP.

Penguji I

M. Mustakim, M.T
NIP.19790331 1 00501 1 004

Penguji II

Agus Mulyanto, M.Kom
NIP. 19710823 199903 1 003

Yogyakarta, 25 Juni 2014
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA UIN SUNAN KALIJAGA FAKULTAS SAINS DAN TEKNOLOGI YOGYAKARTA

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

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
Lamp : 1 Bendel Laporan Skripsi

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	:	Eko Puji Laksono
NIM	:	09650003
Judul Skripsi	:	Analisis Komparasi Algoritma antara metode DES (Data Encryption System) dan AES (Advanced Encryption System)

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

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, 16 Juni 2014
Pembimbing

Arief Ikhwan Wicaksono M.Cs
NIP.

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama : Eko Puji Laksono

NIM : 09650003

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul "**Analisis Komparasi Algoritma antara metode DES (Data Encryption System)dan AES (Advanced Encryption System**)" 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, 16 Juni 2013

Yang menyatakan,

Eko Puji Laksono

NIM. 09650003

MOTTO

“Kita Hidup Hanya Sebentar Jadi Janganlah Kamu Omong Besar Dan Tidak Ada gunanya”

“Janganlah Engkau membicarakan kejelekan orang lain belum tentu orang yang kita omongin lebih jelek dari kita dari segi apapun”

“*Bila anda berani bermimpi tentang sukses berarti anda sudah memegang kunci kesuksesan hanya tinggal berusaha mencari lubangnya kuncinya untuk membuka gerbang kesuksesan*” (john Savique Capone)

“Tuhan mungkin tidak pernah mengabulkan doa kita,tapi tuhan memberi kita pentunjuk dan jalan untuk mendapatkanya” (John Savique Capone)

“*Visi tanpa tindakan adalah lamunan. Tindakan tanpa visi adalah mimpi buruk*”.(Peribahasa Jepang)

HALAMAN PERSEMBAHAN

Puji syukur kehadirat Allah SWT atas limpahan rahmat, innayah dan hidayahnya.

Kupersembahkan penulisan skripsi ini teruntuk :

- Allah SWT, yang selalu melimpahkan banyak kemuliaan dan kenikmatan sehingga skripsi ini dapat terselesaikan pada waktu yang tepat.
- Nabi besar Muhammad SAW, semoga shalawat senantiasa terhatur kepadamu
- Ibu Tetty Setiawaty dan Bapak Gunadi Tjahjono tercinta, berkat beliaulah aku bisa sampai di titik ini. Harapan dan doa yang selalu ibu bapak panjatkan kehadirat Allah SWT, motivasi yang tiada henti, nasihat yang selalu membangun. Terima kasih ibu dan bapak. Anak mu ini belum bisa memberikan yang terbaik. Belum bisa mewujudkan apa yang ibu bapak harapkan.
- Adikku Indriati Pratiwi yang selalu mensupport dan selalu mendukung.
- Teman-teman TIREX 09 tetap kompak tetap jaga tali silaturahim ya...kita satu keluarga.

Teman-teman KKN Angkatan 77 Dukuh Kuton Berbah : Sihru, Rindi, Kiki, Etha, Muhadi, Danu, Nia, Hanif . Terima kasih atas semua kenangan saat kita bersama, kekeluargaan yang indah tak pernah terlupakan.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Assalamu'alaikum Wr.Wb

Segala Puja dan Puji penulis panjatkan bagi Allah SWT yang berhak atas ijabah, pengirim rahmat dan barokah. Sholawat dan salam semoga tercurah kepada Rasulullah pemimpin yang menunjukkan hidayah. Sujud syukur atas segala anugrah dan kenikmatan yang tercurah kepada diri penulis, sehingga penulis mampu menyelesaikan skripsi yang berjudul **"ANALISIS KOMPARASI ALGORITMA KRIPTOGRAFI ANTARA METODE DES (DATA ENCRYPTION SYSTEM) DAN AES (ADVANCED ENCRYPTION SYSTEM)"**. Maksud dan tujuan dari penulisan skripsi ini adalah sebagai salah satu persyaratan guna memperoleh gelar kesarjanaan pada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

Penulisan skripsi ini dapat diselesaikan atas bimbingan dan bantuan berbagai pihak, maka dengan segala kerendahan hati penulis mengucapkan rasa terima kasih dan penghormatan kepada:

1. Bapak Arief Ikhwan Wicaksono, M.Cs., selaku Dosen Pembimbing yang telah berkenan meluangkan waktu untuk membimbing dan mengarahkan penulis dalam menyelesaikan skripsi ini.
2. Bapak Prof. Dr. H. Musa Asy'arie, M.A., selaku Rektor UIN Sunan Kalijaga Yogyakarta.
3. Bapak Prof. Dr. Akh Minhaji, selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
4. Bapak Agus Mulyanto, M.Kom, selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
5. Bapak Agung Fatwanto, S.Si., M.Kom., Ph.D., selaku Dosen Pembimbing Akademik Teknik Informatika angkatan 2009.
6. Para Dosen dan staff Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga.

7. Kepada ayahanda Gunadi Tjahjono, ibunda Tetty Setiawaty dan adik Indriati Pratiwi tersayang yang telah memberikan ketulusan kasih sayang, do'a, motivasi dengan penuh ketulusan dan pengorbanan.
8. Kepada Seluruh Sahabatku TIF 09 yang senantiasa berjalan bersama dalam suka maupun duka.
9. Serta semua pihak yang telah membantu dan memotivasi baik secara langsung maupun tidak yang tidak dapat penulis sebutkan satu persatu.

Akhirnya kepada Allah SWT jualah penulis serahkan segalanya serta panjatkan doa semoga amal kebajikan mereka diterima disisi-Nya, serta diberikan pahala yang berlipat ganda sesuai dengan amal perbuatannya. Penulis berharap semoga skripsi yang sederhana ini dapat bermanfaat bagi penulis khususnya, serta bagi para pembaca pada umumnya, terutama bagi para pendidik (guru) saat ini dan di masa yang akan datang.

Wassalamu'alaikum Wr.Wb

Yogyakarta, 9 Juni 2014
Penulis

EKO PUJI LASKONO
NIM. 09650003

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ANALISIS KOMPARASI ALGORITMA KRIPTOGRAFI ANTARA METODE DES *(DATA ENCRYPTION SYSTEM)* DAN AES *(ADVANCED ENCRYPTION SYSTEM)*

Eko Puji Laksono
NIM. 09650003

INTISARI

Peranan keamanan jaringan saat ini menjadi penting karena semakin berkembang teknologi jaringan menyebabkan ancaman yang akan dihadapi semakin besar. Kondisi tersebut membuka banyak peluang dalam pengembangan aplikasi komputer tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data. Tujuan penelitian ini adalah melakukan analisa perbandingan metode kriptografi antara DES dan AES dari segi struktur enkripsi dan deskripsi, komponen sandi, ronde, karakteristik algoritma, transformasi, dan kunci.

Jenis penelitian adalah analisis komparasi algoritma kriptografi antara metode DES dan AES. Penelitian ini membandingkan dan menganalisis metode DES dan AES dengan cara menguji sampel berdasarkan struktur enkripsi dan deskripsi, ronde, karakteristik algoritma, dan transformasi.

Hasil penelitian menunjukkan: 1) analisis enkripsi dan deskripsi menggunakan program DES lebih sederhana dibandingkan program AES. Data DES diolah hanya dengan empat langkah tanpa menggunakan ronde dan hasilnya dalam bentuk huruf dengan jumlah sesuai dengan huruf yang dianalisa; 2) hasil analisis enkripsi dan deskripsi AES menggunakan algoritma kriptografi AES Rijndael dengan panjang kunci 128 bit memiliki iterasi yang cukup panjang (9 ronde). Langkah yang cukup panjang membuat enkripsi dan deskripsi AES lebih aman; dan 3) penggunaan kriptografi AES Rijndael dengan panjang kunci 192 bit dan 256 bit lebih aman, dan menghasilkan iterasi lebih panjang dan kompleks sehingga sulit untuk diretas oleh hacker atau pihak yang tidak berwenang

Kata Kunci :*kriptografi*, *DES, AES,transformasi*

THE ANALYSIS OF CRYPHTOGRAPHY ALGORITM COMPARISON BETWEEN DES *(DATA ENCRYPTION SYSTEM)* AND AES *(ADVANCED ENCRYPTION SYSTEM)* METHODE

Eko Puji Laksono
NIM. 09650003

ABSTRACT

The network security has a very important role at this time, because the development of network technology caused the greater threat faced. These conditions create a lot of opportunities in the development of computer applications but also makes threats to alter and steal data. The purpose of this research is to analyze the comparison between cryptography method and AES from encryption and description point of view, crypto component, iteration, algorithm character, transformation and key.

The category of this research is cryptography algorithm comparison between DES method *(data encryption system)* and AES *(advanced encryption).* This research is to compare and analyze DES and AES method by examining sample based on the structure of encryption and description, iteration, algorithm character and transformation.

The result of the research reveals: 1) encryption and description analysis uses DES program which is simpler than AES program. DES data is processed by four steps without iteration and the result is alphabet form whose number as many as the analyzed alphabets. ; 2) The result of encryption and description AES analyses uses the cryptography algorithm AES Rijndael with 128 byte key size, it has long iteration (9 iteration). The long steps make encryption and description are more safe ; (3) the usage of cryptography AES Rijndael with 192 and 256 byte key size is more safe and it produces longer and complex iteration so that it is hard to be pirated by hacker or irresponsible hand.

keywords :*cryptography, DES, AES,transformation*

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Internet berasal dari kata *interconnection-networking* adalah sistem global dari seluruh jaringan komputer yang saling terhubung menggunakan standar *Internet Protocol Suite* (TCP/IP) yang melayani miliaran pengguna di seluruh dunia untuk bertukar informasi berbagai arah yang tidak dibatasi oleh jarak dan waktu. Seiring dengan perkembangan teknologi dan informasi, internet telah memberikan pengaruh yang sangat besar pada penyebaran informasi menyebabkan semakin banyak orang mengakses data melalui internet. Kemudahan yang diberikan internet dalam menyebarkan dan transfer informasi menyebabkan jumlah pemakai internet semakin banyak jumlahnya.

Bertambahnya jumlah pengguna internet mendorong banyak tindak kejahatan dalam penggunaan internet. Kejahatan internet yang biasa disebut kejahatan dunia maya (*cyber crime)* akan berdampak buruk bagi perkembangan dan kemajuan internet khususnya untuk keamanan jaringan pengguna internet seperti perusahaan maupun pribadi. Stiawan, Deris (2013: 1) menyatakan sebuah perusahaan yang telah atau akan mengintegrasi jaringan secara terpusat dengan menggunakan komunikasi data via jaringan *private* atau sewa seperti *Leased Channel*, VSAT , VPN atau bahkan menggunakan jaringan publik (internet), maka permasalahan lain yang sangat krusial adalah keamanan *(security)* informasi yang dikirim. Saat ini tidak ada sistem yang aman didunia ini selagi masih dibuat oleh tangan manusia, oleh karena itu kita hanya meningkatkan dari yang tidak aman menjadi aman dan biasanya keamanan akan didapat setelah lubang *(vurnability)* sistem diketahui oleh penyusup. Semua informasi yang dikirim harus dilindungi, oleh karena itu peranan keamanan jaringan saat ini memegang peranan penting

karena semakin berkembang teknologi jaringan menyebabkan ancaman yang akan dihadapi semakin besar. Hal ini membuka banyak peluang dalam pengembangan aplikasi komputer tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data. Sebuah aplikasi yang melintasi jaringan publik seperti internet diasumsikan dapat diakses oleh siapapun termasuk pihak – pihak yang memang berniat untuk mencuri atau mengubah data. Oleh karena itu, untuk melindungi data terhadap akses, pengubahan, dan penghalangan yang tidak dilakukan oleh pihak yang berwenang, peranti keamanan data yang melintas di jaringan komputer harus disediakan. Berkembang teknologi jaringan menyebabkan perkembangan ancaman *vurnerability* jaman sekarang menjadi meningkat. Meningkatkan *vulnerability* keamanan sebuah jaringan seiring dengan berkembangnya teknologi jaringan itu sendiri. Dikarenakan banyak pihak yang tidak berwenang ingin mengancam pengaksesan, pengubahan,dan penghalangan oleh pihak yang tidak berhak.

Kriptografi menjadi solusi mengatasi ancaman keamanan data. Metode – metode kriptografi diantaranya DES *(Data Encryption System)*, AES *(Advance Encryption Standard).* Sistem DES merupakan sistem sandi blok dengan kunci simetri. Ukuran blok yang digunakan adalah 64 bit dan ukuran kunci DES adalah 56 bit tanpa parity bit. Struktur DES menggunakan struktur sandi Feistel, yang terdiri dari 16 ronde. Komponen – komponen system sandi blok modern : boks substitusi, boks permutasi, operasi shift sirkular, operasi bit XOR, dan swap. Sandi produk DES adalah sandi yang tersusun oleh komponen system sandi blok modern. Tujuan utama system sandi blok modern DES adalah tercapainya difusi dan *confusion.* Secara umum, DES masih dianggap aman dari serangan analisis sandi diferensial dan linear. Sistem sandi DES dapat diperluas ukuran ruang kunci dengan menggunakan *triple* DES (3-DES). Sedangkan sistem sandi AES memenuhi spesifikasi sandi blok dengan ukuran blok dengan ukuran blok teks asli

128 bit dan mampu bekerja dengan kunci 128, 192, dan 256 bit. Unit data sandi AES diorganisir sebagai state (128 bit), word (32 bit), byte (8 bit), dan bit. Enkripsi dan deskripsi AES terdiri beberapa ronde. AES dengan 128 bit memiliki 10 ronde, 192 bit memiliki 12 ronde, dan 256 bit memiliki 14 ronde. Setiap ronde AES menggunakan 4 transformasi dasar : SubBytes, ShiftRows, MixColumn, dan AddRoundKey. Ekspansi kunci AES menghasilkan kunci ronde. Pembangkitan kunci diolah dengan unit data word dan menggunakan operasi rotWord dan subWord.

Berdasarkan uraian di atas, skripsi ini menganalisis perbandingan keamanan jaringan menggunakan metode DES dan AES. Kedua metode tersebut menjadi penting karena kerentanan keamanan data saat ini dapat diamankan dengan kedua metode kriptografi DES dan AES.

1.2. Rumusan Masalah

a. Bagaimana hasil perbandingan struktur enskripsi dan deskripsi pada metoda DES dan AES.
b. Bagaimana hasil perbandingan ronde pada struktur enskripsi dan deskripsi metoda DES dan AES.
c. Bagaimana hasil perbandingan analisa karakteristik algoritma pada metoda DES dan AES
d. Bagaimana hasil perbandingan analisa transformasi pada metoda DES dan AES

1.3. Batasan Masalah

Berdasarkan permasalahan di atas, batasan penelitian ini adalah:

a. Menganalisa hanya pada metode DES dan AES.
b. Parameter – parameter kedua metode yang dibandingkan hanya struktur enkripsi dan deskripsi, ronde, karakteristik algoritma, transformasi.

1.4. Tujuan Penelitian

Tujuan dalam penelitian ini adalah:

a. Mendapatkan data tentang cara kerja dan hasil analisis perbandingan menggunakan struktur enskripsi dan deskripsi pada metoda DES dan AES
b. Mendapatkan data tentang perbandingan hasil ronde pada analisis struktur enkripsi dan deskripsi metode DES dan AES
c. Mendapatkan data tentang hasil analisis perbandingan karakteristik algoritma enkripsi dan deskripsi pada metoda DES dan AES
d. Mendapatkan data tentang analisis perbandingan transformasi enkripsi dan deskripsi pada metoda DES dan AES

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah :

a. Mengetahui cara kerja mengamankan data melalui analisis data struktur enskripsi dan deskripsi pada metoda DES dan AES
b. Dapat melakukan analisis dan membandingkan hasil analisis data menggunakan struktur enskripsi dan deskripsi pada metoda DES dan AES
c. Dapat membandingkan hasil analisis ronde pada struktur enkripsi dan deskripsi metoda DES dan AES
d. Dapat membandingkan karakteristik algoritma pada struktur enkripsi dan deskripsi metoda DES dan AES
e. Dapat membandingkan hasil transformasi pada struktur enkripsi dan deskripsi metoda DES dan AES

1.6. Keaslian Penelitian

Penelitian yang berhubungan dengan analisis komparasi algoritma kriptografi antara metode DES dan AES di Fakultas Sains Dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta belum pernah dilakukan.

BAB V

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan hasil analisa yang sudah dilakukan, maka dapat diambil kesimpulan:

1. Hasil analisis enkripsi dan deskripsi menggunakan program DES lebih sederhana dibandingkan program AES. Data DES diolah hanya dengan empat langkah tanpa menggunakan ronde sehingga hasilnya lebih sederhana dalam bentuk huruf yang jumlahnya sama dengan data yang diolah.
2. Hasil analisis enkripsi dan deskripsi AES menggunakan algoritma kriptografi AES Rijndael dengan panjang kunci 128 bit memiliki iterasi yang cukup panjang (9 ronde). Data dimasukkan dalam bentuk matriks input bits setelah diolah 9 ronde akan menghasilkan matriks output. Langkah yang cukup panjang membuat enkripsi dan deskripsi AES lebih aman.
3. DES tidak memiliki ronde. Enkripsi AES memiliki 9 ronde (ronde 1 – 9) dan desripsi AES memiliki 9 ronde (ronde 9 – 1).
4. Karakteristik enskripsi DES menggunakan rumus : C=P+K+1)mod26 dan deskripsi DES menggunakan rumus : P≡(C+26-K-1) mod26. Karakteristik enkripsi AES setiap rondenya memiliki SubBytes, ShiftRows, MixColomn, dan RoundKey. Karakteristik deskripsi AES setiap rondenya memiliki InvShiftRows, InvSubBytes, RoundKey dan AddRoundKey.

Transformasi DES dilakukan berdasarkan langkah Plainteks-Enkripsi-Chiperteks-Deskripsi-Plainteks. Transformasi enskripsi AES menggunakan langkah – langkah kerja SubBytes, ShiftRows, MixColomn, dan6. AddRoundKey setiap rondenya.

Transformasi deskripsnya AES menggunakan kebalikannya dari enkripsinya yaitu: AddRoundKey, InvSSubBytes, InvShiftRows.

5.1. SARAN

1. Hindari mengirim data menggunakan metode DES karena memiliki langkah kerja yang sederhana dan tidak menggunakan ronde sehingga hasil sederhana dalam bentuk huruf bukan matriks.
2. Disarankan mengirim data menggunakan metode AES minimal menggunakan 128 bits karena memiliki iterasi berulang dalam bentuk 10 ronde. Menggunakan metode AES dengan panjang kunci 128 bit memiliki jalan yang cukup panjang sehingga data dikirim dalam bentuk sandi yang diamankan dari para peretas.
3. Sebaiknya mengirim data menggunakan kunci yang lebih panjang seperti kunci 192 bit (12 ronde) dan 256 bit (14 ronde) karena menghasilkan iterasi atau ronde yang lebih panjang sehingga sulit untuk diretas oleh hacker atau pihak yang tidak berwenang. Semakin panjang kunci yang digunakan semakin aman data yang kita sandikan.

DAFTAR PUSTAKA

Ahmadfina. 2010. *Jaringan Komputer*. Diambila dari http://ilmukomputer.org/wp-content/uploads/2013/01/Ilmu-komputer-Jaringan-Komputer-Dan-Pengertiannya.pdf. pada tanggal 14 Januari 2014.

Ayuliana.2011.*Testing dan Implementasi : Software Quality Assurance.* Jakarta: Universitas Gunadarma.

http://people.eku.edu/styere/Encrypt/JS-AES.html. *Tool of Advanced Encryption Standard (AES) dari The Rijndael algorithm 2001.*

http://logicacmg.com. *Tool of Data Encryption Standard (DES) in FIPS 46-3 Using a 56-bit key*.

Bevan, Nigel.1997.*Quality and usability: A new framework Usability Services.* National Physical Laboratory:UK.

Dewananta, Dhida. 2007. *Keamanan Jaringan Komputer.pdf.* Diambil dari http://ilmukomputer.org/wp-content/uploads/2013/01/Ilmu-komputer-Jaringan-Komputer-Dan-Pengertiannya.pdf. pada tanggal 14 Januari 2014.

Handaka, Michell S. 2010. *Analisis AES Rijndael terhadap DES. Makalah IF3058 Kriptografi – Sem. II Tahun 2010/2011.* Bandung: Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung

Johnson, Jeff. 2006. GUI Bloopers 2.0 : *Common User Interface Design Don'ts and Dos.* San Fransisco : Morgan Kauffman

Kurose J. F dan Ross K. W. 2010.Computer Networking A Top-Down Approach Fifth Edition: Addison Wesley.

Kusdiantoro.2012. *Analisis Usability Website Akademik Perguruan Tinggi di Indonesia Menggunakan Metode Promethee, Vikor dan Electree.* Yogyakarta:Universitas Negeri Yogyakarta.

Munir, Rinaldi. 2004. *Advanced Encryption Standard* (*AES*). Bahan Kuliah ke-13. Bandung: Departemen Teknik Informatika Institut Teknologi Bandung

Nasution, Benny Benyamin. 2010. Strategi Untuk Meningkatkan Budaya Transaksi Wireless di Masyarakat. Jurnal Masyarakat Budaya dan Politik. Volume 22, Nomor 4: 360-366. Diambil dari http://mkp.fisip.unair.ac.id.

Nielsen, J. Mack, Robert L. Usability *Inspection Methods. 1994.* New York : John Wiley & Sons.

Proboyekti,2013. Pengantar Teknologi Informasi Prodi Sistem Informasi UKDW: Jaringan Komputer. Diambil dari ttp://lecturer.ukdw.ac.id/othie/ Jaringan_ Komputer.pdf.

Reza, Muhammad Rabbani, Hanum Syarifah.2012. *Metric Of Software Quality Factors.*Surakarta: Universitas Sebelas Maret.

Robert, A.Martin.2009. *Jalan Evolution untuk Metode Evaluasi Kualitas Perangkat Lunak Industri Menerapkan ISO / IEC9126:2001Kualitas Model: Contoh Metode SQAE Mitre's.*Montreal, Canada:MITRE Corporation

Sadikin, Rifki.2012. *Kriptografi untuk Keamanan Jaringan Dan Implementasinya dalam Bahasa Java*.C.V Andi Offset.Yogyakarta.

Stiawan, Deris. 2013. *Sistem Keamanan Komputer* . Jakarta: Penulis Elex Media Komputindo. Diambil dari *books.google.co.id/books/about/Sistem _Keamanan_ Komputer.html?id.*

Suharso, dan Ana Retnoningsih.2005. *Kamus Besar Bahasa Indonesia Departemen Pendidikan Nasional.*Jakarta:Balai Pustaka.

Suraya, Ignasius. 2011. IPSec: Sebagai Salah Satu Aplikasi Teknik Kriptografi/ Keamanan Data Pada Jaringan Komputer. Diambil dari http://jurtek. akprind.ac.id/sites/default/files/52-60_suraya.pdf.

Thomas Tom 2004. *Network Security First-Step.* Diterjemahkan oleh tim penerjemah andi.Yogyakarta:Andi Offset.

Yudianto, Jafar M Noor 2013. Jaringan Komputer dan Jaringannya. Diambil dari http://people.eku.edu/styere/Encrypt/JS-AES.html

Zebua, Jimmy Hendisaro, Restyandito, dan Lucia D. Krisnawati. 2011.*Implementasi Prinsip Usability F-Shape Pattern pada Konten Website.*Yogyakarta : Universitas Kristen Duta Wacana.

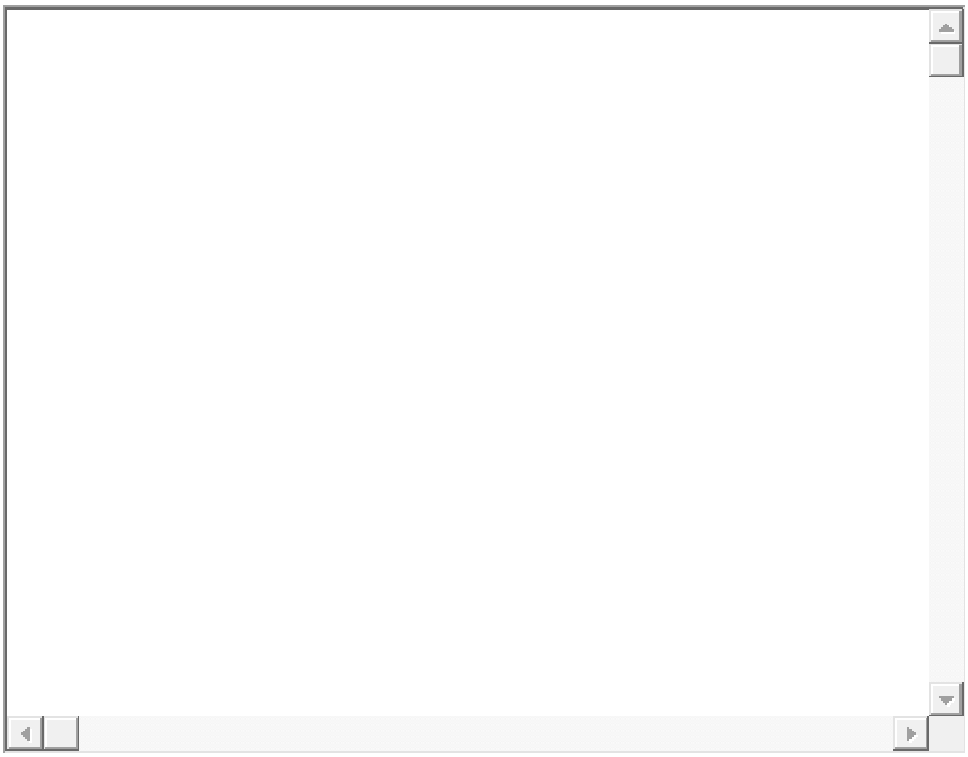
Lampiran-1. Tool DES

The Data Encryption Standard (DES) was introduced in 19xx and is formally defined in FIPS 46-3 Using a 56-bit key (usually entered as a 64-bit value with odd parity bits), working on a 64-bit data block. There are several modes for using DES to encrypt blocks of data that may be more (or less) than 8 bytes in size. Click here for more details on how DES works.

The 56-bit key used by DES is no longer sufficient for good security, but many applications use triple-DES (encrypt using key part A, decrypt using key part B, encrypt using key part A) to acheive a 112-bit key while maintaining compatibility with plain DES (using key part A = key part B).

Message	
	ASCII Hexadecimal
DES Key/Triple DES Key Part A	3b3898371520f75e
Triple DES Key Part B	922fb510c71f436e
Output message	
	ASCII Hexadecimal

Details:



How DES works

Encryption starts with an initial permutation of the 64 input bits. These bits are then divided into two 32-bit halves called L and R. The encryption then proceeds through 16 rounds, each using the existing L and R parts, and a subkey. The R and subkeys are processed in a function *f*, and the output of the *f* function are exclusive-or'ed with the existing L part to create the new R part. The new L part is simply a copy of the incoming R part. In the final round, the L and R parts are swapped once more before the final permutation producing the output block.

Decryption is identical to encryption, except that the subkeys are used in the opposite order. That is, subkey 16 is used in round 1, subkey 15 is used in round 2, etc., ending with subkey 1 being used in round 16.

Here is a diagram of the DES algorithm:

Lampiran-2. Tool AES

The Rijndael algorithm was announced as the winner of the Advanced Encryption Standard (AES) in 2001. This algorithm is intended to replace the DES algorithm. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES is defined in Fips 197. Click here for a description of how AES works.

10/27/06: I have decided to not allow the key to changed to reduce the chance of this page being used to solve homework problems

An input ASCII string that is less than 16 characters long will be padded with NULL characters.

Message: ASCII Hexadecimal

Key 0f 15 71 c9 47 d9 e8 59 0c b7 ad d6 af 7f 67 98

Output message ASCII Hexadecimal

Details:

ii'
iii

How AES Works

This page only describes the 128-bit version, but the 192-bit and 256-bit key versions are similar.

AES is designed to work on bytes. However, each byte is interperted as a representation of the polynomial:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

Where each b_i is either 0 or 1.

Addition and Multiplication

Addition then becomes exclusive-or, but multiplication is defined as polynomial multiplication modulo $x^8 + x^4 + x^3 + x + 1$. For example **2d * a3** would be calculated as follows (remembering $x^y + x^y = 0$):

2d = 00101101 = $x^5 + x^3 + x^2 + 1$

a3 = 10100011 = $x^7 + x^5 + x + 1$

2d * a3 = $(x^{12} + x^{10} + x^9 + x^7) + (x^{10} + x^8 + x^7 + x^5) + (x^6 + x^4 + x^3 + x) + (x^5 + x^3 + x^2 + 1)$

$= x^{12} + x^9 + x^8 + x^6 + x^4 + x^2 + x + 1$

- modulus * x^4 = $x^9 + x^7 + x^6 + x^5 + x^2 + x + 1$

- modulus * x = $x^7 + x^6 + x^4 + 1$

2d * a3 = 11010001 = d1

Although this seems not efficient, all multiplications are by a constant, so they can be calculated in advance and turned into a simple table lookup.

Algorithm State

The 128-bit state can be represented as a 4 by 4 table of bytes. The cipher will perform various operations on this array.

Encryption Algorithm (128-bit version)

```
Cipher(byte in[16], byte out[16], word w[44])
begin

      byte state[4,4]
      state = in
      AddRoundKey(state, w[0, 3])
      for round = 1 step 1 to 10

            SubBytes(state)
            ShiftRows(state)
            MixColumns(state)
            AddRoundKey(state, w[round*4, (round+1)*4-1])
```

```
        end for
        SubBytes(state)
        ShiftRows(state)
        AddRoundKey(state, w[40, 43])
        out = state

    end
```

SubBytes Routine

In this routine, each byte of the state is replaced according to the following formula:

> For each bit *i*, set b_i to b_i *xor* $b_{(i+4) \bmod 8}$ *xor* $b_{(i+5) \bmod 8}$ *xor* $b_{(i+6) \bmod 8}$ *xor* $b_{(i+7) \bmod 8}$ + c_i where c = 63 hex.

As with multiplication, this is usually implemented as a table lookup.

ShiftRows Routine

This routine modifies each row of the state matrix. The top row is not changed, the next row is rotated left one position, the following row two positions, and the bottom row three positions.

MixColumns Routine

This function mixes up the data in each column according to the following formulas:

- Set $s_{0,c}$ to $2*s_{0,c}$ *xor* $3*s_{1,c}$ *xor* $s_{2,c}$ *xor* $s_{3,c}$
- Set $s_{1,c}$ to $_{0,c}$ *xor* $2*s_{1,c}$ *xor* $3*s_{2,c}$ *xor* $s_{3,c}$
- Set $s_{2,c}$ to $s_{0,c}$ *xor* $s_{1,c}$ *xor* $2*s_{2,c}$ *xor* $3*s_{3,c}$
- Set $s_{3,c}$ to $3*s_{0,c}$ *xor* $s_{1,c}$ *xor* $s_{2,c}$ *xor* $2*s_{3,c}$

AddRoundKey Routine

This function does an XOR between each column of the state and a 32-bit word from the key schedule.

Key Expansion

The key schedule *w* is generated in the following form:

- The first four words (*w[0]* through *w[3]*) of the key are the incoming cipher key.
- To calculate *w[i]* for *i* from 4 to 43:
    - Set *temp = w[i-1]*
    - If *i* = 4, 8, 12, 16, ..., 40 (multiples of 4)
        - Rotate this word left one byte
        - Replace each byte (using the same substitution function as SubBytes)
        - Do an exclusive-or with the round constant *Rcon[i]*
    - Set *w[i] = w[i-4]* xor *temp*

AES Decryption

Decryption basically consists of performing each of the encryption steps in reverse, using the following algorithm:

```
InvCipher(byte in[16], byte out[16], word w[44])])
begin

      byte state[4,4]
      state = in
      AddRoundKey(state, w[40, 43])
      for round = 9 step -1 downto 1

            InvShiftRows(state)
            InvSubBytes(state)
            AddRoundKey(state, w[round*3, (round+1)*3-1])
            InvMixColumns(state)

      end for
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state, w[0, 3])
      out = state
end
```

Each of the `Inv...` functions is the inverse of the corresponding encryption function. `InvSubBytes`becomes another table lookup, and the equations for `InvMixColumns` are:

- Set $s_{0,c}$ to $0x0e*s_{0,c}$ *xor* $0x0b*s_{1,c}$ *xor* $0x0d*s_{2,c}$ *xor* $0x09*s_{3,c}$
- Set $s_{1,c}$ to $0x09*s_{0,c}$ *xor* $0x0e*s_{1,c}$ *xor* $0x0b*s_{2,c}$ *xor* $0x0d*s_{3,c}$
- Set $s_{2,c}$ to $0x0d*s_{0,c}$ *xor* $0x09*s_{1,c}$ *xor* $0x0e*s_{2,c}$ *xor* $0x0b*s_{3,c}$
- Set $s_{3,c}$ to $0x0b*s_{0,c}$ *xor* $0x0d*s_{1,c}$ *xor* $0x09*s_{2,c}$ *xor* $0x0e*s_{3,c}$

The algorithm can be rewritten so it looks similar to the encryption algorithm, with a few simple modifications.

Lampiran-3. Analisis Enskripsi DES: Yogi Surya Nugraha

Plainteks
YOGI SURYA NUGRAHA
Kunci : VIGENERE
Enkripsi dengan table
YOGISURYANUGRAHA
Jika dengan menggunakan perhitungan fungsi maka :
Y+V=25+22-1)mod 26=20=>T
O+I=15+9-1)mod26=23=>W
G+G=7+7-1)mod26=13=>M
I+E=9+5-1)mod26=13=>M
S+N=19+14-1)mod26=6=>F
U+E=21+5-1)mod26=25=>Y
R+R=18+18-1)mod26=9=>I
Y+E=25+5-1)mod26=3=>C
A+V=1+22-1)mod26=22=>V
N+I=14+9-1)mod26=22=>V

U+G=21+7-1)mod26=1=>A
G+E=7+5-1)mod26=11=>K
R+N=18+14-1)mod26=5=>E
A+E=1+5-1)mod26=5=>E
H+R=8+18-1)mod26=25=>Y
A+E=1+5-1)mod26=5=>E
Jadi chipper teksnya adalah TWMMFYSCVVAKEEYE

Lampiran -4. Analisis Enskripsi DES: Eko Puji Laksono

State
EKO PUJI LAKSONO
Kunci : VIGENERE
Enkripsi dengan table
EKOPUJILAKSONO
Jika dengan perhitungan fungsi maka:
E+V=5+22-1)mod 26=0=>z
K+I=11+12-1)mod26=22=>v
O+G=15+7-1)mod26=21=>u
P+E=16+5-1)mod26=20=>t
U+N=21+14-1)mod26=8=>h
J+E=10+5-1)mod26=14=>n
I+R=12+18-1)mod26=3=>c
L+E=12+5-1)mod26=16=>P
A+V=1+22-1)mod26=22=>V
K+I=11+9-1)mod26=19=>S
S+G=19+7-1)mod26=25=>Y
O+E=15+5-1)mod26=19=>S
N+N=14+14-1)mod26=1=>A
O+E=15+5-1)mod26=19=>S
Chipper teksnya adalah: ZVUTHNCPVSYSAS

Lampiran-5. Analisis Enskripsi DES: Estu Fardani

state
ESTUFARDANI
Kunci :VIGENERE
Jika menggunakan fungsi maka:
E+V=5+22-1)mod26=0=>Z
S+I=19+9-1)mod26=1=>A
T+G=20+7-1)mod26=0=>Z
U+E=21+5-1)mod26=25=>Y
F+N=6+14-1)mod26=19=>S
A+E=1+5-1)mod26=5=>E
R+R=18+18-1)mod26=9=>I
D+E=4+5-1)mod26=8=>H
A+V=1+22-1)mod26=22=>V
N+I=14+9-1)mod26=22=>V
I+G=9+7-1)mod26=15=>O
Chipper teksnya : ZAZYSEIHVVO

Lampiran-6. Analisis Enskripsi DES: Rahmatullah Priyo Kusuma

State
RAHMATULLAH PRIYO KUSUMA
Kunci
VIGENERE
Jika menggunakan fungsi maka :
R+V=18+22-1)mod26=13=>M
A+I=1+9-1)mod26=9=>I
H+G=8+7-1)mod26=14=>N
M+E=13+5-1)mod26=17=>Q
A+N=1+14-1)mod26=14=>N
T+E=20+5-1)mod26=24=>X
U+R=21+18-1)mod26=12=>L
L+E=12+5-1)mod26=16=>P
L+V=12+22-1)mod26=7=>G
A+I=1+9-1)mod26=9=I
H+G=8+7-1)mod26=14=>N
P+E=16+5-1)mod26=20=>T
R+N=18+14-1)mod26=5=>E
I+E=9+5-1)mod26=13=>M
Y+R=25+18-1)mod26= 16=P
O+E=15+5-1)mod26=19=>S
K+V=11+22-1)mod26=6=>F
U+I=21+9-1)mod26=3=>C
S+G=19+7-1)mod26=25=>Y
U+E=21+5-1)mod26=25=>Y
M+N=13+14-1)mod26=0=>Z
A+E=1+5-1)mod26=5=>E
Chipper teks:MINQNXLPGINTEMPSFCYYZE

Lampiran-7. Analisis Enskripsi DES: Rizki Tunjung Sari

State
RIZKI TUNJUNG SARI
Kunci
VIGENERE
Jika menggunakan fungsi maka :
R+V=18+22-1)mod26=13=>M
I+I=9+9-1)mod26=17=>Q
Z+G=26+7-1)mod26=6=>F
K+E=11+5-1)mod26=15=>O
I+N=9+14-1)mod26=22=>V
T+E=20+5-1)mod26=24=>X
U+R=21+18-1)mod26=12=>L
N+E=14+5-1)mod26=18=>R
J+V=10+22-1)mod26=5=>E
U+I=21+9-1)mod26=3=>C
N+G=14+7-1)mod26=20=>T
G+E=7+5-1-1)mod26=11=>K
S+N=19+14-1)mod26=6=>F
A+E=1+5-1)mod26=5=>E
R+R=18+18-1)mod26=9=>I
I+E=9+5-1)mod26=13=>M
Chipper key: MQFOVXLRECTKFEIM

Lampiran-8. Analisis Deskripsi DES: TWMMFYSCVVAKEEYE

Chipher teksnya TWMMFYSCVVAKEEYE
Kunci VIGENERE
T-V=20+26-22+1)Mod26=25=>Y
w-I=23+26-9+1)MOD26)mod26=15=O
M-G=13+26-7+1)mod26=7=G
M-E=13+26-5+1)mod26=9=I
F-N=6+26-14+1)mod26=19=S
Y-E=25+26-5+1)mod26=21=U
I-R=9+26-18+1)mod26=18=>R
C-E=3+26-5+1)mod26=25=.Y
V-V=22+26-22+1)mod26=1=>A
V-I=22+26-9+1)mod26=14=>N
A-G=1+26-7+1)mod26=21=>U
K-E=11+26-5+1)mod26=7=>G
E-N=5+26-14+1)mod26=18=>R
E-E=5+26-5+1)mod26=1=>A
Y-R=25+26-18+1)mod26=8=>H
E-E=5+26-5+1)mod26=1=>A
Plainteksnya YOGISURYANUGRAHA

Lampiran-9. Analisis Deskripsi DES: ZVUTHNCPVSYSAS

Chipper teksnya:ZVUTHNCPVSYSAS
Kunci :VIGENERE
Z-V=26+26-22+1)mod26=5=>E
V-I=22+26-9+1)mod26=11=>K
U-G=21+26-7+1)mod26=15=>O
T-E=20+26-5+1)mod26=16=>P
H-N=8+26-14+1)mod26=21=>U
N-E=14+26-5+1)mod26=10=>J
C-R=3+26-18+1)mod26=9=>I
P-E=16+26-5+1)mod26=12=>L
V-V=22+26-22+1)mod26=1=>A
S-I=19+26-9+1)mod26=11=>K
Y-G=25+26-7+1)mod26=19=>S
S-E=19+26-5+1)mod26=15=>O
A-N=1+26-14+1)mod26=14=>N
S-E=19+26-5+1)mod26=15=>O
Jadi Plainteksnya adalah EKOPUJILAKSONO

Lampiran-10. Analisis Deskripsi DES: ZAZYSEIHVVO

Chipper teks: ZAZYSEIHVVO
Kunci : VIGENERE
Z-V=26+26-22+1)mod26=E
A-I=1+26-9+1)mod26=19=>S
Z-G=26+26-7+1)mod26=20=>T
Y-E=25+26-5+1)mod26=21=>U
S-N=19+26-14+1)mod26=6=>F
E-E=5+26-5+1)mod26=1=>A
I-R=9+26-18+1)mod26=18=>R
H-E=8+26-5+1)mod26=4=>D
V-V=22+26-22+1)mod26=1=>A
V-I=22+26-9+1)mod26=14=>N
O-G=15+26-7+1)mod26=9=>I
Jadi plainteksnya ESTUFARDANI

Lampiran-11. Analisis Deskripsi DES: MINQNXLPGINTEMPSFCYYZE

Chipper teks: MINQNXLPGINTEMPSFCYYZE
Kunci : VIGENERE
M-V=13+26-22+1)mod26=18=R
I-I=9+26-9+1)mod26=1=>A
N-G=14+26-7+1)mod26=8=>H
Q-E=17+26-5+1)mod26=13=>M
N-N=14+26-14+1)mod26=1=>A
X-E=24+26-5+1)mod26=20=>T
L-R=12+26-18+1)mod26=21=>U
P-E=16+26-5+1)mod26=12=>L
G-V=7+26-22+1)mod26=12=>L
I-I=9+26-9+1)mod26=1=>A
N-G=14+26-7+1)mod26=8=>H
T-E=20+26-5+1)mod26=16=>P
E-N=5+26-14+1)mod26=18=>R
M-E=13+26-5+1)mod26=9=>I
P-R=16+26-18+1)mod26=25=>Y
S-E=19+26-5+1)mod26=15=>O
F-V=6+26-22+1)mod26=11=>K
C-I=3+26-9+1)mod26=21=>U
Y-G=25+26-7+1)mod26=19=>S
Y-E=25+26-5+1)mod26=21=>U
Z-N=26+26-14+1)mod 26=13=>M
E-E=5+26-5+1)mod26=1=>A
Jadi plainteksnya adalah RAHMATULLAHPRIYOKUSUMA

Lampiran-12. Analisis Deskripsi DES: MQFOVXMLRECTKFEIM

Chipper teks: MQFOVXMLRECTKFEIM
Kunci : MQFOVXLRECTKFEIM
M-V=13+26-22+1)mod26=R
Q-I=17+26-9+1)mod26=9=>I
F-G=6+26-7+1)mod26=26=>Z
O-E=15+26-5)mod26=11=>K
V-N=22+26-14+1)mod26=9=>I
X-E=24+26-5+1)mod26=20=>T
L-R=12+26-18+1)mod26=21=>U
R-E=18+26-5+1)mod26=14=>N
E-V=5+26-22+1)mod26=10=>J
C-I=3+26-9+1)mod26=21=>U
T-G=20+26-7+1)mod26=14=>N
K-E=11+26-5+1)mod26=7=>G
F-N=6+26-14+1)mod26=19=>S
E-E=5+26-5+1)mod26=1=>A
I-R=9+26-18+1)mod26=18=>R
M-E=13+26-5+1)mod26=9=>I
Jadi plainteksnya adalah RIZKITUNJUNGSARI

Lampiran-13. Analisis Enskripsi AES: YOGI SURYA NUGRAHA

YOGI SURYA NUGRAHA

Input bits 79 6f 67 69
20 73 75 72
79 61 20 6e
75 67 72 61
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1

w[17] = a5 73 0e 96
w[18] = f2 22 a3 90
w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
 ^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
 ^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
 ^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
 ^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
 ^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
 ^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52

w[41] = ba 98 13 4e
w[42] = 7f 4d 59 20
w[43] = 86 26 18 76

Initial state 79 20 79 75
6f 73 61 67
67 75 20 72
69 72 6e 61

Round Key 0f 47 0c af
15 d9 b7 7f
71 e8 ad 67
c9 59 d6 98

Round 1 76 67 75 da
7a aa d6 18
16 9d 8d 15
a0 2b b8 f9

After SubBytes 38 85 9d 57
da ac f6 ad
47 5e 5d 59
e0 f1 6c 99

After ShiftRows 38 85 9d 57
ac f6 ad da
5d 59 47 5e
99 e0 f1 6c

After MixColumns 5b a9 7b e9
05 79 e4 76
9e fa b6 85
90 e0 af a5

Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7

Round 2 87 32 ec d1
95 30 1a f7
a9 25 c4 90
20 09 90 02

After SubBytes 17 23 ce 3e
2a 04 a2 68
d3 3f 1c 60
b7 01 60 77

After ShiftRows 17 23 ce 3e
04 a2 68 2a

1c 60 d3 3f
77 b7 01 60
After MixColumns 49 6c ed 5d
4c 6b 71 4b
b2 83 18 ca
cf d2 f0 97
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
Round 3 9b 25 33 bb
85 eb 0f b4
d9 37 de 19
78 8c 91 51
After SubBytes 14 3f c3 ea
97 e9 76 8d
35 9a 1d d4
bc 64 81 d1
After ShiftRows 14 3f c3 ea
e9 76 8d 97
1d d4 35 9a
d1 bc 64 81
After MixColumns c4 8c 40 76
2b 08 f9 eb
af 25 88 ca
71 80 2e 31
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
Round 4 04 05 17 c7
84 27 a8 45
70 4e 25 b4
48 e7 28 f1
After SubBytes f2 6b f0 c6
5f cc c2 6e
51 2f 3f 8d
52 94 34 a1
After ShiftRows f2 6b f0 c6
cc c2 6e 5f
3f 8d 51 2f
a1 52 94 34

After MixColumns 2e 54 8c 6d
91 2a 4b 3d
b8 5e 9b 9b
a7 56 07 49
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50
Round 5 02 f1 7e 2e
cd 59 69 b1
dd 50 38 46
56 c0 97 19
After SubBytes 77 a1 f3 31
bd cb f9 c8
c1 53 07 5a
b1 ba 88 d4
After ShiftRows 77 a1 f3 31
cb f9 c8 bd
07 5a c1 53
d4 b1 ba 88
After MixColumns 7b a2 c5 65
27 17 9a 2d
d5 24 77 a9
e6 22 68 b6
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
Round 6 23 5f ca 29
ba f9 56 6d
e3 1c ec ef
0d 5f 85 0b
After SubBytes 26 cf 74 a5
f4 99 b1 3c
11 9c ce df
d7 cf 97 2b
After ShiftRows 26 cf 74 a5
99 b1 3c f4
ce df 11 9c
2b d7 cf 97
After MixColumns 19 45 72 5d
6d 1b f0 7e

45 b9 20 d0
6b 91 34 a9
Round Key 71 8c 83 cf
c7 29 e5 a5
4c 74 ef a9
c2 bf 52 ef
Round 7 68 c9 f1 92
aa 32 15 db
09 cd cf 79
a9 2e 66 46
After SubBytes 45 dd a1 4f
ac 23 59 b9
01 bd 8a b6
d3 31 33 5a
After ShiftRows 45 dd a1 4f
23 59 b9 ac
8a b6 01 bd
5a d3 31 33
After MixColumns 3f 2f b9 ff
dc 7d fa e3
87 9d 49 d7
d2 2e 22 a6
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
Round 8 08 94 81 08
c8 40 22 9e
14 7a 41 76
9a d9 87 ec
After SubBytes 30 22 0c 30
e8 09 93 0b
fa da 83 38
b8 35 17 ce
After ShiftRows 30 22 0c 30
09 93 0b e8
83 38 fa da
ce b8 35 17
After MixColumns 36 6a ca 8e
72 ef 3a 99
6d 12 b7 4e
5d a6 8f 4c

Round Key 48 f3 cb 3c
26 1b c3 be
45 a2 aa 0b
20 d7 72 38

Round 9 7e 99 01 b2
54 f4 f9 27
28 b0 1d 45
7d 71 fd 74
After SubBytes f3 ee 7c 37
20 bf 99 cc
34 e7 a4 6e
ff a3 54 92
After ShiftRows f3 ee 7c 37
bf 99 cc 20
a4 6e 34 e7
92 ff a3 54
After MixColumns 11 e6 20 bd
f3 8a 00 11
b2 b1 26 3e
2a 3b 21 36
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After SubBytes ce 9b d9 1b
bb de 03 da
8c d1 50 d2
f8 cc 84 d0
After ShiftRows ce 9b d9 1b
de 03 da bb
50 d2 8c d1
d0 f8 cc 84
Output 7a 21 a6 9d
50 9b 97 9d
a3 c1 d5 c9
82 b6 ec f2

Lampiran-14. Analisis Enskripsi AES: EKO PUJI LAKSONO

EKO PUJI LAKSONO

Input bits 65 6b 6f 20
70 75 6a 69
20 6c 61 6b
73 6f 6e 6f
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96
w[18] = f2 22 a3 90
w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb

```
w[21] =   fd ee 38 7d
w[22] =   0f cc 9b ed
w[23] =   4c 40 46 bd
RotWord()=  40 46 bd 4c
SubWord()=  09 5a 7a 29
 ^ Rcon()=  29 5a 7a 29
w[24] =   71 c7 4c c2
w[25] =   8c 29 74 bf
w[26] =   83 e5 ef 52
w[27] =   cf a5 a9 ef
RotWord()=  a5 a9 ef cf
SubWord()=  06 d3 df 8a
 ^ Rcon()=  46 d3 df 8a
w[28] =   37 14 93 48
w[29] =   bb 3d e7 f7
w[30] =   38 d8 08 a5
w[31] =   f7 7d a1 4a
RotWord()=  7d a1 4a f7
SubWord()=  ff 32 d6 68
 ^ Rcon()=  7f 32 d6 68
w[32] =   48 26 45 20
w[33] =   f3 1b a2 d7
w[34] =   cb c3 aa 72
w[35] =   3c be 0b 38
RotWord()=  be 0b 38 3c
SubWord()=  ae 2b 07 eb
 ^ Rcon()=  b5 2b 07 eb
w[36] =   fd 0d 42 cb
w[37] =   0e 16 e0 1c
w[38] =   c5 d5 4a 6e
w[39] =   f9 6b 41 56
RotWord()=  6b 41 56 f9
SubWord()=  7f 83 b1 99
 ^ Rcon()=  49 83 b1 99
w[40] =   b4 8e f3 52
w[41] =   ba 98 13 4e
w[42] =   7f 4d 59 20
w[43] =   86 26 18 76
Initial state   65 70 20 73
                6b 75 6c 6f
                6f 6a 61 6e
                20 69 6b 6f
Round Key  0f 47 0c af
           15 d9 b7 7f
           71 e8 ad 67
           c9 59 d6 98
Round 1  6a 37 2c dc
         7e ac db 10
```

1e 82 cc 09
e9 30 bd f7

After SubBytes 02 9a 71 86
f3 91 b9 ca
72 13 4b 01
1e 04 7a 68
After ShiftRows 02 9a 71 86
91 b9 ca f3
4b 01 72 13
68 1e 04 7a
After MixColumns 8f e0 d1 70
8e ee 6c 34
bd 03 53 dd
0c 31 23 85
Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7
Round 2 53 7b 46 48
1e a7 92 b5
8a dc 21 c8
bc d8 1c 22
After SubBytes ed 21 5a 52
72 5c 4f d5
7e 86 fd e8
65 61 9c 93
After ShiftRows ed 21 5a 52
5c 4f d5 72
fd e8 7e 86
93 65 61 9c
After MixColumns 4b 1e cf 28
da f9 08 bb
fe 0a d0 88
b0 0e 87 21

Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
Round 3 99 57 11 ce
13 79 76 44
95 be 16 5b
07 50 e6 e7
After SubBytes ee 5b 82 8b
7d b6 38 1b
2a ae 47 39
c5 53 8e 94

After ShiftRows ee 5b 82 8b
b6 38 1b 7d
47 39 2a ae
94 c5 53 8e
After MixColumns d5 02 4b aa
c4 a5 99 16
71 45 38 38
eb 7d 0a 52
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
Round 4 15 8b 1c 1b
6b 8a c8 b8
ae 2e 95 46
d2 1a 0c 92
After SubBytes 59 3d 9c af
7f 7e e8 6c
e4 31 2a 5a
b5 a2 fe 4f
After ShiftRows 59 3d 9c af
7e e8 6c 7f
2a 5a e4 31
4f b5 a2 fe
After MixColumns 55 b6 d1 0b
94 ad d1 fc
a2 a5 de ab
21 84 68 43
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50
Round 5 79 13 23 48
c8 de f3 70
c7 ab 7d 76
d0 12 f8 13
After SubBytes b6 7d 26 52
e8 1d 0d 51
c6 62 ff 38
70 c9 41 7d
After ShiftRows b6 7d 26 52
1d 0d 51 e8
ff 38 c6 62
7d 70 c9 41
After MixColumns d2 a5 b0 a4
eb 5f 1c 7e
c9 90 a0 bd
d9 52 74 fe

Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
Round 6 8a 58 bf e8
76 b1 d0 3e
ff a8 3b fb
32 2f 99 43
After SubBytes 7e 6a 08 9b
38 c8 70 b2
16 c2 e2 0f
23 15 ee 1a
After ShiftRows 7e 6a 08 9b
c8 70 b2 38
e2 0f 16 c2
1a 23 15 ee
After MixColumns 47 68 de 49
d2 b8 58 58
47 61 a9 15
9c 87 96 8b
Round Key 71 8c 83 cf
c7 29 e5 a5
4c 74 ef a9
c2 bf 52 ef
Round 7 36 e4 5d 86
15 91 bd fd
0b 15 46 bc
5e 38 c4 64
After SubBytes 05 69 4c 44
59 81 7a 54
2b 59 5a 65
58 07 1c 43
After ShiftRows 05 69 4c 44
81 7a 54 59
5a 65 2b 59
43 58 07 1c
After MixColumns 8b 61 48 26
b1 6a 9e 01
f5 31 47 8b
52 14 a5 f4
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
Round 8 bc da 70 d1
a5 57 46 7c
66 d6 4f 2a
1a e3 00 be

```
After SubBytes  65 57 51 3e
                06 5b 5a 10
                33 f6 84 e5
                a2 11 63 ae
After ShiftRows  65 57 51 3e
                 5b 5a 10 06
                 84 e5 33 f6
                 ae a2 11 63
After MixColumns  0d 07 b0 e3
                  ea 75 35 50
                  c4 21 14 6a
                  37 19 f2 74
Round Key    48 f3 cb 3c
             26 1b c3 be
             45 a2 aa 0b
             20 d7 72 38
Round 9      45 f4 7b df
             cc 6e f6 ee
             81 83 be 61
             17 ce 80 4c
After SubBytes  6e bf 21 9e
                4b 9f 42 28
                0c ec ae ef
                f0 8b cd 29
After ShiftRows  6e bf 21 9e
                 9f 42 28 4b
                 ae ef 0c ec
                 29 f0 8b cd
After MixColumns  e1 bc bd db
                  8b e1 ee ea
                  cd 33 97 5a
                  d1 8c 4a 9f
Round Key    fd 0e c5 f9
             0d 16 d5 6b
             42 e0 4a 41
             cb 1c 6e 56
After SubBytes  9c 37 bc 93
                44 68 e2 0c
                73 66 c1 af
                a2 60 36 dd
After ShiftRows  9c 37 bc 93
                 68 e2 0c 44
                 c1 af 73 66
                 dd a2 60 36
Output  28 8d c3 15
        e6 7a 41 62
        32 bc 2a 7e
        8f ec 40 40
```

Lampiran-15. Analisis Enskripsi AES: ESTU FARDANI

ESTU FARDANI

Input bits 65 73 74 75
20 66 61 72
64 61 6e 69
00 00 00 00

Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98

w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96
w[18] = f2 22 a3 90

w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52
w[41] = ba 98 13 4e
w[42] = 7f 4d 59 20

w[43] = 86 26 18 76
Initial state 65 20 64 00
73 66 61 00
74 61 6e 00
75 72 69 00
Round Key 0f 47 0c af
15 d9 b7 7f
71 e8 ad 67
c9 59 d6 98
Round 1 6a 67 68 af
66 bf d6 7f
05 89 c3 67
bc 2b bf 98
After SubBytes 02 85 45 79
33 08 f6 d2
6b a7 2e 85
65 f1 08 46
After ShiftRows 02 85 45 79
08 f6 d2 33
2e 85 6b a7
46 65 f1 08
After MixColumns 74 f0 7d 08
26 83 b6 e5
9c cd 49 07
ac 2d 8f 0f
Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7
Round 2 a8 6b ea 30
b6 ca 48 64
ab 12 3b 12
1c c4 b0 a8
After SubBytes c2 7f 87 04
4e 74 52 43
62 c9 e2 c9
9c 1c e7 c2
After ShiftRows c2 7f 87 04
74 52 43 4e
e2 c9 62 c9
c2 9c 1c e7
After MixColumns 23 5d ae f4

d5 07 bb 3f
34 1b 24 f1
54 39 8b 5e
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
Round 3 f1 14 70 12
1c 87 c5 c0
5f af e2 22
e3 67 ea 98
After SubBytes a1 fa 51 c9
9c 17 a6 ba
cf 79 98 93
11 85 87 46
After ShiftRows a1 fa 51 c9
17 a6 ba 9c
98 93 cf 79
46 11 85 87
After MixColumns be 9c 3d c8
7a 12 f1 e6
57 52 fa 35
fb 02 97 b0
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
Round 4 7e 15 6a 79
d5 3d a0 48
88 39 57 4b
c2 65 91 70
After SubBytes f3 59 02 b6
03 27 e0 52
c4 12 5b b3
25 4d 81 51
After ShiftRows f3 59 02 b6
27 e0 52 03
5b b3 c4 12
51 25 4d 81
After MixColumns 9e 1f 7b e1
01 69 bc 07
91 ab 14 09

d0 f2 0a c9
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50
Round 5 b2 ba 89 a2
5d 1a 9e 8b
f4 a5 b7 d4
21 64 9a 99
After SubBytes 37 f4 a7 3a
4c a2 0b 3d
bf 06 a9 48
fd 43 b8 ee
After ShiftRows 37 f4 a7 3a
a2 0b 3d 4c
a9 48 bf 06
ee fd 43 b8
After MixColumns d4 5b ee 1e
66 c7 44 10
f5 73 3a a9
95 a5 f6 6f
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
Round 6 8c a6 e1 52
fb 29 88 50
c3 4b a1 ef
7e d8 1b d2
After SubBytes 64 24 f8 00
0f a5 c4 53
2e b3 32 df
f3 61 af b5
After ShiftRows 64 24 f8 00
a5 c4 53 0f
32 df 2e b3
b5 f3 61 af
After MixColumns bb 33 51 0d
d6 3e 4d 7f
61 4b 54 98
4a 8a ac f9
Round Key 71 8c 83 cf

c7 29 e5 a5
4c 74 ef a9
c2 bf 52 ef
Round 7 ca bf d2 c2
11 17 a8 da
2d 3f bb 31
88 35 fe 16
After SubBytes 74 08 b5 25
82 f0 c2 57
d8 75 ea c7
c4 96 bb 47
After ShiftRows 74 08 b5 25
f0 c2 57 82
ea c7 d8 75
47 c4 96 bb
After MixColumns 4e 4e c6 19
ed 01 fe 1e
82 08 e8 9b
08 8e 7c f5
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
Round 8 79 f5 fe ee
f9 3c 26 63
11 ef e0 3a
40 79 d9 bf
After SubBytes b6 e6 bb 28
99 eb f7 fb
82 df e1 80
09 b6 35 08
After ShiftRows b6 e6 bb 28
eb f7 fb 99
e1 80 82 df
08 09 b6 35
After MixColumns b8 5c 4f 0a
4b 81 7d 4e
9c 11 9e 4b
db 54 d8 54
Round Key 48 f3 cb 3c
26 1b c3 be
45 a2 aa 0b

20 d7 72 38
Round 9 f0 af 84 36
6d 9a be f0
d9 b3 34 40
fb 83 aa 6c
After SubBytes 8c 79 5f 05
3c b8 ae 8c
35 6d 18 09
0f ec ac 50
After ShiftRows 8c 79 5f 05
b8 ae 8c 3c
18 09 35 6d
50 0f ec ac
After MixColumns 98 1d e8 8f
9f 2a ef 66
f4 d4 96 0c
8f 32 9b 1d
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After SubBytes 4d 7d d8 38
4f eb 80 d7
4e 18 86 e3
1b 31 e6 b3
After ShiftRows 4d 7d d8 38
eb 80 d7 4f
86 e3 4e 18
b3 1b 31 e6
Output f9 c7 a7 be
65 18 9a 69
75 f0 17 00
e1 55 11 90

Lampiran-16. Analisis Enskripsi AES: RAHMATULLAH PROYO KUSUMA

RAHMATULLAH PRIYO KUSUMA

Input bits 72 61 68 6d
61 74 75 6c
6c 61 68 20
70 72 69 79
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96
w[18] = f2 22 a3 90

w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52
w[41] = ba 98 13 4e
w[42] = 7f 4d 59 20

w[43] = 86 26 18 76
Initial state 72 61 6c 70
61 74 61 72
68 75 68 69
6d 6c 20 79
Round Key 0f 47 0c af
15 d9 b7 7f
71 e8 ad 67
c9 59 d6 98
Round 1 7d 26 60 df
74 ad d6 0d
19 9d c5 0e
a4 35 f6 e1
After SubBytes ff f7 d0 9e
92 95 f6 d7
d4 5e a6 ab
49 96 42 f8
After ShiftRows ff f7 d0 9e
95 f6 d7 92
a6 ab d4 5e
f8 49 96 42
After MixColumns 1f 16 9b 96
c7 af 94 01
2e 97 15 76
c2 cd 5f f1
Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7

Round 2 c3 8d 0c ae
57 e6 6a 80
19 48 67 63
72 24 60 56
After SubBytes 2e 5d fe e4
5b 8e 02 cd
d4 52 85 fb
40 36 d0 b1
After ShiftRows 2e 5d fe e4
8e 02 cd 5b
85 fb d4 52
b1 40 36 d0

After MixColumns e1 07 49 bc
0c 0f 2e 74
79 72 da 70
00 9e 6c 85
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
Round 3 33 4e 97 5a
c5 8f 50 8b
12 c6 1c a3
b7 c0 0d 43
After SubBytes c3 2f 88 be
a6 73 53 3d
c9 b4 9c 0a
a9 ba d7 1a
After ShiftRows c3 2f 88 be
73 53 3d a6
9c 0a c9 b4
1a a9 ba d7
After MixColumns 8e 08 3f f5
80 3e 08 f9
bd 88 e9 09
85 61 18 7e
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
Round 4 4e 81 68 44
2f 11 59 57
62 e3 44 77
bc 06 1e be
After SubBytes 2f 0c 45 1b
15 82 cb 5b
aa 11 1b f5
65 6f 72 ae
After ShiftRows 2f 0c 45 1b
82 cb 5b 15
1b f5 aa 11
ae 65 6f 72
After MixColumns 76 ce a2 6a
b3 e0 79 70

72 99 e0 ba
af e0 e0 cd
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50
Round 5 5a 6b 50 29
ef 93 5b fc
17 97 43 67
5e 76 70 9d
After SubBytes be 7f 53 a5
df dc 39 b0
f0 88 1a 85
58 38 51 5e
After ShiftRows be 7f 53 a5
dc 39 b0 df
1a 85 f0 88
5e 58 38 51
After MixColumns 5c 68 a5 f2
6d c1 1b d2
b4 bf 50 82
a3 8d c5 01
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
Round 6 04 95 aa be
f0 2f d7 92
82 87 cb c4
48 f0 28 bc
After SubBytes f2 2a ac ae
8c 15 0e 4f
13 17 1f 1c
52 8c 34 65
After ShiftRows f2 2a ac ae
15 0e 4f 8c
1f 1c 13 17
65 52 8c 34
After MixColumns ba 08 0d eb
9c 40 8b a0
76 ea 4a 50
cd c8 b0 1a

Round Key 71 8c 83 cf
c7 29 e5 a5
4c 74 ef a9
c2 bf 52 ef
Round 7 cb 84 8e 24
5b 69 6e 05
3a 9e a5 f9
0f 77 e2 f5
After SubBytes 1f 5f 19 36
39 f9 9f 6b
80 0b 06 99
76 f5 98 e6
After ShiftRows 1f 5f 19 36
f9 9f 6b 39
06 99 80 0b
e6 76 f5 98
After MixColumns ce eb fa b4
1a bc a1 c1
db 73 6d aa
09 0b 31 43
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
Round 8 f9 50 c2 43
0e 81 79 bc
48 94 65 0b
41 fc 94 09
After SubBytes 99 53 25 1a
ab 0c b6 65
52 22 4d 2b
83 b0 22 01
After ShiftRows 99 53 25 1a
0c b6 65 ab
4d 2b 52 22
01 83 b0 22
After MixColumns 71 cf 07 d2
57 da a9 13
0c 2d 2f 93
f3 75 23 e3
Round Key 48 f3 cb 3c
26 1b c3 be

45 a2 aa 0b
20 d7 72 38
Round 9 39 3c cc ee
71 c1 6a ad
49 8f 85 98
d3 a2 51 db
After SubBytes 12 eb 4b 28
a3 78 02 95
3b 73 97 46
66 3a d1 b9
After ShiftRows 12 eb 4b 28
78 02 95 a3
97 46 3b 73
b9 66 3a d1
After MixColumns 82 eb 33 0c
f9 43 0d 31
8f cf e6 05
b0 ae 07 11
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After SubBytes d2 d9 42 e6
bf fc 61 be
bd 15 91 1b
21 37 f9 a0
After ShiftRows d2 d9 42 e6
fc 61 be bf
91 1b bd 15
a0 21 37 f9
Output 66 63 3d 60
72 f9 f3 99
62 c08 e4 0d
f2 6f 17 8f

Lampiran-17. Analisis Enskripsi AES: RIZKI TUNJUNG SARI

RIZKI TUNJUNG SARI

Input bits 72 69 7a 6b
69 20 74 75
6e 6a 75 6e
67 20 73 61
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1

w[17] = a5 73 0e 96
w[18] = f2 22 a3 90
w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52

```
w[41] =   ba 98 13 4e
w[42] =   7f 4d 59 20
w[43] =   86 26 18 76
Initial state  72 69 6e 67
               69 20 6a 20
               7a 74 75 73
               6b 75 6e 61
Round Key  0f 47 0c af
           15 d9 b7 7f
           71 e8 ad 67
           c9 59 d6 98
Round 1  7d 2e 62 c8
         7c f9 dd 5f
         0b 9c d8 14
         a2 2c b8 f9
After SubBytes  ff 31 aa e8
                10 99 c1 cf
                2b de 61 fa
                3a 71 6c 99
After ShiftRows  ff 31 aa e8
                 99 c1 cf 10
                 61 fa 2b de
                 99 3a 71 6c
After MixColumns  ad fa 5f 49
                  ec 87 23 dd
                  14 51 a0 eb
                  cb 1c e3 35
Round Key  dc 9b 97 38
           90 49 fe 81
           37 df 72 15
           b0 e9 3f a7
Round 2  71 61 c8 71
         7c ce dd 5c
         23 8e d2 fe
         7b f5 dc 92
After SubBytes  a3 ef e8 a3
                10 8b c1 4a
                26 19 b5 bb
                21 e6 86 4f
After ShiftRows  a3 ef e8 a3
                 8b c1 4a 10
                 b5 bb 26 19
```

4f 21 e6 86
After MixColumns 21 07 d5 f2
25 81 f0 2e
88 20 df 10
5e 12 98 e0
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
Round 3 f3 4e 0b 14
ec 01 8e d1
e3 94 19 c3
e9 4c f9 26
After SubBytes 0d 2f 2b fa
ce 7c 19 3e
11 22 d4 2e
1e 29 99 f7
After ShiftRows 0d 2f 2b fa
7c 19 3e ce
d4 2e 11 22
f7 1e 29 99
After MixColumns bd 45 2c 1d
65 71 4d 82
c0 48 4c c0
4a 7a 00 d0

Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
Round 4 7d cc 7b ac
ca 5e 1c 2c
1f 23 e1 be
73 1d 06 10
After SubBytes ff 4b 21 91
74 58 9c 71
c0 26 f8 ae
8f a4 6f ca
After ShiftRows ff 4b 21 91
58 9c 71 74
f8 ae c0 26
ca 8f a4 6f

After MixColumns 3f 08 b5 ec
96 0e 3c 7c
09 1a 3c 18
35 ea 81 24
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50
Round 5 13 ad 47 af
ca 7d 1e f0
6c 14 9f c5
c4 7c 11 74
After SubBytes 7d 95 a0 79
74 ff 72 8c
50 fa db a6
1c 10 82 92
After ShiftRows 7d 95 a0 79
ff 72 8c 74
db a6 50 fa
92 1c 10 82
After MixColumns a9 1d 94 16
7c 9c 43 06
82 94 bc 7f
9c 48 07 1a
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
Round 6 f1 e0 9b 5a
e1 72 8f 46
b4 ac 27 39
77 35 ea a7
After SubBytes a1 e1 14 be
f8 40 73 5a
8d 91 cc 12
f5 96 87 5c
After ShiftRows a1 e1 14 be
40 73 5a f8
cc 12 8d 91
5c f5 96 87
After MixColumns 09 ab dd 62
32 c4 ba 7a

86 b2 ee ed
cc a8 dc a5
Round Key 71 8c 83 cf
c7 29 e5 a5
4c 74 ef a9
c2 bf 52 ef
Round 7 78 27 5e ad
f5 ed 5f df
ca c6 01 44
0e 17 8e 4a
After SubBytes bc cc 58 95
e6 55 cf 9e
74 b4 7c 1b
ab f0 19 d6
After ShiftRows bc cc 58 95
55 cf 9e e6
7c 1b 74 b4
d6 ab f0 19
After MixColumns 36 79 8d ad
44 cf 13 9c
70 d3 25 2b
41 d6 f9 c4
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
Round 8 01 c2 b5 5a
50 f2 cb e1
e3 34 2d 8a
09 21 5c 8e
After SubBytes 7c 25 d5 be
53 89 1f f8
11 18 d8 7e
01 fd 4a 19
After ShiftRows 7c 25 d5 be
89 1f f8 53
d8 7e 11 18
19 01 fd 4a
After MixColumns b9 14 4e c0
1f 98 f0 7a
75 c5 13 03
e7 0c 6c 06
Round Key 48 f3 cb 3c
26 1b c3 be

45 a2 aa 0b
20 d7 72 38
Round 9 f1 e7 85 fc
39 83 33 c4
30 67 b9 08
c7 db 1e 3e
After SubBytes a1 94 97 b0
12 ec c3 1c
04 85 56 30
c6 b9 72 b2
After ShiftRows a1 94 97 b0
ec c3 1c 12
56 30 04 85
b2 c6 b9 72

After MixColumns 92 9b ac ba
2a 9f 1a 72
2c 66 53 25
3d c3 d3 b8
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After SubBytes a8 2a f9 1a
cc a7 8a d4
9f 44 d4 43
42 9e 7a 28
After ShiftRows a8 2a f9 1a
a7 8a d4 cc
d4 43 9f 44
28 42 9e 7a
Output 1c 90 86 9c
29 12 99 ea
27 50 c6 5c
7a 0c be 0c

Lampiran-18. Analisis Deskripsi AES: YOGI SURYA NUGRAHA

YOGI SURYA NUGRAHA

Input bits 79 6f 67 69
20 73 75 72
79 61 20 6e
75 67 72 61
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96
w[18] = f2 22 a3 90
w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb

```
w[21] =   fd ee 38 7d
w[22] =   0f cc 9b ed
w[23] =   4c 40 46 bd
RotWord()=  40 46 bd 4c
SubWord()=  09 5a 7a 29
 ^ Rcon()=  29 5a 7a 29
w[24] =   71 c7 4c c2
w[25] =   8c 29 74 bf
w[26] =   83 e5 ef 52
w[27] =   cf a5 a9 ef
RotWord()=  a5 a9 ef cf
SubWord()=  06 d3 df 8a
 ^ Rcon()=  46 d3 df 8a
w[28] =   37 14 93 48
w[29] =   bb 3d e7 f7
w[30] =   38 d8 08 a5
w[31] =   f7 7d a1 4a
RotWord()=  7d a1 4a f7
SubWord()=  ff 32 d6 68
 ^ Rcon()=  7f 32 d6 68
w[32] =   48 26 45 20
w[33] =   f3 1b a2 d7
w[34] =   cb c3 aa 72
w[35] =   3c be 0b 38
RotWord()=  be 0b 38 3c
SubWord()=  ae 2b 07 eb
 ^ Rcon()=  b5 2b 07 eb
w[36] =   fd 0d 42 cb
w[37] =   0e 16 e0 1c
w[38] =   c5 d5 4a 6e
w[39] =   f9 6b 41 56
RotWord()=  6b 41 56 f9
SubWord()=  7f 83 b1 99
 ^ Rcon()=  49 83 b1 99
w[40] =   b4 8e f3 52
w[41] =   ba 98 13 4e
w[42] =   7f 4d 59 20
w[43] =   86 26 18 76
Initial state  79 20 79 75
                6f 73 61 67
               67 75 20 72
               69 72 6e 61
Round Key  b4 ba 7f 86
               8e 98 4d 26
              f3 13 59 18
             52 4e 20 76
Round 9  cd 9a 06 f3
            e1 eb 2c 41
```

94 66 79 6a
3b 3c 4e 17
After InvShiftRows cd 9a 06 f3
41 e1 eb 2c
79 6a 94 66
3c 4e 17 3b
After SubBytes 80 37 a5 7e
f8 e0 3c 42
af 58 e7 d3
6d b6 87 49
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After AddRoundKey 7d 39 60 87
f5 f6 e9 29
ed b8 ad 92
a6 aa e9 1f
Round 8 81 e1 8f b4
13 6e 9e bc
8c c1 c3 e7
dd 93 1f cc
After InvShiftRows 81 e1 8f b4
bc 13 6e 9e
c3 e7 8c c1
93 1f cc dd
After SubBytes 91 e0 73 c6
78 82 45 df
33 b0 f0 dd
22 cb 27 c9
Round Key 48 f3 cb 3c
26 1b c3 be
45 a2 aa 0b
20 d7 72 38
After AddRoundKey d9 13 b8 fa
5e 99 86 61
76 12 5a d6
02 1c 55 f1
Round 7 6c d0 c3 4c
4f 7e e6 49
3e c2 43 03
ee e8 57 ba
After InvShiftRows 6c d0 c3 4c
49 4f 7e e6
43 03 3e c2
e8 57 ba ee
After SubBytes b8 60 33 5d
a4 92 8a f5

64 d5 d1 a8
c8 da c0 99
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
After AddRoundKey 8f db 0b aa
b0 af 52 88
f7 32 d9 09
80 2d 65 d3
Round 6 34 a4 50 2d
c0 ae 0f 9f
dc 9b 53 65
60 fa e9 2f
After InvShiftRows 34 a4 50 2d
9f c0 ae 0f
53 65 dc 9b
fa e9 2f 60
After SubBytes 28 1d 6c fa
6e 1f be fb
50 bc 93 e8
14 eb 4e 90
Round Key 71 8c 83 cf
c7 29 e5 a5
4c 74 ef a9
c2 bf 52 ef
After AddRoundKey 59 91 ef 35
a9 36 5b 5e
1c c8 7c 41
d6 54 1c 7f
Round 5 5c 43 c8 e3
ce ba 3c 2f
6d 6c e8 3d
c5 ae c8 a4
After InvShiftRows 5c 43 c8 e3
2f ce ba 3c
e8 3d 6d 6c
ae c8 a4 c5
After SubBytes a7 64 b1 4d
4e ec c0 6d
c8 8b b3 b8
be b1 1d 07
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
After AddRoundKey ff 99 be 01
d3 02 0c 2d

fe b3 28 fe
55 cc f0 ba
Round 4 70 99 b8 8d
74 eb 8e ff
64 60 fa a2
e7 f6 a6 b8
After InvShiftRows 70 99 b8 8d
ff 74 eb 8e
fa a2 64 60
f6 a6 b8 e7
After SubBytes d0 f9 9a b4
7d ca 3c e6
14 1a 8c 90
d6 c5 9a b0
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50
After AddRoundKey fc 5c 68 f7
21 b9 1e 6a
71 14 2f 4d
27 53 0a e0
Round 3 e0 73 7e a3
26 b8 d1 91
60 64 9f 79
2d 0d 63 7b
After InvShiftRows e0 73 7e a3
91 26 b8 d1
9f 79 60 64
0d 63 7b 2d
After SubBytes a0 8f 8a 71
ac 23 9a 51
6e af 90 8c
f3 00 03 fa
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
After AddRoundKey 60 06 dd c0
03 0c cb ff
b1 c4 3d f2
ca 67 05 3a
Round 2 17 a1 19 78
ad a6 6c d2
f6 2a a5 bf
54 84 fe e2
After InvShiftRows 17 a1 19 78
d2 ad a6 6c

a5 bf f6 2a
84 fe e2 54
After SubBytes 87 f1 8e c1
7f 18 c5 b8
29 f4 d6 95
4f 0c 3b fd
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
After AddRoundKey 55 b8 50 27
b6 98 bb 47
42 40 10 46
f8 52 5a 3b
Round 1 73 8c 58 8d
c1 8f 81 5b
d6 10 41 d6
3d 21 39 1d
After InvShiftRows 73 8c 58 8d
5b c1 8f 81
41 d6 d6 10
21 39 1d 3d
After SubBytes 8f f0 5e b4
57 dd 73 91
f8 4a 4a 7c
7b 5b de 8b
Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7
After AddRoundKey 53 6b c9 8c
c7 94 8d 10
cf 95 38 69
cb b2 e1 2c
After InvShiftRows 5a 19 b1 5d
59 9b 4c 4e
61 11 fd 4c
c1 03 cc ac
After SubBytes 46 8e 56 8d
15 e8 5d b6
d8 e3 21 5d
dd d5 27 aa
Output 49 c9 5a 22
00 31 ea c9
a9 0b 8c 3a
14 8c f1 32

Lampiran-19. Analisis Deskripsi AES: EKO PUJI LAKSONO

EKO PUJI LAKSONO

Input bits 65 6b 6f 20
70 75 6a 69
20 6c 61 6b
73 6f 6e 6f
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96

w[18] = f2 22 a3 90
w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
 ^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
 ^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
 ^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
 ^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
 ^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
 ^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52
w[41] = ba 98 13 4e

w[42] = 7f 4d 59 20
w[43] = 86 26 18 76
Initial state 65 70 20 73
6b 75 6c 6f
6f 6a 61 6e
20 69 6b 6f
Round Key b4 ba 7f 86
8e 98 4d 26
f3 13 59 18
52 4e 20 76
Round 9 d1 ca 5f f5
e5 ed 21 49
9c 79 38 76
72 27 4b 19
After InvShiftRows d1 ca 5f f5
49 e5 ed 21
38 76 9c 79
27 4b 19 72
After SubBytes 51 10 84 77
a4 2a 53 7b
76 0f 1c af
3d cc 8e 1e
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After AddRoundKey ac 1e 41 8e
a9 3c 86 10
34 ef 56 ee
f6 d0 e0 48
Round 8 55 46 5c d1
4a e9 6a 6f
58 8d a9 c1
80 3f ee 47
After InvShiftRows 55 46 5c d1
6f 4a e9 6a
a9 c1 58 8d
3f ee 47 80
After SubBytes ed 98 a7 51
06 5c eb 58
b7 dd 5e b4
25 99 16 3a

Round Key 48 f3 cb 3c
26 1b c3 be
45 a2 aa 0b
20 d7 72 38
After AddRoundKey a5 6b 6c 6d
20 47 28 e6
f2 7f f4 bf
05 4e 64 02
Round 7 3c 96 9c 98
c4 e6 8e 74
8f b8 b7 26
05 d5 71 fc
After InvShiftRows 3c 96 9c 98
74 c4 e6 8e
b7 26 8f b8
d5 71 fc 05
After SubBytes 6d 35 1c e2
ca 88 f5 e6
20 23 73 9a
b5 2c 55 36
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
After AddRoundKey 5a 8e 24 15
de b5 2d 9b
b3 c4 7b 3b
fd db f0 7c
Round 6 00 d4 af 71
48 eb 26 aa
66 d6 ef d6
e4 cd e4 c4
After InvShiftRows 00 d4 af 71
aa 48 eb 26
ef d6 66 d6
cd e4 c4 e4
After SubBytes 52 19 1b 2c
62 d4 3c 23
61 4a d3 4a
80 ae 88 ae
Round Key 71 8c 83 cf
c7 29 e5 a5

4c 74 ef a9
c2 bf 52 ef
After AddRoundKey 23 95 98 e3
a5 fd d9 86
2d 3e 3c e3
42 11 da 41
Round 5 ec 96 54 8c
ff b4 ec d8
2b b3 a5 19
d1 d6 ba 8a
After InvShiftRows ec 96 54 8c
d8 ff b4 ec
a5 19 2b b3
d6 ba 8a d1
After SubBytes 83 35 fd f0
2d 7d c6 83
29 8e 0b 4b
4a c0 cf 51
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
After AddRoundKey db c8 f2 bc
b0 93 0a c3
1f b6 90 0d
a1 bd 22 ec
Round 4 17 7b a6 b2
96 87 a9 fa
62 a5 50 24
36 09 15 f2
After InvShiftRows 17 7b a6 b2
fa 96 87 a9
50 24 62 a5
09 15 f2 36
After SubBytes 87 03 c5 3e
14 35 ea b7
6c a6 ab 29
40 2f 04 24
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50

After AddRoundKey ab a6 37 7d
48 46 c8 3b
09 a8 08 f4
b1 b9 94 74
Round 3 7d 7d 78 4f
b6 68 6e 35
69 8a 81 51
f9 6e f4 ed
After InvShiftRows 7d 7d 78 4f
35 b6 68 6e
81 51 69 8a
6e f4 ed f9
After SubBytes 13 13 c1 92
d9 79 f7 45
91 70 e4 cf
45 ba 53 69
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
After AddRoundKey d3 9a 96 23
76 56 a6 eb
4e 1b 49 b1
7c dd 55 a9
Round 2 83 71 f0 dc
6d 8c d5 46
2b e4 77 f5
52 13 7e bf
After InvShiftRows 83 71 f0 dc
46 6d 8c d5
77 f5 2b e4
13 7e bf 52
After SubBytes 41 2c 17 93
98 b3 f0 b5
02 77 0b ae
82 8a f4 48
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
After AddRoundKey 93 65 c9 75
51 33 8e 4a

69 c3 cd 7d
35 d4 95 8e

Round 1 cb 18 b0 dd
a8 06 83 ef
16 3c 8a 56
eb 63 a6 a8

After InvShiftRows cb 18 b0 dd
ef a8 06 83
8a 56 16 3c
63 a6 a8 eb

After SubBytes 59 34 fc c9
61 6f a5 41
cf b9 ff 6d
00 c5 6f 3c

Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7

After AddRoundKey 85 af 6b f1
f1 26 5b c0
f8 66 8d 78
b0 2c 50 9b

After InvShiftRows 45 2e 7a 99
c4 3b 0f 04
5d af 40 7a
98 ce 20 02

After SubBytes 68 c3 bd f9
88 49 fb 30
8d 1b 72 bd
e2 ec 54 6a

Output 67 84 b1 56
9d 90 4c 4f
fc f3 df da
2b b5 82 f2

Lampiran-20. Analisis Deskripsi AES: ESTU FARDANI

ESTU FARDANI

Input bits 65 73 74 75
20 66 61 72
64 61 6e 69
00 00 00 00
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96

w[18] = f2 22 a3 90
w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
 ^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
 ^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
 ^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
 ^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
 ^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
 ^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52
w[41] = ba 98 13 4e

w[42] = 7f 4d 59 20
w[43] = 86 26 18 76
Initial state 65 20 64 00
73 66 61 00
74 61 6e 00
75 72 69 00
Round Key b4 ba 7f 86
8e 98 4d 26
f3 13 59 18
52 4e 20 76
Round 9 d1 9a 1b 86
fd fe 2c 26
87 72 37 18
27 3c 49 76
After InvShiftRows d1 9a 1b 86
26 fd fe 2c
37 18 87 72
3c 49 76 27
After SubBytes 51 37 44 dc
23 21 0c 42
b2 34 ea 1e
6d a4 0f 3d
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After AddRoundKey ac 39 81 25
2e 37 d9 29
f0 d4 a0 5f
a6 b8 61 6b
Round 8 f6 e3 88 2d
b1 bf c0 35
19 ca 80 27
8a f4 51 07
After InvShiftRows f6 e3 88 2d
35 b1 bf c0
80 27 19 ca
f4 51 07 8a
After SubBytes d6 4d 97 fa
d9 56 f4 1f
3a 3d 8e 10
ba 70 38 cf

Round Key 48 f3 cb 3c
26 1b c3 be
45 a2 aa 0b
20 d7 72 38
After AddRoundKey 9e be 5c c6
ff 4d 37 a1
7f 9f 24 1b
9a a7 4a f7
Round 7 3d 0e 5c ee
a3 be d3 32
cf a2 2e 3e
d5 d9 a4 69
After InvShiftRows 3d 0e 5c ee
32 a3 be d3
2e 3e cf a2
d9 a4 69 d5
After SubBytes 8b d7 a7 99
a1 71 5a a9
c3 d1 5f 1a
e5 1d e4 b5
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
After AddRoundKey bc 6c 9f 6e
b5 4c 82 d4
50 36 57 bb
ad ea 41 ff
Round 6 26 02 fb 37
11 4b 41 e9
39 bb 25 05
Fa 0e 94 25
After InvShiftRows 26 02 fb 37
e9 11 4b 41
25 05 39 bb
0e 94 25 fa
After SubBytes 23 6a 63 b2
eb e3 cc f8
c2 36 5b fe
d7 e7 c2 14
Round Key 71 8c 83 cf
c7 29 e5 a5

4c 74 ef a9
c2 bf 52 ef
After AddRoundKey 52 e6 e0 7d
2c ca 29 5d
8e 42 b4 57
15 58 90 fb
Round 5 7f 85 e6 15
1b 22 1e 67
72 4d 73 3c
f3 dc 66 c2
After InvShiftRows 7f 85 e6 15
67 1b 22 1e
73 3c 72 4d
dc 66 c2 f3
After SubBytes 6b 67 f5 2f
0a 44 94 e9
8f 6d 1e 65
93 d3 a8 7e
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
After AddRoundKey 33 9a fa 63
97 aa 58 a9
b9 55 85 23
78 ae 45 c3
Round 4 1e 22 1d 96
3a 96 d2 74
5e 60 a6 82
1f 1f 0b 4a
After InvShiftRows 1e 22 1d 96
74 3a 96 d2
a6 82 5e 60
1f 0b 4a 1f
After SubBytes e9 94 de 35
ca a2 35 7f
c5 11 9d 90
cb 9e 5c cb
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50

After AddRoundKey c5 31 2c 76
96 d1 17 f3
a0 1f 3e 4d
3a 08 cc 9b
Round 3 37 5c c9 76
a7 11 df d2
db 87 52 eb
82 3d 8d 1c
After InvShiftRows 37 5c c9 76
d2 a7 11 df
52 eb db 87
3d 8d 1c 82
After SubBytes b2 a7 12 0f
7f 89 e3 ef
48 3c 9f ea
8b b4 c4 11
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
After AddRoundKey 72 2e 45 be
d0 a6 b2 41
97 57 32 94
b2 d3 c2 d1
Round 2 47 b6 48 ee
1e fc 4d 9b
b7 d7 31 ab
69 91 33 64
After InvShiftRows 47 b6 48 ee
9b 1e fc 4d
31 ab b7 d7
91 33 64 69
After SubBytes 16 79 d4 99
e8 e9 55 65
2e 0e 20 0d
ac 66 8c e4
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
After AddRoundKey c4 30 0a 7f
21 69 2b 9a

45 ba e6 de
1b 38 ed 22

Round 1 33 c5 b4 cd
15 d2 fe 15
df e2 0c 5e
42 2e 6c 9f

After InvShiftRows 33 c5 b4 cd
15 15 d2 fe
0c 5e df e2
2e 6c 9f 42

After SubBytes 66 07 c6 80
2f 2f 7f 0c
81 9d ef 3b
c3 b8 6e f6

Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7

After AddRoundKey ba 9c 51 b8
bf 66 81 8d
b6 42 9d 2e
73 51 51 51

After InvShiftRows 1a c6 0b 90
a1 2a 12 28
ff 92 8d d1
ec c0 e9 7d

After SubBytes 43 c7 9e 96
f1 95 39 ee
7d 74 b4 51
83 1f eb 13

Output 4c 80 92 39
e4 4c 8e 91
0c 9c 19 36
4a 46 3d 8b

Lampiran-21. Analisis Deskripsi AES: RAHMATULLAH PRIYO KUSUMA

RAHMATULLAH PRIYO KUSUMA

Input bits 72 61 68 6d
61 74 75 6c
6c 61 68 20
70 72 69 79

Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98

w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
cw[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96
w[18] = f2 22 a3 90

w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
 ^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
 ^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
 ^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
 ^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
 ^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
 ^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52
w[41] = ba 98 13 4e
w[42] = 7f 4d 59 20

w[43] = 86 26 18 76
Initial state 72 61 6c 70
61 74 61 72
68 75 68 69
6d 6c 20 79
Round Key b4 ba 7f 86
8e 98 4d 26
f3 13 59 18
52 4e 20 76
Round 9 c6 db 13 f6
ef ec 2c 54
9b 66 31 71
3f 22 00 0f
After InvShiftRows c6 db 13 f6
54 ef ec 2c
31 71 9b 66
22 00 0f 3f
After SubBytes c7 9f 82 d6
fd 61 83 42
2e 2c e8 d3
94 52 fb 25
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After AddRoundKey 3a 91 47 2f
f0 77 56 29
6c cc a2 92
5f 4e 95 73
Round 8 86 40 d1 7f
29 97 89 a9
39 d5 78 17
6f 66 06 26
After InvShiftRows 86 40 d1 7f
a9 29 97 89
78 17 39 d5
66 06 26 6f
After SubBytes dc 72 51 6b
b7 4c 85 f2
c1 87 5b b5
d3 a5 23 06
Round Key 48 f3 cb 3c

26 1b c3 be
45 a2 aa 0b
20 d7 72 38
After AddRoundKey 94 81 9a 57
91 57 46 4c
84 25 f1 be
f3 72 51 3e
Round 7 11 75 3f c7
e7 c2 de 4f
e5 c8 ac 03
61 fe 31 10
After InvShiftRows 11 75 3f c7
4f e7 c2 de
ac 03 e5 c8
fe 31 10 61
After SubBytes e3 3f 25 31
92 b0 a8 9c
aa d5 2a b1
0c 2e 7c d8
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
After AddRoundKey d4 84 1d c6
86 8d 70 e1
39 32 22 10
44 d9 d9 92
Round 6 a5 cb 71 07
8a 10 0c 35
16 a2 79 80
16 9b 92 17
After InvShiftRows a5 cb 71 07
35 8a 10 0c
79 80 16 a2
9b 92 17 16
After SubBytes 29 59 2c 38
d9 cf 7c 81
af 3a ff 1a
e8 74 87 ff
Round Key 71 8c 83 cf
c7 29 e5 a5
4c 74 ef a9

c2 bf 52 ef
After AddRoundKey 58 d5 af f7
1e e6 99 24
e3 4e 10 b3
2a cb d5 10
Round 5 95 98 23 9c
b4 68 91 1c
2b 74 61 38
85 32 20 c8
After InvShiftRows 95 98 23 9c
1c b4 68 91
61 38 2b 74
32 20 c8 85
After SubBytes ad e2 32 1c
c4 c6 f7 ac
d8 76 0b ca
a1 54 b1 67
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd

After AddRoundKey f5 1f 3d 50
59 28 3b ec
ee 4e 90 8c
4a 29 5c da
Round 4 92 c8 73 95
28 06 31 0f
99 39 51 86
2b a7 d9 f6
After InvShiftRows 92 c8 73 95
0f 28 06 31
51 86 99 39
a7 d9 f6 2b
After SubBytes 74 b1 8f ad
fb ee a5 2e
70 dc f9 5b
89 e5 d6 0b
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50

After AddRoundKey 58 14 7d ee
a7 9d 87 a2
15 d2 5a 86
78 73 46 5b
Round 3 fc 5b 99 b8
e7 e5 98 56
8e cd 69 e9
07 5b 8e 96
After InvShiftRows fc 5b 99 b8
56 e7 e5 98
69 e9 8e cd
5b 8e 96 07
After SubBytes 55 57 f9 9a
b9 b0 2a e2
e4 eb e6 80
57 e6 35 38
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
After AddRoundKey 95 de ae 2b
16 9f 7b 4c
3b 80 4b fe
6e 81 33 f8
Round 2 3a 49 14 d8
8b af 92 91
23 97 b0 cf
44 31 9b e7
After InvShiftRows 3a 49 14 d8
91 8b af 92
b0 cf 23 97
31 9b e7 44
After SubBytes a2 a4 9b 2d
ac ce 1b 74
fc 5f 32 85
2e e8 b0 86
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
After AddRoundKey 70 ed 45 cb
65 4e 65 8b

97 eb f4 56
99 b6 d1 40
Round 1 28 e7 da d9
84 9d 97 fb
f9 06 61 e8
4e 82 29 9c
After InvShiftRows 28 e7 da d9
fb 84 9d 97
61 e8 f9 06
82 29 9c 4e
After SubBytes ee b0 7a e5
63 4f 75 85
d8 c8 69 a5
11 4c 1c b6
Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7
After AddRoundKey 32 2b ed dd
f3 06 8b 04
ef 17 1b b0
a1 a5 23 11
After InvShiftRows 69 8a 4c 4e
b6 03 95 be
06 d3 b1 93
13 aa 53 54
After SubBytes e4 cf 5d b6
79 d5 ad 5a
a5 a9 56 22
82 62 50 fd
Output eb 88 51 19
6c 0c 1a 25
d4 41 fb 45
4b 3b 86 65

Lampiran-22. Analisis Deskripsi AES: RIZKI TUNJUNG SARI

RIZKI TUNJUNG SARI

Input bits 72 69 7a 6b
69 20 74 75
6e 6a 75 6e
67 20 73 61
Key bits 0f 15 71 c9
47 d9 e8 59
0c b7 ad d6
af 7f 67 98
w[0] = 0f 15 71 c9
w[1] = 47 d9 e8 59
w[2] = 0c b7 ad d6
w[3] = af 7f 67 98
RotWord()= 7f 67 98 af
SubWord()= d2 85 46 79
^ Rcon()= d3 85 46 79
w[4] = dc 90 37 b0
w[5] = 9b 49 df e9
w[6] = 97 fe 72 3f
w[7] = 38 81 15 a7
RotWord()= 81 15 a7 38
SubWord()= 0c 59 5c 07
^ Rcon()= 0e 59 5c 07
w[8] = d2 c9 6b b7
w[9] = 49 80 b4 5e
w[10] = de 7e c6 61
w[11] = e6 ff d3 c6
RotWord()= ff d3 c6 e6
SubWord()= 16 66 b4 8e
^ Rcon()= 12 66 b4 8e
w[12] = c0 af df 39
w[13] = 89 2f 6b 67
w[14] = 57 51 ad 06
w[15] = b1 ae 7e c0
RotWord()= ae 7e c0 b1
SubWord()= e4 f3 ba c8
^ Rcon()= ec f3 ba c8
w[16] = 2c 5c 65 f1
w[17] = a5 73 0e 96

w[18] = f2 22 a3 90
w[19] = 43 8c dd 50
RotWord()= 8c dd 50 43
SubWord()= 64 c1 53 1a
^ Rcon()= 74 c1 53 1a
w[20] = 58 9d 36 eb
w[21] = fd ee 38 7d
w[22] = 0f cc 9b ed
w[23] = 4c 40 46 bd
RotWord()= 40 46 bd 4c
SubWord()= 09 5a 7a 29
^ Rcon()= 29 5a 7a 29
w[24] = 71 c7 4c c2
w[25] = 8c 29 74 bf
w[26] = 83 e5 ef 52
w[27] = cf a5 a9 ef
RotWord()= a5 a9 ef cf
SubWord()= 06 d3 df 8a
^ Rcon()= 46 d3 df 8a
w[28] = 37 14 93 48
w[29] = bb 3d e7 f7
w[30] = 38 d8 08 a5
w[31] = f7 7d a1 4a
RotWord()= 7d a1 4a f7
SubWord()= ff 32 d6 68
^ Rcon()= 7f 32 d6 68
w[32] = 48 26 45 20
w[33] = f3 1b a2 d7
w[34] = cb c3 aa 72
w[35] = 3c be 0b 38
RotWord()= be 0b 38 3c
SubWord()= ae 2b 07 eb
^ Rcon()= b5 2b 07 eb
w[36] = fd 0d 42 cb
w[37] = 0e 16 e0 1c
w[38] = c5 d5 4a 6e
w[39] = f9 6b 41 56
RotWord()= 6b 41 56 f9
SubWord()= 7f 83 b1 99
^ Rcon()= 49 83 b1 99
w[40] = b4 8e f3 52
w[41] = ba 98 13 4e

w[42] = 7f 4d 59 20
w[43] = 86 26 18 76
Initial state 72 69 6e 67
69 20 6a 20
7a 74 75 73
6b 75 6e 61
Round Key b4 ba 7f 86
8e 98 4d 26
f3 13 59 18
52 4e 20 76
Round 9 c6 d3 11 e1
e7 b8 27 06
89 67 2c 6b
39 3b 4e 17
After InvShiftRows c6 d3 11 e1
06 e7 b8 27
2c 6b 89 67
3b 4e 17 39
After SubBytes c7 a9 e3 e0
a5 b0 9a 3d
42 05 f2 0a
49 b6 87 5b
Round Key fd 0e c5 f9
0d 16 d5 6b
42 e0 4a 41
cb 1c 6e 56
After AddRoundKey 3a a7 26 19
a8 a6 4f 56
00 e5 b8 4b
82 aa e9 0d
Round 8 7d be 59 95
db 18 f7 5a
67 60 b7 d5
d1 88 21 13
After InvShiftRows 7d be 59 95
5a db 18 f7
b7 d5 67 60
88 21 13 d1
After SubBytes 13 5a 15 ad
46 9f 34 26
20 b5 0a 90
97 7b 82 51

Round Key 48 f3 cb 3c
26 1b c3 be
45 a2 aa 0b
20 d7 72 38
After AddRoundKey 5b a9 de 91
60 84 f7 98
65 17 a0 9b
b7 ac f0 69
Round 7 35 77 f3 c9
fb 53 d9 15
c2 fe 7f 2e
e5 4c 2c 09
After InvShiftRows 35 77 f3 c9
15 fb 53 d9
7f 2e c2 fe
4c 2c 09 e5
After SubBytes d9 02 7e 12
2f 63 50 e5
6b c3 a8 0c
5d 42 40 2a
Round Key 37 bb 38 f7
14 3d d8 7d
93 e7 08 a1
48 f7 a5 4a
After AddRoundKey ee b9 46 e5
3b 5e 88 98
f8 24 a0 ad
15 b5 e5 60
Round 6 e4 c5 cb 63
fd c0 c8 78
82 b4 20 50
a3 c7 a8 fb
After InvShiftRows e4 c5 cb 63
78 fd c0 c8
20 50 82 b4
c7 a8 fb a3
After SubBytes ae 07 59 00
c1 21 1f b1
54 6c 11 c6
31 6f 63 71
Round Key 71 8c 83 cf
c7 29 e5 a5

4c 74 ef a9
c2 bf 52 ef
After AddRoundKey df 8b da cf
06 08 fa 14
18 18 fe 6f
f3 d0 31 9e
Round 5 fe c9 dc b5
7a 40 25 9d
5d cc 3d 41
eb 0e 2b 43
After InvShiftRows fe c9 dc b5
9d 7a 40 25
3d 41 5d cc
0e 2b 43 eb
After SubBytes 0c 12 93 d2
75 bd 72 c2
8b f8 8d 27
d7 0b 64 3c
Round Key 58 fd 0f 4c
9d ee cc 40
36 38 9b 46
eb 7d ed bd
After AddRoundKey 54 ef 9c 9e
e8 53 be 82
bd c0 16 61
3c 76 89 81
Round 4 70 6a e4 2a
f1 a0 0b 0e
e3 51 0f 36
5f 91 5d ee
After InvShiftRows 70 6a e4 2a
0e f1 a0 0b
0f 36 e3 51
91 5d ee 5f
After SubBytes d0 58 ae 95
d7 2b 47 9e
fb 24 4d 70
ac 8d 99 84
Round Key 2c a5 f2 43
5c 73 22 8c
65 0e a3 dd
f1 96 90 50

After AddRoundKey fc fd 5c d6
8b 58 65 12
9e 2a ee ad
5d 1b 09 d4
Round 3 e2 85 a4 90
b7 f3 b7 60
f3 61 b1 8a
12 83 7c c7
After InvShiftRows e2 85 a4 90
60 b7 f3 b7
b1 8a f3 61
83 7c c7 12
After SubBytes 3b 67 1d 96
90 20 7e 20
56 cf 7e d8
41 01 31 39
Round Key c0 89 57 b1
af 2f 51 ae
df 6b ad 7e
39 67 06 c0
After AddRoundKey fb ee 4a 27
3f 0f 2f 8e
89 a4 d3 a6
78 66 37 f9
Round 2 3d 24 37 5b
c9 dd 49 1e
25 28 b7 2d
e4 f2 48 9e
After InvShiftRows 3d 24 37 5b
1e c9 dd 49
b7 2d 25 28
f2 48 9e e4
After SubBytes 8b a6 b2 57
e9 12 c9 a4
20 fa c2 ee
04 d4 df ae
Round Key d2 49 de e6
c9 80 7e ff
6b b4 c6 d3
b7 5e 61 c6
After AddRoundKey 59 ef 6c b1
20 92 b7 5b

4b 4e 04 3d
b3 8a be 68
Round 1 06 a1 3e 48
69 57 aa 6b
0d 69 94 a1
e3 26 61 3d
After InvShiftRows 06 a1 3e 48
6b 69 57 aa
94 a1 0d 69
26 61 3d e3
After SubBytes a5 f1 d1 d4
05 e4 da 62
e7 f1 f3 e4
23 d8 8b 4d

Round Key dc 9b 97 38
90 49 fe 81
37 df 72 15
b0 e9 3f a7
After AddRoundKey 79 6a 46 ec
95 ad 24 e3
d0 2e 81 f1
93 31 b4 ea
After InvShiftRows 88 b6 6a 32
57 a7 b4 da
03 07 64 59
83 e4 76 e4
After SubBytes 97 79 58 a1
da 89 c6 7a
d5 38 8c 15
41 ae 0f ae
Output 98 3e 54 0e
cf 50 71 05
a4 d0 21 72

88 f7 d9 36