SISTEM PEMBELAJARAN ELEKTRONIK UNTUK KRIPTOLOGI SIMETRIS DAN ASIMETRIS
(Studi Kasus Enkripsi)

E-LEARNING SYSTEM FOR SYMMETRIC AND ASYMMETRIC CRYPTOLOGY (Case Study Encryption)

EVANITA VERONICA MANULLANG
P2700211426

PROGRAM PASCASARJANA TEKNIK ELEKTRO
KONSENTRASI TEKNIK INFORMATIKA
UNIVERSITAS HASANUDDIN
MAKASSAR
2013

SISTEM PEMBELAJARAN ELEKTRONIK UNTUK KRIPTOLOGI SIMETRIS DAN ASIMETRIS
(Studi Kasus Enkripsi)

Tesis

Sebagai Salah Satu Syarat Untuk Mencapai Gelar Magister

Program Studi

Teknik Elektro

Disusun dan diajukan oleh

EVANITA VERONICA MANULLANG

Kepada

PROGRAM PASCASARJANA

UNIVERSITAS HASANUDDIN

MAKASSAR

2013

TESIS

SISTEM PEMBELAJARAN ELEKTRONIK UNTUK KRIPTOLOGI SIMETRIS DAN ASIMETRIS (STUDI KASUS ENKRIPSI)

Di susun dan di ajukan oleh

EVANITA V MANULLANG

Nomor Pokok P2700211426

Telah dipertahankan di depan Panitia Ujian Tesis

Pada tanggal 15 Agustus 2013

Dan dinyatakan telah memenuhi syarat

Menyetujui

Komisi Penasehat

Drs.Suarga,M.Sc.,M.Math.,Ph.D	Dr. Ir.Zahir Zainuddin, M.Sc
Ketua	Sekretaris

Ketua Program Studi	Direktur Program Pascasarjana
Teknik Elektro	Universitas Hasanuddin
Prof. Dr. Ir. Salama Manjang, MT	Prof. Dr. Ir. Mursalim,M.Sc

PERNYATAAN KEASLIAN TESIS

Yang bertanda tangan di bawah ini :

Nama : Evanita Veronica Manullang
Nomor mahasiswa : P2700211426
Program studi : Teknik Elektro

Menyatakan dengan sebenarnya bahwa tesis yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilalihan tulisan atau pemikiran orang lain. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan tesis ini hasil karya orang lain, saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, JULI 2013

Yang menyatakan,

Evanita Veronica Manullang

PRAKATA

Puji Syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa, karena atas berkat dan rahmat karunia-Nya penulis dapat menyelesaikan tesis ini. Tesis merupakan salah satu syarat kelulusan di Jurusan Teknik Informatika Strata Dua pada Fakultas Teknik Elektro Universitas Hasanuddin Makassar.

Dalam menyelesaikan tesis ini, penulis sudah berusaha sebaik mungkin, namun penulis hanyalah insan yang tidak sempurna dan tidak terlepas dari keterbatasan, penulis menyadari bahwa masih banyak terdapat kesalahan dan kesilapan dalam menyajikan isi dari tesis ini. Untuk itu penulis dengan hati terbuka akan menerima saran dan kritik dalam upaya menyempurnakan tesis ini nantinya.

Terwujudnya tesis ini tidak terlepas dari bantuan dan bimbingan dari berbagai pihak, untuk itu pada kesempatan ini penulis dengan tulus dan ikhlas menyampaikan ucapan terima kasih sebesar-besarnya kepada:

1. Bapak Prof. Dr. dr. Idrus A. Paturusi, selaku Rektor Universitas Hasanuddin Makassar.
2. Bapak Prof. Dr. Mursalim, M.Sc., selaku Direktur Program Pascasarjana Universitas Hasanuddin Makassar.
3. Bapak Prof. Dr. Ir. Salama Manjang, MT., selaku Ketua Program Studi Teknik Elektro Universitas Hasanuddin Makassar.
4. Bapak Drs. Suarga, M.Sc., M.Math., Ph.D., selaku Ketua Komisi Penasehat dan Dr. Ir. Zahir Zainuddin, M.Sc., selaku Anggota Komisi Penasehat yang telah membimbing, mengarahkan serta memberi saran bagi penulis dalam menyelesaikan tesis ini.
5. Bapak Dr. Elyas Palentei,ST.,M.Eng, Dr.-Ing. Faisal Arya Samman, ST.,MT dan Dr.Adnan, ST.,MT, selaku Dosen penguji yang telah mengarahkan dan memberi saran bagi penulis dalam menyelesaikan tesis ini.

6. Kepada seluruh staf Administrasi Program Pascasarjana dan Fakultas Teknik Elektro Universitas Hasanuddin Makassar.
7. Seluruh unsur pimpinan, dosen dan karyawan Universitas Sains dan Teknologi Jayapura.
8. Penghargaan yang setinggi-tingginya kepada Ayahanda dan Ibunda yang tercinta yang telah banyak mendoakan dan memberikan baik materil, spritual, motivasi serta harapan-harapan Ayah dan Bunda kepada penulis agar bisa menyelesaikan tesis ini.
9. Kepada seluruh teman-teman PPs-UH Teknik Elektro angkatan 2011, terima kasih telah menjadi sahabat yang memberikan dukungan dan semangat kebersamaan kepada penulis.
10. Semua pihak yang telah turut membantu penyelesaian tesis ini yang tidak sempat penulis sebutkan satu persatu.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, semoga bantuan tersebut mendapat amal yang berlipat ganda. Dan penulis berharap semoga tesis ini bermanfaat bagi pembaca terutama bagi penulis sendiri.

Makassar, Juli 2013
Penulis,

Evanita Manullang

ABSTRAK

Evanita V. Manullang. Sistem Pembelajaran Elektronik untuk Kriptografi Simetris dan Asimetris (Studi Kasus Enkripsi).
(dibimbing oleh **Suarga** dan **Zahir zainuddin**).

Penelitian ini bertujuan menghasilkan sistem pembelajaran elektonik untuk kriptolgrafi simetris dan asimetris dengan menampilkan proses enkripsi, sehingga dapat membantu pengguna dalam memahami materi pembelajaran kriptografi.

Metode yang digunakan dalam penelitian ini adalah metode deskriptif. Untuk mencapai tujuan yang dimaksud maka dibuat rancangan sistem pembelajaran yang terdiri dari pengenalan kriptografi, pemilihan jenis kriptografi, dan proses kriptografi yang memuat interaksi pengguna dengan aplikasi.

Hasil penelitian ini menunjukkan pengenalan teori kriptografi serta proses-proses dalam kriptografi yaitu Vigenere, Caesar, Transposisi, Rijndael secara rinci dan bertahap, dilengkapi dengan ruang interaksi antara pengguna dengan aplikasi, Pengguna dapat mempelajari kriptografi secara sederhana dan fleksibel sepanjang pengguna terhubung dengan internet. Kualitas sistem pembelajaran kriptografi yang dihasilkan sekitar 85% berdasarkan penilaian pengguna.

Kata kunci : Pembelajaran Elektronik, Kriptografi, Simetris, Asimetris, Enkripsi.

ABSTRACT

Evanita V. Manullang. E-Learning System for Symmetric and Asymmetric Cryptography (Encryption Case Study). (Supervised by **Suarga** and **Zahir Zainuddin**).

This research aims to produce electronic learning system for cryptography symmetric and asymmetric encryption with the display process, so as to assist the user in understanding the learning material cryptography.

The method used in this research is descriptive method. To achieve the intended goal then made learning system design that consists of an introduction to cryptography, the choice of cryptography and cryptographic process that includes user interaction with the application.

Results of this study indicate the introduction of the theory of cryptography and cryptographic processes in the Vigenere, Caesar, Transposition, Rijndael in detail and in stages, equipped with a user interaction with the application, users can learn in a simple and flexible cryptography all users connected to the internet. System quality learning cryptography generated approximately 85% based on user ratings.

Keywords: E-Learning, Cryptography, Symmetric, Asymmetric, Encryption.

DAFTAR ISI

DAFTAR TABEL

nomor **halaman**

DAFTAR GAMBAR

nomor **halaman**

BAB I

PENDAHULUAN

Pada bab ini diuraikan mengenai latar belakang yang mendasari dilakukannya penelitian, perumusan masalah, ruang lingkup dan batasan penelitian serta tujuan dan manfaat yang diharapkan dari penelitian ini.

A. Latar Belakang

Seiring perkembangan Teknologi Informasi dan Komunikasi (TIK) yang makin pesat, kebutuhan akan suatu konsep dan mekanisme belajar mengajar berbasis TIK juga semakin meningkat. Konsep pembelajaran yang akhirnya dikenal dengan sebutan e-learning membawa pengaruh terjadinya proses tranformasi dari pembelajaran konvensional ke dalam bentuk digital, baik content maupun sistemnya. Ada banyak jenis dan bentuk e-learning dan pada penelitian ini digunakan model e-learning yang mendeskripsikan proses-proses secara rinci dimana pengguna dapat memberikan inputan yang kemudian akan diberikan penjelasan mengenai proses-proses yang terjadi sehingga menghasilkan output. Aplikasi e-learning yang akan dibuat berbasis web sehingga mudah untuk dikembangkan lebih lanjut.

Pada matakuliah keamanan komputer juga terdapat pokok bahasan mengenai kriptologi. Kriptologi adalah bidang ilmu yang membahas kriptografi dan kriptanalisis. Kriptografi adalah ilmu dan seni untuk menjaga

keamanan pesan [SCH96]. Kriptografi berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia), sedangkan Kriptanalisis adalah cara untuk memecahkan teknik kriptografi.

Dalam pokok bahasan kriptologi tersebut dijelaskan beberapa algoritma simetris dan asimetris. Algoritma simetris ada yang klasik dan modern sedangkan algoritma asimetris adalah algoritma modern yang sudah menggunakan proses komputasi yang rumit sehingga tidak mudah untuk dipecahkan.

Kurangnya penguasaan akan teori mengenai algoritma kriptografi, kurangnya kemampuan matematis dalam menguraikan proses dari algoritma ini dan terbatasnya waktu untuk menjelaskan secara detail menjadi penyebab kesulitan dalam mempelajari algoritma kriptologi.

Teknologi komputer yang berkembang saat ini sangat membantu manusia dalam proses pembelajaran berbasis komputer atau lebih dikenal dengan *e-learning*. Kelebihan yang didapat dari pembelajaran dengan menggunakan komputer adalah adanya interaksi dalam proses belajar. Perangkat lunak yang dibuat ini berusaha membantu mahasiswa/pembaca dalam proses pembelajaran kriptologi. Pada penelitian terdahulu telah dibuat alat pembelajaran berupa animasi dan aplikasi sederhana yang ditujukan untuk pembelajaran kriptologi, akan tetapi tidak ada penjelasan secara rinci tentang proses yang terjadi. Adapun animasi yang sudah ada tidak diberikan

keterangan bagaimana proses perhitungan yang dilakukan pada aplikasi serta inputan pada animasi sudah paten dan tidak dapat diubah inputannya.

Dengan adanya perangkat lunak aplikasi pembelajaran kriptologi ini diharapkan dapat membantu mahasiswa/pembaca dalam memahami algoritma kriptografi simetris dan asimetris serta kriptanalisis. Selain itu juga dapat memberikan alternatif metode belajar berbasis komputer selain dari buku maupun di lembaga pendidikan.

B. Rumusan Masalah

Beberapa permasalahan yang menjadi rumusan masalah yaitu:

1. Aplikasi pembelajaran kriptologi yang dikembangkan di Indonesia hanya menggunakan satu atau dua metode saja.
2. Aplikasi pembelajaran kriptologi yang dikembangkan masih terpisah-pisah dan belum ada tools pembelajaran kriptologi dalam bahasa Indonesia.

C. Tujuan Penelitian

Tujuan penelitian ini adalah:

Menghasilkan sistem pembelajaran elektonik untuk kriptologi simetris dan asimetris yang menampilkan proses enkripsi.

D. Manfaat Penelitian

Manfaat dari penelitian ini diharapkan dapat membantu mahasiswa/pembaca dalam memahami algoritma kriptografi simetris dan asimetris serta kriptanalisis dalam proses enkripsi. Selain itu juga dapat memberikan alternatif metode belajar berbasis komputer selain dari buku maupun di lembaga pendidikan.

E. Ruang Lingkup dan Batasan Penelitian

Agar dalam perancangan ini dapat mencapai sasaran dan tujuan yang diharapkan, maka permasalahan yang ada dibatasi sebagai berikut :

1. Diimplementasikan metode simetris klasik Transposisi (Vigenere) dan Substitusi (Caesar Cipher)
2. Metode simetris modern (Rijndael)
3. Metode asimetris (RSA)
4. Metode kriptanalisis untuk metode Vigenere dan Caesar Cipher sehingga nantinya dapat dikembangkan secara berkelanjutan.

F. Sistematika Penulisan

Dalam penelitian ini pembahasan materi disusun menjadi 5 bab. Materi tersebut disusun dengan sistematika berikut ini:

BAB I PENDAHULUAN

Pada bab ini dibahas mengenai latar belakang yang mendasari dilakukannya penelitian, perumusan masalah, ruang lingkup dan batasan penelitian serta tujuan dan manfaat yang diharapkan dari penelitian ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini dibahas mengenai teori-teori yang berkaitan dengan topik penelitian yang dilakukan. Teori-teori yang dibahas antara lain pembelajaran secara elektronik (e-learning) dan kriptologi.

BAB III METODOLOGI PENELITIAN

Pada bab ini dibahas mengenai perkembangan model e-learning dalam bidang kriptologi, teori-teori kriptologi serta contoh perhitungan pada beberapa algoritma kriptologi.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini dibahas mengenai implementasi, hasil rancangan dan output, analisis dan perancangan sistem, proses pembentukan kunci, proses enkripsi dan dekripsi, serta bentuk pengujian terhadap perangkat lunak.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisikan mengenai kesimpulan yang dapat diambil dari pembuatan perangkat lunak penunjang proses pembelajaran kriptologi simetris dan asimetris. Selain itu disertakan pula saran-saran untuk membantu pengembangan perangkat lunak selanjutnya supaya menjadi lebih baik.

BAB II

TINJAUAN PUSTAKA

Pada bab ini dibahas mengenai teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan. Teori-teori yang dibahas antara lain teori pembelajaran secara elektronik (e-learning) dan kriptologi.

A. Elektronic Learning (E-Learning)

Elektronic learning atau belajar dengan bantuan komputer sudah ada sejak 1970. Dengan menggunakan monitor layar hijau melalui sebuah komputer mainframe berkecepatan rendah, tetapi apakah metode tersebut dapat dikatakan sebagai *E-learning*. Tentu saja hal tersebut bukan merupakan jawaban yang tepat mengenai *E-learning*. Tanpa definisi yang jelas mengenai *E-learning*, sangatlah sulit memutuskan benar atau tidak untuk disebut sebagai *E-learning*.

Berbagai pendapat dikemukakan untuk dapat mendefinisikan *E-learning* secara tepat. *E-learning* atau *Internet enabled learning* menggabungkan metode pengajaran dan teknologi sebagai sarana dalam belajar. (Dr. Jo Hamilton-Jones).

Menurut Turban(2005), *E-learning* adalah proses belajar yang didukung oleh *web*, bisa digunakan dalam kelas biasa atau kelas virtual.

E-Learning (Vaughan Waller, 2001) adalah proses belajar secara efektif yang dihasilkan dengan cara menggabungkan penyampaian materi secara digital yang terdiri dari dukungan dan layanan dalam belajar.

Menurut Matt Comerchero (2006), *E-learning* adalah salah satu bentuk pendidikan yang menggabungkan motivasi, komunikasi, efisiensi dan teknologi. Karena keterbatasan dalam interaksi sosial yang ada siswa harus menjaga motivasi mereka. Pada dasarnya *E-learning* membutuhkan komunikasi antar siswa dengan pembimbing yang cukup sering untuk menyelesaikan tugas yang diberikan. *E-learning* cukup efisien dengan menghilangkan jarak dan kendala lainnya. Jarak dapat di eliminasi karena isi *E-learning* di desain dengan media yang dapat diakses dengan perangkat yang terhubung dengan internet.

Menurut Matt Commerchero (2006), *E-learning* dapat dibedakan jenisnya berdasarkan 4 hal, yaitu :

1. Jalan berkomunikasi: terdapat berbagai jenis cara setiap individu untuk berkomunikasi dengan sesamanya atau pun dengan pembimbingnya.
2. *Schedule*: menurut *schedule* terjadinya, *E-learning* dapat dibedakan menjadi 2, yaitu :
   a. *Synchronous*

      Disebut *synchronous* ketika komunikasi berbasis *real-time* diimplementasikan dalam *E-learning* seperti *video confrence*,

teleconfrence dan *on-line chat*.

b. Asynchronous

Asynchronous mengindikasikan bahwa komunikasi yang terjadi tidak membutuhkan response saat itu juga. Contoh dari *E-learning Asynchorous* adalah *email*, *threaded disscusion*, dan *on-line forum*.

3. Struktur kelas *E-learning*.
4. Teknologi, seperti media, cd interaktif, dan *web* aplikasi.

1. Keuntungan E-Learning

Menurut Kristy DelVecchio dan Megan Loughney (2006), *E-learning* sangat berguna bagi pendidikan dan perusahaan serta untuk semua tipe pelajar. *E-learning* sangat terjangkau, menghemat waktu, dan memiliki hasil yang dapat diukur. *E-learning* mempunyai berbagai keuntungan, yaitu:

a. Mengurangi biaya: *E-learning* lebih hemat dibanding dengan cara belajar tradisional karena hemat waktu dan uang yang dihabiskan saat dalam transportasi.
b. Fleksibilitas: *E-learning* memiliki kelebihan dalam pengaksesan dimana saja dan kapan saja. Pendidikan tersedia kapanpun dan dimanapun dibutuhkan. *E-learning* dapat digunakan di kantor, rumah, jalan, 24 jam sehari dan 7 hari dalam satu minggu. *E-learning* juga memiliki pengukuran terhadap hasil belajar yang dapat dibuat agar instruktur dan pelajar dapat mengetahui apa saja yang telah dipelajari, kapan

mereka akan menyelesaikan pelajarannya dan bagaimana hasil yang telah mereka capai.

c. Pelajar sangat menyukai *E-learning* karena mengakomodir cara belajar yang berbeda. Pelajar bisa mengambil keuntungan belajar sesuai dengan keinginan mereka. Pelajar juga bisa menyesuaikan *E-learning* dengan jadwal kesibukan mereka. Apabila pelajar bekerja maka ia masih dapat belajar dengan *E-learning*. Apabila pelajar menginginkan waktu belajar di malam hari, maka pilihannya juga tersedia.

Perbedaan e-learning dan conventional learning dapat dilihat pada tabel 2.1.

Tabel 2.1. Perbedaan conventional dan electronic learning

	Conventional Learning	*Electronic Learning*
Ruang Belajar	Kelas	Dimana saja asalkan ada fasilitas
Sumber belajar	Buku, Guru / Pengajar	Internet (tidak terbatas)
Content	sedikit dan kurang menarik	banyak pilihan menarik

Menurut Matt Commerchero (2006), *E-learning* dapat dibedakan jenisnya berdasarkan 4 hal, yaitu :

1. Jalan berkomunikasi: terdapat berbagai jenis cara setiap individu untuk berkomunikasi dengan sesamanya atau pun dengan pembimbingnya.
2. *Schedule*: menurut *schedule* terjadinya, *E-learning* dapat dibedakan menjadi 2, yaitu :
   a. *Synchronous*

Disebut *synchronous* ketika komunikasi berbasis *real-time* diimplementasikan dalam *E-learning* seperti *video confrence*, *teleconfrence* dan *on-line chat*.

b. *Asynchronous*

Asynchronous mengindikasikan bahwa komunikasi yang terjadi tidak membutuhkan response saat itu juga. Contoh dari *E-learning Asynchorous* adalah *email*, *threaded disscusion*, dan *on-line forum*.

3. Struktur kelas *E-learning*.
4. Teknologi, seperti media, cd interaktif, dan *web* aplikasi.

2. CAL (Computer Aided Learning)

CAL atau Computer Aided Learning adalah metode pembelajaran yang menggunakan sistem komputer yang menyampaikan pengajaran kepada penerima informasi dengan cara berinteraksi dengan mata pelajaran yang telah disiapkan.

Pembelajaran dengan berbasis komputer bukanlah merupakan hal baru dalam pendidikan. Hasil kajian yang dikembangkan dalam pemanfaatan pembelajaran berbasis komputer adalah:

1. Meningkatkan minat pada pelajaran tersebut.
2. Menimbulkan kesan terhadap mata pelajaran itu apabila siswa mulai menyukai mata pelajaran itu. (Hussin, n.d).

Selain itu, penggunaan media sebagai alat bantu dalam pendidikan merupakan pembelajaran yang lebih efektif dan efisien dibandingkan

dengan pembacaan buku maupun studi langsung dengan obyek tertentu. (Koesnandar, n.d).

Teknologi CAL sendiri memiliki beberapa variabel yang dapat dipakai antara lain:

1. Perkenalan akan masalah/pemberian teori dan rumus.
2. Pemberian contoh kasus dalam menjelaskan masalah.
3. Pemberian simulasi yang mendukung terhadap materi.
4. Pemberian soal-soal dimana user diharapkan menyelesaikannya.
5. Kreatifitas dalam menjabarkan isi/materi/penyelesaian soal sehingga *user* mudah dalam memahaminya.
6. Penggunaan konsep *step by step*, dimana pemberian materi diberikan mulai dari pendahuluan hingga ke contoh kasus.

Penggunaan komputer sebagai media pembelajaran tidak terlepas dari metode psikologi belajar yang sering dipakai dalam proses belajar.

B. Kriptologi

Kriptologi adalah ilmu yang mempelajari kriptografi dan kriptanalisis. Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Sedangkan kriptanalisis adalah cara untuk memecahkan tulisan rahasia

tanpa mengetahui kunci yang digunakan untuk melakukan proses enkripsi.

Ada berbagai jenis algoritma yang digunakan dalam proses kriptologi, mulai dari yang sederhana sampai yang membutuhkan proses komputasi yang besar. Dalam mempelajari kriptologi dibutuhkan pengetahuan matematika karena algoritma yang dirancang untuk proses kriptologi menggunakan ilmu matematika yang rumit sehingga proses komputasinya menjadi rumit dan algoritma tidak mudah dipecahkan.

Topik kriptologi ini sangat penting untuk diimplementasikan dalam e-learning dengan metode penyajian materi yang lebih menarik dan ada proses uji coba perhitungan dari tiap-tiap algoritma sehingga lebih mudah untuk dipelajari.

Kriptologi dibagi menjadi kriptografi dan kriptanalisis. Algoritma yang dirancang ditujukan untuk proses kriptografi, sedangkan untuk kriptanalisis dibuat berdasarkan algoritma kriptografi yaitu cara memecahkan algoritma tersebut. Algoritma kriptografi dibagi menjadi dua bagian besar yaitu simetris dan asimetris. Kriptografi simetris menggunakan kunci yang sama dalam proses enkripsi (membuat tulisan asli menjadi kode) dan juga dekripsi (mengembalikan kode menjadi tulisan asli), sedangkan algorima asimetris tidak menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Kunci yang digunakan berbeda tetapi tidak sembarang kunci yang digunakan, ada aturan-aturan penentuan kunci sesuai dengan algortima yang digunakan.

1. Kriptografi

Kriptografi dibagi menjadi dua bagian besar yaitu enkrispi dan dekripsi yang bertujuan menyembunyikan atau mengkodekan suatu pesan, dan ada juga hashing yang bertujuan untuk menjaga integritas. Enkripsi dan Dekripsi juga dibagi menjadi dua yaitu Simetris dan Asimetris.

a. Kriptografi Simetris

Kriptografi simetris merupakan teknik enkripsi yang menggunakan kunci yang sama untuk melakukan proses dekripsi. Kriptografi simetris ada yang sederhana menggunakan teknik transposisi dan substitusi yang merupakan kriptografi klasik atau yang digunakan pada jaman dulu, namun dalam perkembangannya saat ini sudah menggunakan proses komputasi yang rumit atau modern. Berikut contoh algoritma simetris klasik dan modern.

1) Klasik

Ada dua teknik dalam kriptografi klasik, yaitu teknik substitusi dan teknik transposisi. Teknik substitusi dilakukan dengan mengganti setiap karakter asli dengan karakter lain. contoh :

Karakter asli : a b c d e f g h i j k l m n o p q r s t u v w x y z, diganti menjadi : e f g h i j k l m n o p q r s t u v w x y z a b c d, maka apabila kita ingin menulis pesan : “ SAYA LAPAR” menjadi “WECE PETEV”. Sedangkan untuk teknik transposisi dilakukan dengan permutasi, ada banyak jenis algortima yang digunakan. contoh :

Ada teks “SAYA SEDANG BELAJAR KEAMANAN KOMPUTER”, teks tersebut dibagi menjadi 6 blok.

S	D	L	E	N	T
A	A	A	A	K	E
Y	N	J	M	O	R
A	G	A	A	M	X
S	B	R	N	P	X
E	E	K	A	U	X

Bagian blok yang kosong dapat diisi dengan karakter x. kemudian blok dapat diacak, misalnya susunan kolom 123456 ditukar menjadi 326514 maka apabila teks disusun kembali menjadi : "LAJARK DANGBE TERXXX NKOMPU SAYASE EAMANA".

2) Modern

Ciri dari kriptografi modern yaitu sudah menggunakan proses komputasi yang rumit. Salah satu contoh algoritma simetris modern yaitu rijndael. Dalam algoritma rijndael terjadi 4 proses yaitu Substitusi Byte dengan S-Box, Pergeseran kunci, Pencampuran kolom (mix colums), dan Penambahan kunci. Proses tersebut akan diulang beberapa kali tergantung panjang kunci.

Tabel 2.2. Parameter AES Rijndael

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

Ada empat proses yang terjadi dalam tiap putaran rijndael yaitu :

a). Sub bytes

Sub bytes adalah proses transformasi substitusi byte. Operasi ini merupakan suatu operasi substitusi tak linear yang beroperasi secara mandiri pada setiap byte dengan menggunakan kotak – S.

b). Shift Rows

Shift Rows adalah transformasi pergeseran kunci. Pada operasi ini, byte-byte yang ada pada baris terakhir state digeser secara memutar dengan jumlah pergeseran acak, tetapi baris pertama tidak digeser.

c). Mix Colums

Mix Colums adalah transformasi percampuran kolom. Operasi ini beroperasi pada state kolom dengan memperlakukan setiap kolom sebagai polinomial. Kolom dianggap sebagai polinomial pada GF (2^8).

d). Add Round Key.

Add Round Key adalah Transformasi Penambahan kunci. Operasi ini merupakan suatu operasi penambahan kunci dengan operasi XOR dan setiap kunci putaran terdiri dari w[i] dimana w[i] merupakan upa-kunci yang diturunkan dari kunci primer.

b. Kriptografi Asimetris

1) RSA

Dari sekian banyak algoritma kriptografi kunci public yang pernah dibuat, algoritma yang paling popular adalah algoritma RSA. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar. Oleh karena alas an tersebut RSA dianggap aman. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets Institute of Technology*)

pada tahun 1976, yaitu : Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. RSA mengekspresikan teks asli yang dienkripsi menjadi blok-blok yang mana setiap blok memiliki nilai bilangan biner yang diberi symbol “n”, blok-blok teks asli “M” dan blok teks kode “C”. Untuk melakukan enkripsi pesan “M”, pesan dibagi ke dalam blok-blok numeric yang lebih kecil daripada “n” (data biner dengan pangkat terbesar). Jika bilangan prima yang panjangnya 200 digit, dapat ditambah beberapa bit 0 di kiri bilangan untuk menjaga agar pesan tetap kurang dari nilai “n”.

Parameter-parameter yang digunakan yaitu dalam RSA sebagai berikut.

- *p* dan *q* bilangan prima (rahasia)
- $n = p \cdot q$ (tidak rahasia)
- $\emptyset(n) = (p-1)(q-1)$ (rahasia)
- e (kunci enkripsi) (tidak rahasia)
- d (kunci dekripsi) (rahasia)
- X (teks asli dalam desimal) (rahasia)
- Y (teks kode dalam desimal) (tidak rahasia)

2) Kriptografi Kurva Eliptik

Kriptografi kurva eliptik atau *Elliptic Curve Cryptography* (ECC) merupakan kriptografi kunci publik. Dalam kriptografi kunci publik setiap pengguna atau perangkat yang mengambil bagian dalam komunikasi memiliki pasangan kunci yaitu kunci rahasia dan kunci publik. Kunci publik

akan didistribusikan kepada setiap pengguna, sedangkan kunci privat hanya beberapa pengguna saja yang mengetahuinya dan diperlukan satu set konstanta yang telah ditetapkan untuk diketahui semua perangkat yang mengambil bagian dalam komunikasi.

Operasi matematika pada ECC didefenisikan atas kurva eliptik

$$y^2 = x^3 + ax + b \text{……..} \quad (2.1)$$

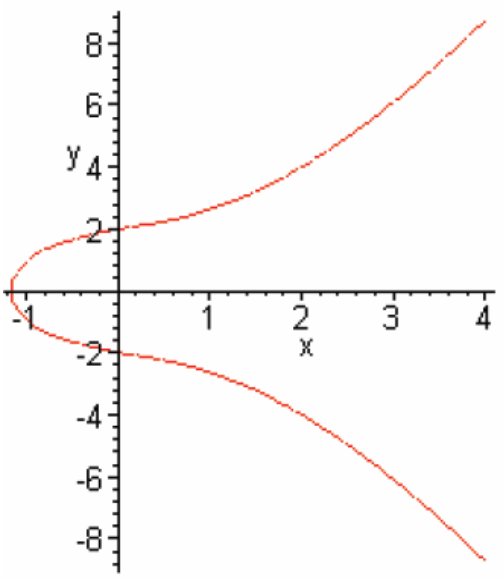
dimana $4a^3 + 27b^2 \neq 0$, setiap nilai a dan b memberikan kurva eliptik yang berbeda. Semua titik (x,y) yang memenuhi persamaan di atas ditambah titik pada medan tak berhingga terletak pada kurva eliptik. Keuntungan menggunakan ECC yaitu ukuran kunci yang digunakan kecil. Sebuah kunci 160 bit ECC dianggap sebagaimana dijamin oleh RSA dengan panjang kunci 1024 bit.

Adapun dasar-dasar matematika yang perlu dipahami sebelum mengetahui lebih jauh mengenai kurva eliptik yaitu aritmetika modular, aritmetika polinomial, dan konsep medan berhingga.

Contok Kurva Eliptik pada himpunan bilangan real.

$y^2 = x^3 + ax + b$ a,b {real}

misalkan nilai a = 2 dan b = 4, maka akan terbentuk kurva seperti Gambar 2.1.



Gambar 2.1. Kurva eliptik dengan persamaan $y^2 = x^3 + 2x + 4$

Aritmetika kurva eliptik E(a,b) meliputi elemen identitas penjumlahan, elemen invers penjumlahan dan defenisi penjumlahan titik namun untuk keperluan Kriptografi kurva eliptik, variabel dan koefisien persamaan kurva dibatasi pada medan berhingga. Medan berhingga yang umum digunakan adalah *prime finite field Zp* (medan berhingga Zp yang berisi hasil modulo dengan suatu bilangan prima p) dan medan berhingga $GF(2^m)$.

2. Kriptanalisis

Kriptanalisis adalah sebuah studi mengenai cipher, ciphertext atau cyrptosystems yang bertujuan menemukan kelemahan dalam system penyandian, sehingga dimungkinkan untuk memperoleh plaintext dari ciphertext yang ada, tanpa perlu mengetahui kunci ataupun algoritma

pembangun ciphertext tersebut. Cara ini disebut dengan memecahkan cipher, ciphertext atau cryptosystem.

Dalam memecahkan cipher, dilakukan pencarian kesalahan dalam desain atau implementasi dari cipher itu sendiri sehingga dapat mengurangi jumlah kunci yang harus dicoba ketika melakukan brute force attack (mencoba memecahkan cipher dengan menggunakan semua kunci yang mungkin sampai akhirnya ditemukan satu kunci yang benar). Contohnya, jika kunci yang digunakan untuk mengenkripsi sepanjang 2128 , makabrute force attack akan mencoba semua kunci yang mungkin, yaitu sebanyak (21282127)(atau rata-rata kali untuk menemukan kunci yang tepat. Iterasi sebesar itu masih belum dapat dilakukan secara cepat oleh sistem komputasi saat ini. Dengan adanya studi kriptanalisis, telah ditemukan cara pengekstraksian plaintext hanya dalam 240 kali iterasi. Walaupun belum sepenuhnya terpecahkan, namun plaintext telah dapat diekstrak daricipher dengan menggunakan sumberdaya komputasi yang relatif jauh lebih kecil.

a. Teknik-teknik Kriptanalisis

Terdapat beberapa teknik dalam melakukan kriptanalisis, tergantung kepada akses yang dimiliki oleh kriptanalis, apakah melalui ciphertext, plaintext, ataupun aspek lain dari sistem kriptografi. Berikut adalah beberapa tipe penyerangan yang umum dipakai untuk memecahkan sandi :

1) Known-Plaintext Analysis

Dengan prosedur ini, kriptanalis mengetahui sebagian isi plaintext dari ciphertext yang berhasil didapatkan. Menggunakan informasi yang ada ini, kriptanalis berusaha untuk mencari kunci yang digunakan untuk menghasilkan ciphertext.

Pesan-pesan yang memiliki format terstruktur memberikan peluang kepada kriptanalis untuk menebak plaintext dari ciphertext yang bersesuaian. Contoh dari pesan-pesan terstruktur ini adalah email dengan kolom from, to, subject, kemudian salam penutup dan pembuka pada surat seperti ”dengan hormat”, salam, dan lainnya.

Linear Cryptanalysis adalah salah satu algoritma yang termasuk ke dalam seranganknown-plaintext. Linear Cryptanalysis diperkenalkan oleh Mitsuru Matsui pada tahun 1993. Pada algoritma ini penyerang akan mempelajari fungsi linear yang merepresentasikan hubungan antara ciphertext dan plaintext untuk mendapatkan kunci.

Algoritma berbasis XOR, termasuk ke dalam algortima enkripsi/dekripsi yang tidak aman karena dapat dipecahkan menggunakan linear cryptanalysis.

2) Chosen-Plaintext Analysis

Kriptanalis telah dapat menghasilkan plaintext dari ciphertext yang ada, namun kuncinya sendiri belum ditemukan. Pada serangan jenis ini

kriptanalis dapat memilihplaintext tertentu untuk dienkripsikan, yaitu plaintext yang lebih mengarahkan penemuan kunci.

Kriptanalis berusaha untuk menemukan kunci pembangun ciphertext dengan membandingkan keseluruhan ciphertext dengan plaintext yang ada. Teknik enkripsi RSA (Rivest-Shanir-Adleman) telah terbukti dapat dipecahkan menggunakan teknik analisis ini.

Differential Analysis adalah sebuah teknik yang dikembangkan oleh Eli Biham dan Adi Shamir. Teknik ini memberikan suatu cara untuk menemukan beberapa bit kunci dari plaintext dan ciphertext yang tersedia, dengan begitu jumlah kemungkinan kunci yang akan dicoba pada exhaustive key search atau brute force attack dapat berkurang drastis, mengurangi waktu kalkulasi.

Differential Analysis secara garis besar membahas pola lengkap dari bit-bit mana saja yang berubah dan tidak berubah pada proses pengubahan input menjadi output.

3) Ciphertext-Only Analysis

Pada teknik ini, kriptanalis hanya berbekal ciphertext saja, tanpa adanya pengetahun mengenai plaintext. Teknik ini membutuhkan akurasi yang tinggi dalam melakukan penaksiran mengenai bagaimana sebuah pesan dapat disandikan.

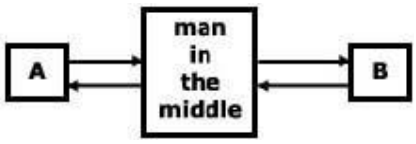
Teknik ini dapat bekerja lebih baik dengan dukungan adanya pengetahuan tambahan mengenai teks. Misalnya dengan pengetahuan

bahwa plainteks asal ditulis dalam bahasa inggris maka kriptanalis dapat menghitung frekuensi huruf dari chiperteks kemudian membandingkannya dengan frekuensi rata-rata huruf pada teks berbahasa inggris. Namun cara penghitungan frekuensi huruf seperti ini hanya bekerja untukplaintext yang didekripsi menggunakan teknik substitusi satu ke satu.

Algoritma kriptografi modern memiliki daya tahan yang lebih tinggi terhadap jenis serangan seperti ini.

4) Man-in-the-middle attack

Penyerang, yang dalam hal ini adalah kriptanalis, masuk kedalam saluran komunikasi antara kedua pihak yang akan saling bertukar kunci mereka. Penyerang menempatkan dirinya sedemikian sehingga kedua pihak tadi merasa bahwa mereka saling bertukar kunci, namun sebenarnya penyeranglah memberikan kunci-kunci yang nantinya digunakan oleh pihak-pihak tadi.



Gambar 2.2. Serangan kriptografi man-in-themiddle

Teknik ini dapat dipatahkan dengan menggunakan kombinasi fungsi hash dan algoritma kunci publik. B dapat memeriksa apakan kunci publik yang ia terima benar,dengan cara memeriksa sidik jari (fingerprint). Sidik jari ini adalah suatu fungsi hash dari kunci publik tersebut yang

diberikan melalui jalur yang berbeda dengan pengiriman kunci publik. Sidik jari digunakan karena ukurannya yang lebih kecil dibandingakan dengan kunci publik sehingga lebih mudah ditentukan nilai kebenarannya.

Cara lain untuk mematahkan serangan tipe ini adalah dengan menyimpan kunci publik dalam suatu basisdata online yang menjamin kebenaran dari kunci publik. Suatu CA (Certificate Authority) atau server kunci publik dapat memberikan keyakinan pada pengguna, pada saat mereka menyimpan (download) kunci, bahwa kunci tersebut bernilai benar.

5) Timing/differential power analysis

Sangat berguna jika digunakan melawan smartcard, yang menghitung perbedaan konsumsi elektrik dalam jangka waktu tertentu ketika microchip melakukan pengamanan informasi. Teknik ini dapat digunakan untuk memperoleh informasi mengenai perhitungan pembangkitan kunci yang digunakan dalam algoritma enkripsi dan fungsi-fungsi pengamanan lainnya.

Teknik ini dapat ditangkal dengan menggunakan random noise ketika melakukan enkripsi, atau mengacak alur fungsi sehingga lebih sulit untuk melacak fluktuasi tenaga listrik yang terpakai. Tipe analisis ini dikembangkan oleh Paul Kocher dari Cryptography Research. Penyerangan seperti ini umumnya terlepas dari jenis algoritma kriptografi yang digunakan.

6) Correlation

Keterhubungan antara kunci dengan hasil pengenkripsian merupakan sumber utama yang akan digunakan oleh kriptanalis. Pada kasus yang paling mudah, kunci justru secara tidak sengaja terbocorkan oleh sistem krptografinya sendiri. Untuk kasus yang lebih kompleks, dicari keterhubungan antara informasi yang dapat diperoleh mengenai kriptosistem dan informasi mengenai perkiraan kunci. Ide mengenai keterhubungan merupakan ide dasar pada kriptosistem.

7) Kesalahan dalam kriptosistem

Kesalahan dalam kriptosistem dapat digunakan dalam kriptanalisis dan bahkan dapat membocorkan kuncinya sendiri. Kesalahan tersebut dapat dimanfaatkan dalam kriptanalisis. Kesalahan disini dapat juga berupa kelemahan dari fungsi matematis yang digunakan oleh algoritma enkripsi/dekripsi atau pemilihan kunci lemah.

Algoritma RSA merupakan contoh algoritma yang memiliki kesalahan yang dapat diserang. Begitu pula algoritma DES, karena algoritma ini memiliki beberapa pasang kunci lemah.

8) Rubber-hose cryptanalysis

Serangan jenis ini dapat dikatakan sebagai serangan yang paling efektif dan dapat langsung memberikan hasil. Serangan ini berupa serangan langsung kepada pihak pengirim.

Rubber-hose attack didasarkan pada teori bahwa manusia yang berada dibawah tekanan akan menjadi lebih lemah. Di lain pihak, komputer tidak mengalami stress (dibawah tekanan) sehingga tidak akan terpengaruh dengan serangan semacam ini.

Pada serangan ini, pihak ketiga akan mengirimkan surat gelap, mengancam atau bahkan menyiksa hingga pihak pengirim mau memberikan kunci atau bahkan langsung memberikan plaintext yang besangkutan.

Serangan jenis ini tidak memandang tipe algoritma enkripsi/dekripsi, ia bekerja untuk mematahkan seluruh algoritma enkripsi/dekripsi. Karena alasan inilah rubber-hose attackdisebut sebagai serangan paling efektif.

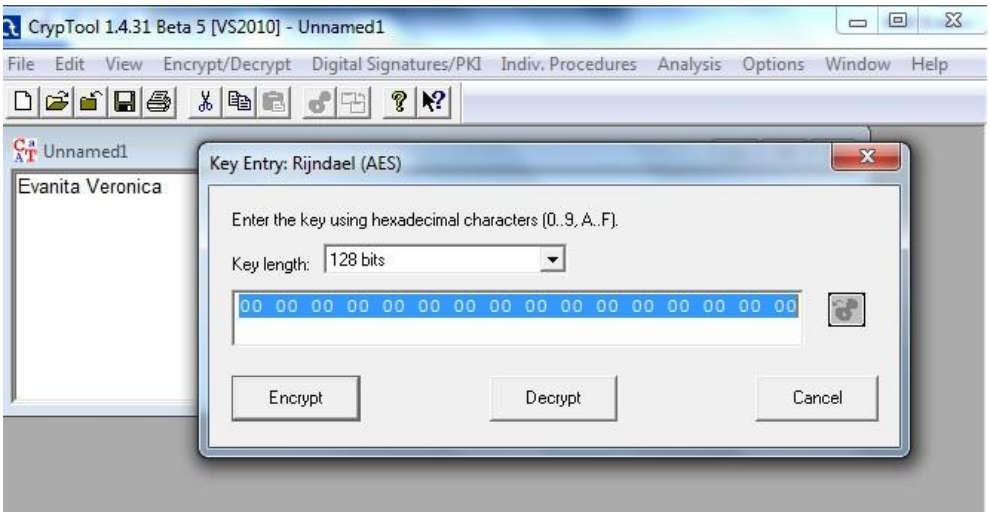
Terdapat beberapa cara efektif untuk menghadapi serangan jenis ini yaitu tetap tenang dan gunakan steganografi, pindah di luar jangkauan pihak-pihak lawan, misalnya di luar negeri, tingkatkan ketahanan fisik, untuk menghindari serangan secara sosial menjauhlah dari orang-orang terdekat dan jangan bina hubungan dekat (teman) baru, Gunakan multipart key yang membutuhkan lebih dari satu orang untuk melakukan enkripsi/ dekripsi terhadap informasi, gunakan One-Time Pad dimana tidak mungkin memecahkan ciphertext tanpa menggunakan kunci, karena sifatnya yang terlalu panjang (sama dengan plaintext).

9) Serangan terhadap atau menggunakan hardware dari cryptosystem

Serangan jenis ini merupakan serangan jenis baru yang diprediksikan akan semakin sering muncul dengan semakin meluasnya penggunaan mobile crypto devices. Serangan ini didasarkan kepada perhitungan rinci dari proses enkripsi yang dilakukan oleh suatu perangkat kripto.

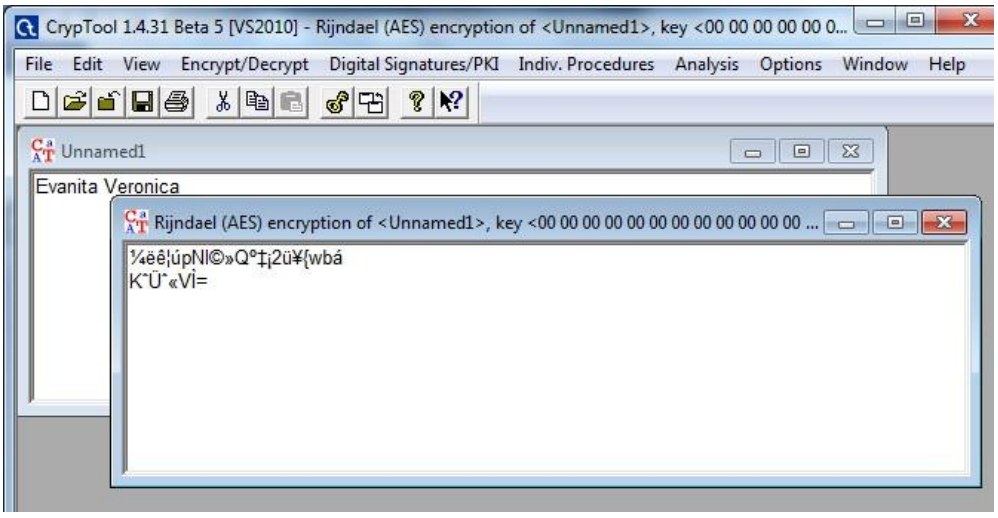
C. PENELITIAN SEJENIS

Penelitian-penelitian sebelumnya yang terkait dengan aplikasi kriptofrafi dan kriptanalisis sudah dilakukan di beberapa Negara dan sampai saat ini masih terus dikembangkan. Informasi dari portal pengembang kriptografi www.cryptool.org (20 November 2012) menunjukkan ada 50 relawan pengembang di seluruh dunia yang mengembangkan tools kriptografi dan kriptanalisis untuk e-learning, game dan lain sebagainya. Tools ini dikembangkan dalam lima bahasa sehingga memudahkan proses belajar akan tetapi dari kelima bahasa belum ada yang berbahasa Indonesia. Aplikasi yang dikembangkan juga belum sepenuhnya memberikan informasi proses yang terjadi dalam algoritma kriptografi.



Gambar 2.3. Proses Algoritma Rijndael Pada CrypTool

Gambar 2.3 menunjukkan proses enkripsi menggunakan cryptool. Tidak ada penjelasan langkah-langkah proses yang terjadi sampai menjadi kode seperti pada Gambar 2.4.



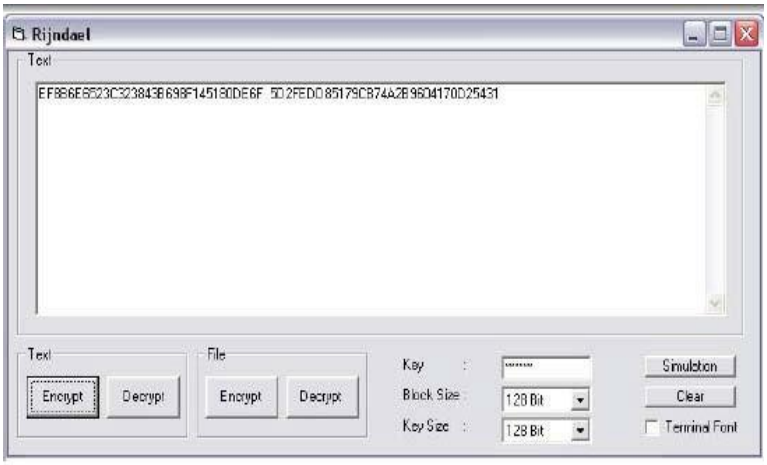
Gambar 2.4. Hasil Proses Enkripsi Algoritma Rijndael Pada CrypTool

Gambar 2.4 adalah hasil enkripsi algoritma rijndael pada cryptool. Informasi yang diberikan oleh aplikasi sangat terbatas sehingga pengguna hanya mengetahui input dan hasil tanpa mengetahui proses yang terjadi pada algoritma.

Ada beberapa penelitian terkait kriptografi dan pembelajaran kriptografi di Indonesia tetapi seperti cryptool, aplikasi yang dibagun hanya menampilkan input dan output tanpa menampilkan proses. Sedangkan dalam proses pembelajaran diharapkan target pengguna aplikasi dapat memahami proses algoritma kriptografi.

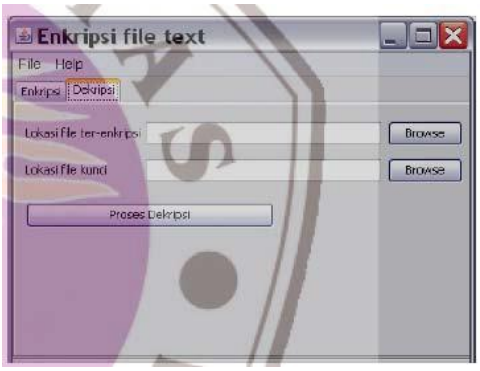
Beberapa Penelitian kriptografi di Indonesia yaitu sebagai berikut.

a. Eko Saputra (2009) Penggunaan Algoritma Rijndael untuk membuat Aplikasi Enkripsi. Aplikasi yang dibangun hanya menampilkan input dan output enkripsi dan dekripsi.



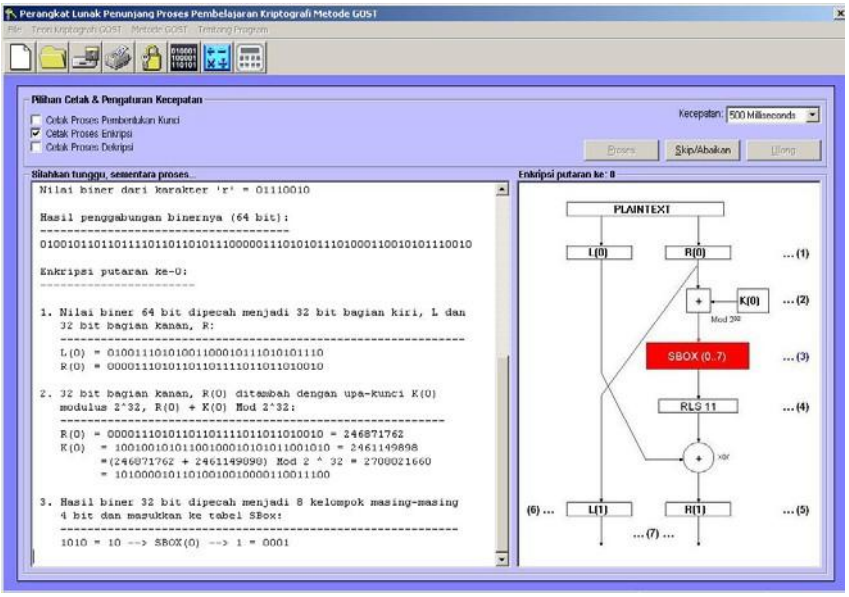
Gambar 2.5. Aplikasi Enkripsi Rijndael Dari Penelitian Eko Saputra

b. Hayatun Nufus (2009) Menggunakan Algoritma Base64 untuk aplikasi enkripsi dekripsi saja dan hanya menampilkan input dan output enkripsi dekripsi.



Gambar 2.6. Aplikasi Base 64 Dari Penelitian Hayatun Nufus

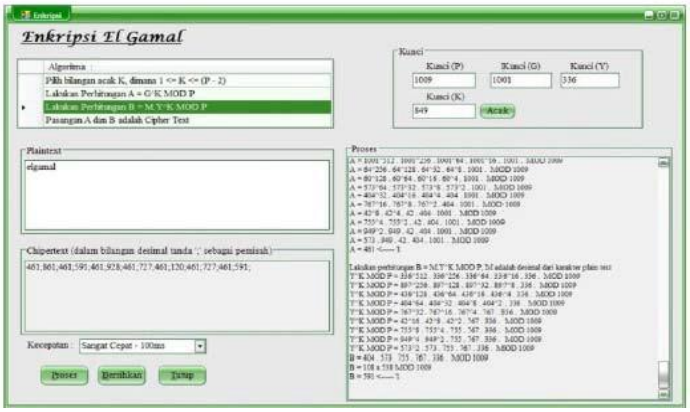
c. Dikwan Moeis, Universitas Hasanuddin (2011) Pembelajaran kriptografi dengan menggunakan metode GOST.



Gambar 2.7. Pembelajaran Metode GOST Dari Peneltian Dikwan Moeis.

Pada penelitian yang dilakukan oleh dikwan moeis sudah menampilkan proses algoritma kriptografi yang digunakan.

d. Zelvina Anandia et al (2012) Perancangan Aplikasi Pembelajaran Kriptografi kunci publik ElGamal untuk mahasiswa.



Gambar 2.8. Pembelajaran ElGamal Dari Penelitian Zelvina et al

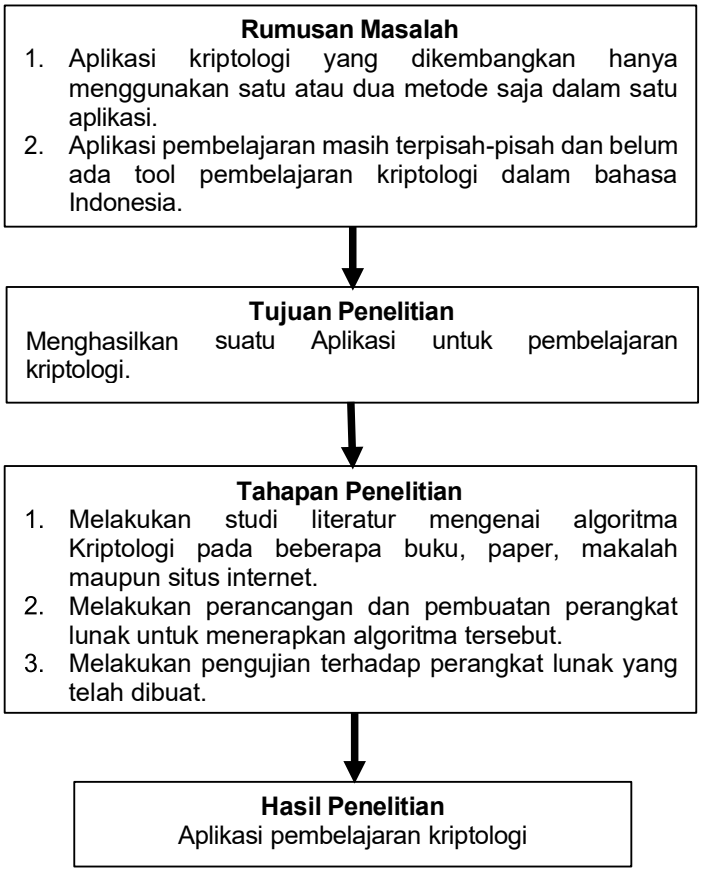
Pembelajaran ElGamal juga sudah menunjukkan langkah-langkah yang dilakukan dalam proses enkripsi ElGamal. Dari roadmap yang ada dapat dilihat bahwa aplikasi pembelajaran yang dibangun masih terpisah dan sulit dikembangkan. Ada juga yang sudah digabungkan dalam satu tools namun tidak ada penjelasan terperinci mengenai langkah-langkah dari proses kriptografi yang ada pada aplikasi yang dibangun.

D. Rencana Penelitian

Dalam penelitian ini akan dirancang model pembelajaran kriptografi yang dapat diakses secara luas dan bebas oleh setiap orang yaitu berbasis web yang menyajikan algoritma-algoritma kriptografi sehingga nantinya aplikasi dapat dikembangkan. Aplikasi berbasis web yang akan

diracang menyajikan dasar-dasar teori dari algoritma dan juga pengujian algoritma. Yang dimaksud dengan pengujian algoritma yaitu pengguna aplikasi dapat menginput data kemudian melihat proses kriptografi yang terjadi, langkah-langkah apa saja yang dilakukan oleh algoritma yang disajikan sehingga menghasilkan output enkripsi maupun dekripsi.

E. Kerangka Berpikir



Gambar. 2.9 Bagan Kerangka Pikir

BAB III

METODOLOGI PENELITIAN

Pada bab ini dibahas mengenai lokasi dan waktu penelitian, Metode penelitian, Perangkat penelitian, Desain Penelitian, Desain Proses dan Desain Aplikasi.

A. Lokasi dan Waktu Penelitian

Penelitian dilaksanakan di Makassar selama kurang lebih 5 bulan (Pebruari – Juni) tahun 2013.

B. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode deskriptif yaitu dengan melakukan studi literatur untuk mengumpulkan teori dasar mengenai kriptografi, kemudian membuat rancangan sistem pembelajaran elektronik, pembuatan aplikasi dan pengujian aplikasi.

Dalam melakukan studi literatur, data yang dikumpulkan berupa jenis-jenis algoritma kriptografi, langkah-langkah melakukan enkripsi sesuai dengan jenis algoritma. Setelah data-data terkumpul dilakukan proses enkripsi manual, kemudian berdasarkan urutan langkah-langkah enkripsi tersebut dibuat model pembelajaran yaitu aplikasi pembelajaran kriptografi

yang sesuai dengan jenis algoritma dimana pengguna aplikasi dapat melakukan proses input data berupa teks asli dan kunci.

Aplikasi dirancang untuk memberikan informasi langkah-langkah melakukan proses kriptografi dalam kasus enkripsi sehingga pengguna aplikasi dapat memahami langkah-langkah proses enkripsi sesuai dengan jenis algoritma.

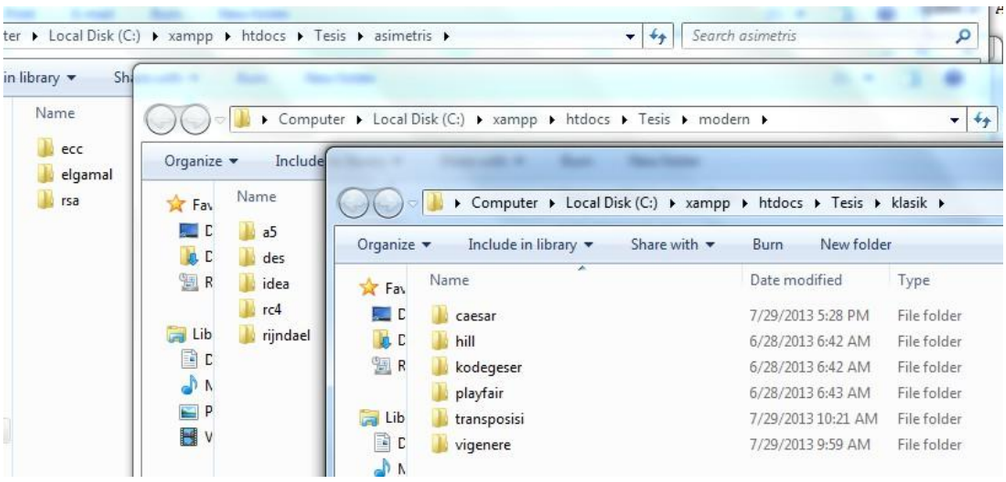
Aplikasi dibangun menggunakan bahasa pemrograman php dan javascript sehingga mudah untuk dikembangkan. Struktur aplikasi pembelajaran yang dibangun ditunjukkan seperti tabel berikut.

Tabel 3.1. Struktur folder aplikasi

Nama	Jenis	fungsi
Images	folder	sebagai tempat menyimpan file yang berupa gambar
css	folder	berisi file-file css yang digunakan oleh aplikasi
js	folder	berisi file-file javascript yang juga berguna untuk aplikasi
klasik	folder	berisi algoritma-algortima Simetris Klasis
modern	folder	berisi algoritma-algortima Simetris Modern
asimetris	folder	berisi algoritma-algortima Asimetris
kriptanalisis	folder	berisi algoritma kriptanalisis
index	file php	sebagai halaman utama program
home	file html	sebagai isi pada content awal program

Struktur folder aplikasi yang dibangun dibuat seperti tabel 3.1 sehingga memudahkan pengembang dalam mengembangkan aplikasi. Apabila akan mengubah desain maupun warna tulisan ataupun layout maka source code terdapat dalam folder css dan js. Di dalam folder tersebut terdapat keseluruhan kode yang digunakan dalam desain layout aplikasi pembelajaran kriptologi.

Kemudian ada folder klasik, modern, asimetris dan kriptanalisis. Folder tersebut disesuaikan dengan menu pada aplikasi sehingga memudahkan pengembang lain yang ingin mengembangkan aplikasi pembelajaran secara berkelanjutan. Struktur folder di dalam folder klasik, modern, asimetris dan kriptanalisis dapat dilihat pada gambar 3.1.



Gambar 3.1. Struktur sub folder modern, klasik dan asimetris

Apabila ada pengembang yang mengembangkan salah satu jenis algoritma kriptografi, misalnya kodegeser maka pengembang dapat memasukkan modul yang telah dibuat pada folder kode geser. Kemudian tambahkan sub menu pada aplikasi yaitu pada halaman index.php (dapat dilihat pada lampiran koding) pada baris program :

```
<tr align = 'center'><td>
<a href='klasik/kodegeser/kodegeserteori.php' target='utama'>
KodeGeser</a></td></tr>
```

KodeGeser yang digarisbawahi merupakan link yang dibuat untuk menampilkas isi modul dari folder klasik, sub folder kode geser. `'klasik/kodegeser/kodegeserteori.`

Apabila belum ada jenis algoritmanya dalam sub folder jenis kriptografi, maka pengembang dapat menciptakan folder baru, kemudian pada baris program pada halaman index.php pengembang membuat baris program seperti di atas untuk menciptakan link baru dan target folder serta sub folder yang akan ditampilkan pada aplikasi.

C. Perangkat Penelitian

Spesifikasi peralatan yang digunakan dalam penelitian ini sebagai berikut :

1. Spesifikasi Perangkat Keras, terdiri dari :
   a. Processor: Intel Pentium IV atau yang diatasnya.
   b. Kapasitas memory: 512 MB.
   c. Kapasistas hardisk: 100 GB.
   d. VGA card 128 MB.
   e. Monitor dengan resolusi 1024 x 768 pixel.
   f. Keyboard dan Mouse.
2. Spesifikasi Perangkat Lunak, terdiri dari :
   a. Microsoft Windows 7
   b. Bahasa Pemrograman PHP dan Java script.

D. Desain Penelitian

Tahapan-tahapan yang dilakukan dalam penelitian ini yaitu:

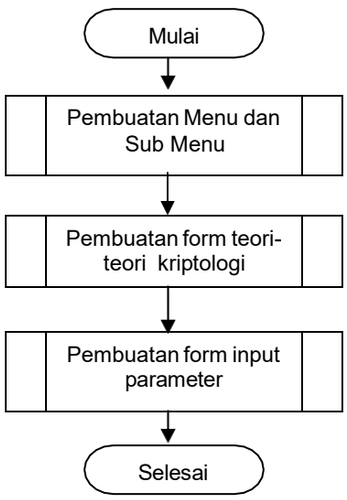
1. Analisis dan defenisi persyaratan. Pada tahap ini akan dilakukan kegiatan sebagai berikut :
   a. Pengumpulan literature mengenai kriptografi.
   b. Menganalisa kebutuhan pengguna terhadap aplikasi pembelajaran elektronik untuk kriptografi.
   c. Membuat batasan masalah yakni hanya pada kasus enkripsi.
2. Perancangan sistem dan perangkat lunak. Pada proses ini akan dilakukan perancangan menu berupa menu kriptogtafi dan kriptoanalisis. Kemudian merancang modul-modul aplikasi berupa modul fungsi untuk masing-masing algoritma kriptografi seperti Vigenere, Caesar, dan Rijndael.
3. Implementasi dan pengujian unit. Pada tahap ini, akan dilakukan pemrograman aplikasi dan pengujian aplikasi dengan memasukkan data inputan untuk mengetahui kebenaran hasil dari setiap proses dalam algoritma kriptografi.
4. Operasi dan pemeliharaan. Melakukan koreksi dari berbagai error yang tidak ditemukan pada tahap-tahap sebelumnya sehingga dapat dilakukan perbaikan.

E. Desain Proses

Perancangan dibagi menjadi alur proses pembuatan perangkat lunak, perancangan input, perancangan output dan perancangan antarmuka (*Interface*).

Alur proses pembuatan perangkat lunak

Dalam pembuatan suatu perangkat lunak, dibutuhkan suatu perencanaan dan alur. Hal ini bertujuan untuk mempermudah proses pembuatan dari perangkat lunak tersebut. Gambar berikut ini adalah *flowchart* dari proses pembuatan perangkat lunak:

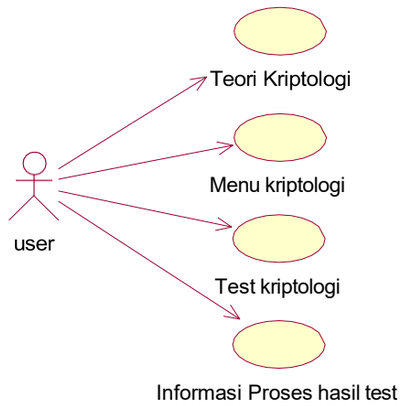


Gambar 3.2. Alur proses pembuatan perangkat lunak

F. Desain Aplikasi

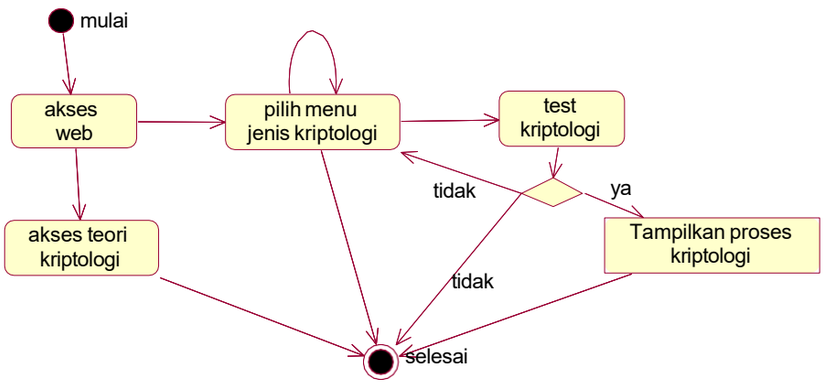
a. Perancangan Sistem

Rancangan dari sistem pembelajaran elektronik yang akan dikerjakan adalah sebagai berikut.



Gambar 3.3. Diagram usecase

Perancangan sistem yang akan dibangun ditunjukkan seperti pada Gambar 3.3, dimana terdapat teori dari algoritma kriptologi, menu kriptologi untuk memilih jenis algoritma yang akan dipelajari, test kriptologi untuk melakukan percobaan algoritma dengan memberikan inputan sesuai dengan parameter input dari algoritma yang dipilih, setelah melakukan inputan maka sistem akan memberikan informasi proses langkah-langkah dari algoritma kriptologi tersebut. Aktivitas sistem ditunjukkan Gambar 3.4.



Gambar 3.4. Activity Diagram

b. Perancangan input

Desain *input* meliputi desain dari bentuk dokumen dasar yang akan digunakan untuk menangkap data *input* beserta semua kode-kode yang digunakan. Desain *input* pada aplikasi pembelajaran kriptografi ini disesuaikan dengan jenis algoritmanya.

c. Perancangan output

Output (keluaran) adalah produk dari sistem informasi yang dapat dilihat. *Output* digunakan untuk menjawab kebutuhan pemakai dalam bentuk-bentuk informasi yang diinginkan. Beberapa bentuk *output* yang dapat digunakan untuk memberikan informasi yang tepat seperti dokumen teks.

Desain *output* aplikasi pembelajaran kriptologi adalah bentuk dokumen teks. Dokumen teks berupa uraian proses proses enkripsi dan proses dekripsi.

d. Perancangan antarmuka (*Interface*)

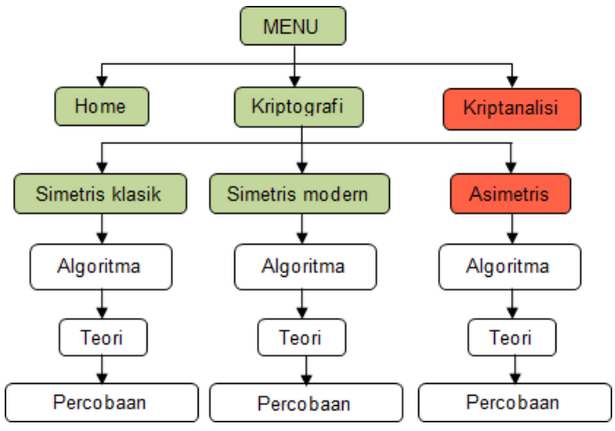
Pada bagian ini dijelaskan mengenai perancangan antarmuka perangkat lunak. Rancangan antarmuka ini merupakan desain awal perangkat lunak dimana akan ditampilkan secara umum rancangan keseluruhan.

Perangkat lunak penunjang proses pembelajaran ini memiliki beberapa rancangan *form* antarmuka, yaitu:

1) Menu Utama pada *Form Main*.
2) Area Tampilan teori algoritma
3) Tampilan Proses Enkripsi dan Dekripsi.
4) *Form Input* parameter yang dibutuhkan algoritma

1. Struktur menu

Dalam pembuatan perangkat lunak ini, dirancang beberapa menu utama beserta sub-sub menunya. Struktur menunya sebagai berikut:



Gambar 3.5. Struktur menu

BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini dibahas mengenai implementasi, hasil rancangan dan output, analisis dan perancangan sistem, proses pembentukan kunci, proses enkripsi dan dekripsi, serta bentuk pengujian terhadap perangkat lunak.

A. HASIL

Perangkat lunak untuk pembelajaran kriptografi simetris dan asimetris ini dibuat secara terbuka, sehingga dapat dikembangkan oleh berbagai pihak dan dapat juga digunakan oleh berbagai kalangan yang membutuhkan.

1. Form Utama

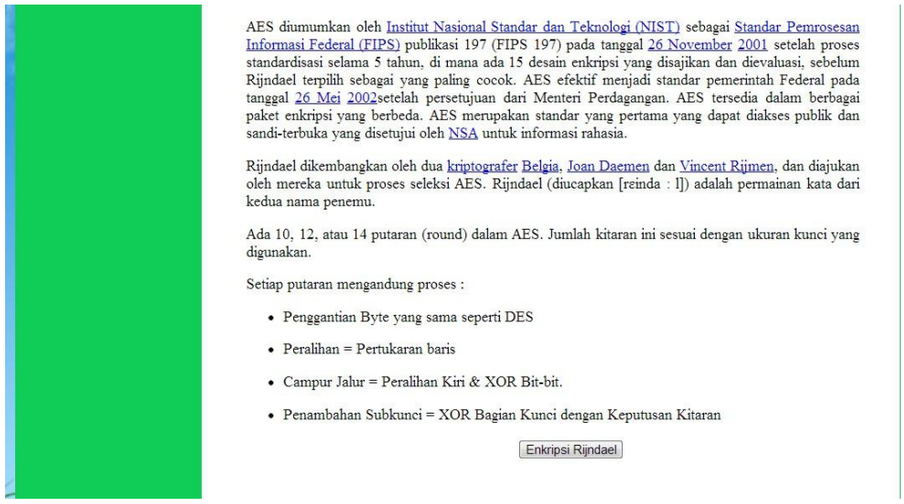
Form utama adalah *form* yang pertama kali tampil pada saat aplikasi dijalankan, berfungsi sebagai *form* pembuka. Ketika aplikasi dijalankan atau di akses maka akan muncul tampilan utama dari aplikasi kriptologi seperti pada Gambar 4.1.

Gambar 4.1. Tampilan form utama

Pilihan menu yang ada yaitu kriptografi dan kriptanalisis, dan pada menu kriptografi terdapat sub menu simetris klasik, simetris modern dan asimetris, apabila menu tersebut di pilih maka akan tampil pilihan menu pada sidebar kiri yang berisi algoritma-algoritma sesuai dengan pengelompokan pada sub menu yang dipilih. Tampilan menu dapat dilihat pada Gambar 4.2.

Gambar 4.2. Tampilan menu kriptografi

Pada menu kriptografi yang ada pada sidebar kiri apabila di pilih maka akan muncul teori dari algoritma yang dipilih, kemudian di bagian akhir dari teori terdapat pilihan untuk melakukan test kriptografi misalnya enkripsi, kemudian pengguna aplikasi dapat memberikan inputan berupa teks asli dan kunci, sesuai parameter yang dibutuhkan dalam proses algoritma kriptografi.



Gambar 4.3. Tampilan isi teori dan pilihan enkripsi

Di bagian akhir dari isi teori dari kriptografi akan ditampilkan pilihan menu enkripsi dan dekripsi, sehingga pengguna dapat melakukan percobaan algoritma dengan memasukkan inputan sesuai dengan parameter yang dibutuhkan setelah itu aplikasi akan menampilkan setiap proses algoritma.

Gambar 4.4. Tampilan input enkripsi rijndael

Contoh tampilan enkripsi rijndael pada Gambar 4.4 menunjukkan paramater input yang dibutuhkan oleh algoritma ini yaitu plain teks atau teks

asli dan juga kunci. Panjang kunci dibatasi 128 bit atau hanya 16 karakter dan juga panjang plain teks dibatasi sebanyak 16 karakter sehingga prosesnya lebih mudah dimengerti. Untuk panjang kunci 128 bit dilakukan sebanyak 10 kali putaran.

Langkah-Langkah melakukan proses enkripsi Rijndael adalah sebagai berikut.

1. Mengubah karakter Ascii dari Teks Asli dan Kunci menjadi Hexadesimal. Contoh sebagai berikut.

   Dalam aplikasi dibatasi proses hitung 128 bit sehingga terjadi 10 putaran.

   Teks asli : “evanita veronica”

   kunci : “percobaan sajaxx“

   Teks Asli : evanita veronica =

   65 76 61 6E 69 74 61 20 76 65 72 6F 6E 69 63 61

   Masukkan ke dalam kolom 4x4

65	69	76	6E
76	74	65	69
61	61	72	63
6E	20	6F	61

   Kunci : percobaan sajaxx =

   70 65 72 63 6F 62 61 61 6E 20 73 61 6A 61 78 78

70	6F	6E	6A
65	62	20	61
72	61	73	78
63	61	61	78

2. Teks Asli dalam hexadecimal di XOR dengan kunci dalam hexadecimal. Contoh sebagai berikut

   65 76 61 6E 69 74 61 20 76 65 72 6F 6E 69 63 61

   X O R

   70 65 72 63 6F 62 61 61 6E 20 73 61 6A 61 78 78

   65 xor 70 dilakukan dengan cara mengkonversi ke dalam biner terlebih dahulu, 65 = 0110 0101, 70 = 0111 0000

   Tabel Kebenaran XOR

x	y	x XOR y
0	0	0
0	1	1
1	0	1
1	1	0

   Sehingga hasilnya : 0001 0101 = 15, hasil keseluruhan yang diperoleh yaitu : 15 13 13 0D 06 16 00 41 18 45 01 0E 04 07 1B 19

15	06	18	04
13	16	45	07
13	00	01	1B
0D	41	0E	19

   Hasil ini sebagai input yang dimasukkan dalam 4 proses rijndael yang akan diulang sebanyak 10 kali putaran.

3. Proses Rijndael yaitu Substitusi Byte, Pergeseran Baris, Pencampuran Kolom dan Penambahan Kunci.

Proses-proses yang dilakukan sebagai berikut.

a. Substitusi bytes

Substitusikan dengan s-box.

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 4.5. s-box

S-box adalah tabel yang berisi bilangan hexadesimal dengan urutan bilangan yang sudah di standarisasi oleh Federal Information Processing Standards Publications (FIPS PUBS) yang dipublikasikan oleh National Istitute of Standards and Technology (NIST). Cara melakukan substitusi yaitu tiap bilangan hexadesimal yang terdapat dalam cell terdiri dari dua digit, sehingga digit sebelah kiri dinyatakan sebagai baris atau x dalam tabel s-box, sedangkan digit disebelah kanan dinyatakan sebagai kolom atau y dalam s-box. Contohnya, pada tabel hasil XOR teks asli terhadap kunci, pada baris 1 kolom 1 terdapat bilangan biner 15 sehingga apabila disubstitusi terhadap s-box maka “1” adalah digit disebelah kiri berarti baris dan “5” digit di sebelah kanan sebagai kolom, maka baris 1 dan kolom 5 pada s-box

adalah 59, sehingga hasil substitusi 15 adalah “59”. Hasil substitusi dapat dilihat sebagai berikut.

59	6F	AD	F2
7D	47	6E	30
7D	63	7C	AF
D7	83	AB	D4

b. Shift Rows

Cara melakukan shift rows yaitu pada baris ke 2 digeser 1 kolom ke kanan, pada baris ke 3 di geser sebanyak 2 kolom dan pada baris ke 4 digeser sebanyak 3 kolom, sedangkan untuk baris pertama tidak mengalami perubahan.

59	6F	AD	F2
7D	47	6E	30
7D	63	7C	AF
D7	83	AB	D4

59	6F	AD	F2
47	6E	30	7D
7C	AF	7D	63
D4	D7	83	AB

c. Mix Colums atau Pencampuran kolom.

Dalam proses mix colums atau pencampuran kolom ada beberapa aturan khusus. Transformasi yang dilakukan yaitu dengan proses seperti perkalian matriks namun dengan menggunakan XOR. Berikut adalah contoh gambaran mix kolom.

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

s-box

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

hasil dari shift rows

a’	b’	c’	d’
e’	f’	g’	h’
i’	j’	k’	l’
m’	n’	o’	p’

hasil mix kolom

Cara melakukan mix kolom seperti perkalian matriks baris x kolom:

a’ = {2.a} XOR {3.e} XOR {1.i} XOR {1.m}

e’= {1.a} XOR {2.e} XOR {3.i} XOR {1.m}

i’= {1.a} XOR {1.e} XOR {2.i} XOR {3.m}

m’= {3.a} XOR {1.e} XOR {1.i} XOR {2.m}

b’ = {2.b} XOR {3.f} XOR {1.j} XOR {1.n}

f’= {1.a} XOR {2.f} XOR {3.j} XOR {1.n}

j’= {1.a} XOR {1.f} XOR {2.j} XOR {3.n}

n’= {3.a} XOR {1.f} XOR {1.j} XOR {2.n}

c’ = {2.c} XOR {3.g} XOR {1.k} XOR {1.o}

g’= {1.c} XOR {2.g} XOR {3.k} XOR {1.o}

k’= {1.c} XOR {1.g} XOR {2.k} XOR {3.o}

o’= {3.c} XOR {1.g} XOR {1.k} XOR {2.o}

d’ = {2.d} XOR {3.h} XOR {1.l} XOR {1.p}

h’= {1.d} XOR {2.h} XOR {3.l} XOR {1.p}

l’= {1.d} XOR {1.h} XOR {2.l} XOR {3.p}

p’= {3.d} XOR {1.h} XOR {1.l} XOR {2.p}

Ada catatan penting dalam melakukan mix kolom yang harus diperhatikan yaitu apabila bilangan dimultiplikasi dengan 2 dan angka biner paling kiri dari bilangan tersebut adalah 1 maka digit biner dari bilangan

tersebut digeser 1 digit ke kiri dan ditambahkan 0 pada bagian kanan serta nilai multiplikasi untuk 2 digunakan {0001 1011} dengan operasi xor, tetapi apabila digit biner paling kiri adalah 0 maka bilangan tersebut langsung di kalikan (multiplikasi) dengan 2 {0000 0010}. Apabila di multiplikasi dengan 3 digunakan aturan sebagai berikut. Bilangan biner dari 3 = 11, 11 = 10 xor 01 atau 2 xor 1, sehingga misalnya {a.3} = {a.2} xor {a}.

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

Matriks Mix kolom

59	6F	AD	F2
47	6E	30	7D
7C	AF	7D	63
D4	D7	83	AB

untuk menghitung baris 1 kolom 1

a’ = {2.59} XOR {3.47} XOR {1.7C} XOR {1.D4}

Bilangan biner dari 59 = 0101 1001 (Digit paling kiri adalah 0 sehingga dilakukan perkalian biasa terhadap 2 = 10) , sehingga

{ 2.59 } = 10 x 0101 1001 = **1011 0010**

sedangkan {3.47} = {2.47} xor {47}

47 = 0100 0111 (paling kiri adalah 0)

{2.47} = 0100 0111 x 10 = 1000 1110

{ 3.47 } = 1000 1110 xor 0100 0111 = **1100 1001**

{ 1.7C } = 7C = **0111 1100**

{ 1.D4 } = D4 = **1101 0100**

a’ = 1011 0010 xor 1100 1001 xor 0111 1100 xor 1101 0100

= 1110 1111 = **D3**

dilakukan proses yang sama untuk setiap kolom yang lain.

d. Penambahan kunci

Transformasi penambahan kunci dilakukan pada putaran ke 1 sampai ke 10. Proses ke 4 adalah proses xor hasil dari mix kolom terhadap hasil penambahan kunci.

H_{11}	H_{12}	H_{13}	H_{14}
H_{21}	H_{22}	H_{23}	H_{24}
H_{31}	H_{32}	H_{33}	H_{34}
H_{41}	H_{42}	H_{43}	H_{44}

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

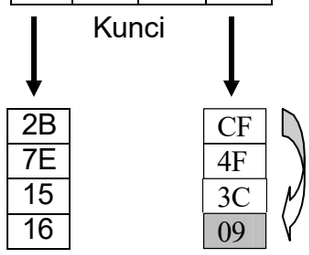
Key/Kunci

H11 – H44 adalah hasil dari proses mix kolom.

Proses Penambahan kunci dilakukan sebagai berikut.

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

Kunci

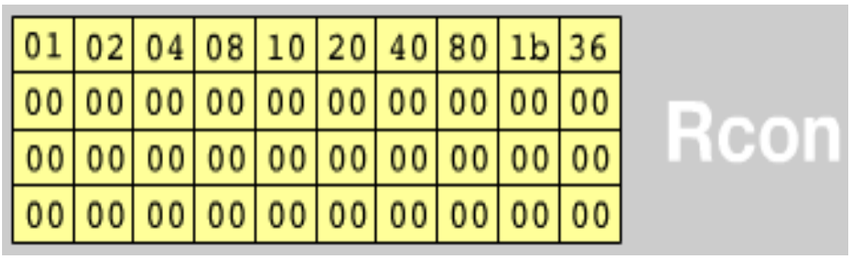


Langkah pertama yaitu kolom 1 dan kolom 4 yang digunakan sebagai isi dari kolom 1 kunci baru. Pada kolom ke 4, baris pertama digeser ke bawah 1 kali. Kemudian di substitusi dengan S-BOX.

Hasil Substitusi kolom ke empat dengan s-box.

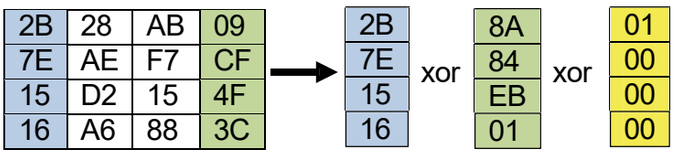
8A
84
EB
01

Rcon adalah komponen dari putaran tiap larik kata dalam perhitungan kunci



Gambar 4.6. Rcon

Lakukan proses perhitungan sebagai berikut.



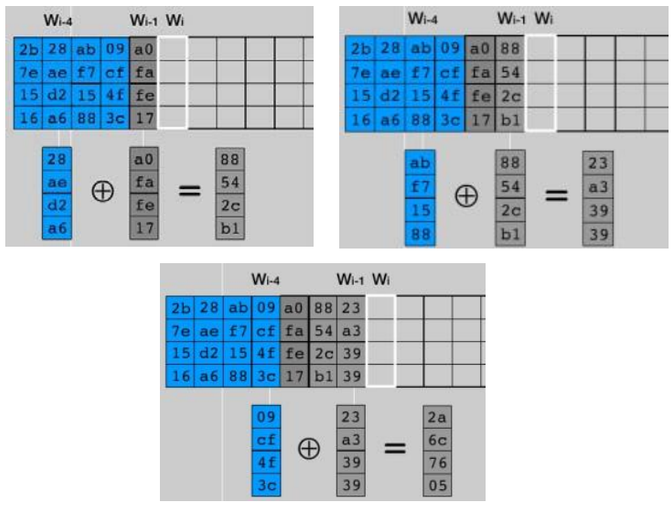
Key

Sehingga menghasilkan :

A0	88	23	2A
FA	54	A3	6C
FE	2C	39	76
17	B1	39	05

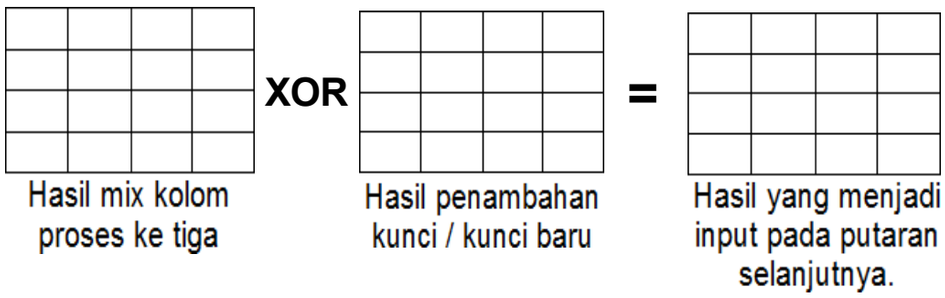
Hasil Penambahan kunci

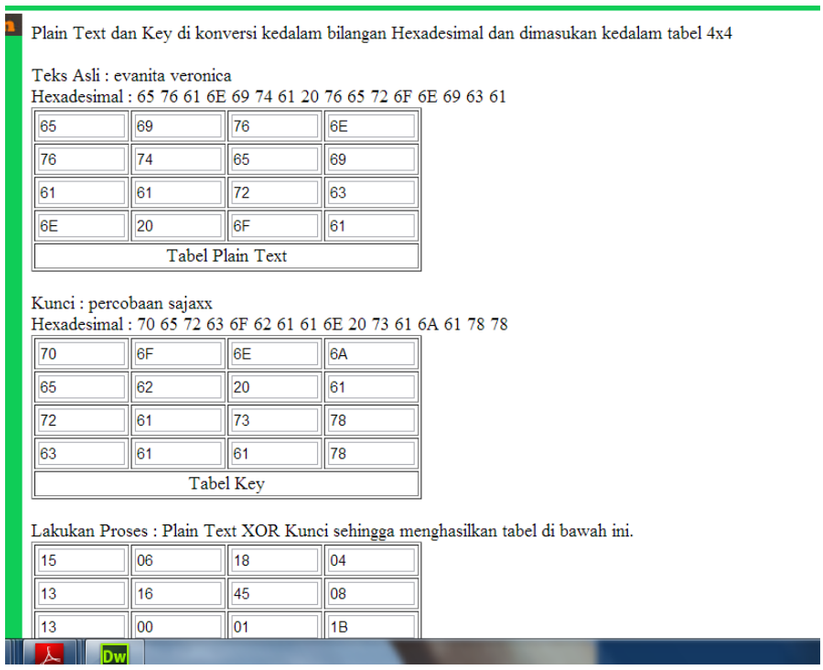
Dalam proses penjadwalan kunci, pada kolom pertama saja yang perhitungannya berbeda yaitu menggunakan s-box dan r-con. sedangkan untuk kolom 2, 3 dan 4 langsung di xor terhadap kolom kunci sebelumnya seperti terlihat pada Gambar 4.7.



Gambar 4.7. Gambaran proses penjadwalan kunci untuk kolom 2,3,4

Setelah kunci baru terbentuk lakukan proses xor hasil dari mix kolom dengan kunci baru, sehingga hasilnya menjadi input pada putaran selanjutnya.




Plain Text dan Key di konversi kedalam bilangan Hexadesimal dan dimasukan kedalam tabel 4x4

Teks Asli : evanita veronica
Hexadesimal : 65 76 61 6E 69 74 61 20 76 65 72 6F 6E 69 63 61

65	69	76	6E
76	74	65	69
61	61	72	63
6E	20	6F	61

Tabel Plain Text

Kunci : percobaan sajaxx
Hexadesimal : 70 65 72 63 6F 62 61 61 6E 20 73 61 6A 61 78 78

70	6F	6E	6A
65	62	20	61
72	61	73	78
63	61	61	78

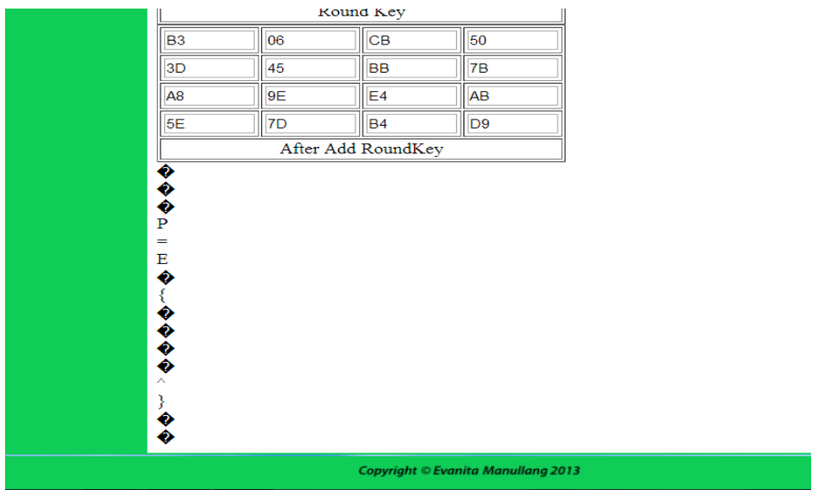
Tabel Key

Lakukan Proses : Plain Text XOR Kunci sehingga menghasilkan tabel di bawah ini.

15	06	18	04
13	16	45	08
13	00	01	1B

Gambar 4.8. Tampilan proses enkripsi rinjael

Gambar 4.8 menunjukkan langkah pertama proses enkripsi rindael. Proses akan ditampilkan hingga putaran ke 10 dan ditampilkan hasil enkripsi dari algoritma tersebut seperti pada Gambar 4.9 berikut.


Round Key

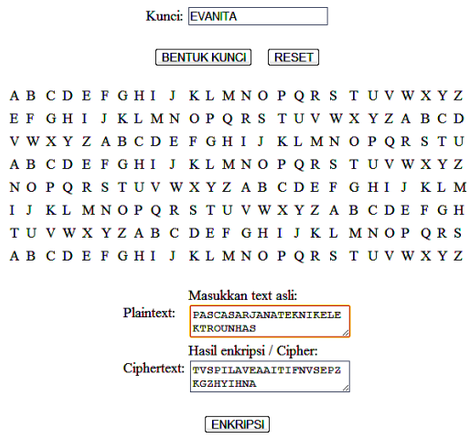
B3	06	CB	50
3D	45	BB	7B
A8	9E	E4	AB
5E	7D	B4	D9

After Add RoundKey

Copyright © Evanita Manullang 2013

Gambar 4.9. Tampilan hasil enkripsi rijndael

Beberapa algoritma lain yang diimplementasikan yaitu Vigenere, Caesar, dan Transposisi.



Gambar 4.10. Tampilan vigenere cipher

Vigenere merupakan salah satu algoritma substitusi. Proses awal algoritma vigenere yaitu pembentukan kunci dimana semua huruf disusun perbaris dimulai dari kata kunci yang diberikan. contoh kata kunci “UNHAS” maka proses pembentukan kunci sebagai berikut.

baris	A	B	C	D	E	F	G	H	…
1	U	V	W	X	Y	Z	A	B	…
2	N	O	P	Q	R	S	T	U	…
3	H	I	J	K	L	M	N	O	…
4	A	B	C	D	E	F	G	H	…
5	S	T	U	V	W	X	Y	Z	…

Setelah kunci terbentuk maka masukkan teks asli misalnya “cabe”, maka proses enkripsi dilakukan dengan cara huruf pertama di lihat dari baris pertama, huruf ke dua dari baris ke dua dan seterusnya hingga kembali ke baris 1.

Huruf “C” pada baris pertama : W

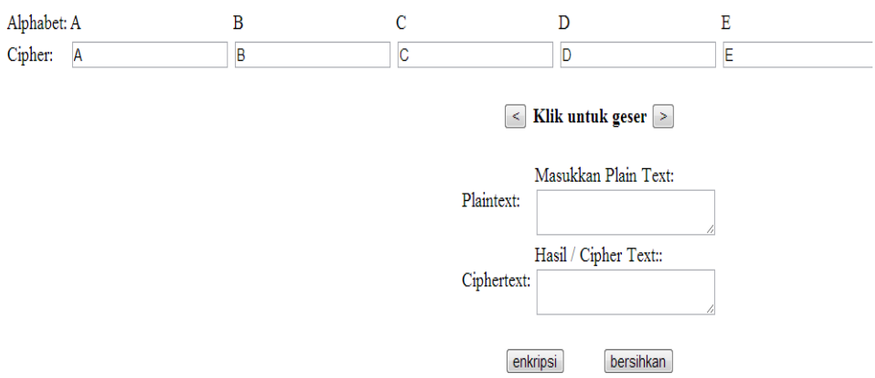
Huruf “A” pada baris kedua : N

Huruf “B” pada baris ketiga I

Huruf “E” pada baris keempat : E

Sehingga hasil enkripsi kata “CABE” dengan kunci “UNHAS” hasilnya adalah “WNIE”.

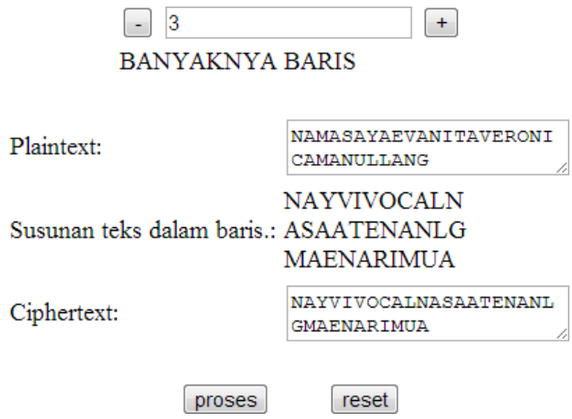
Selain Vigenere ada juga algoritma yang menggunakan teknik substitusi yaitu Caesar cipher. Perbedaan vigenere dan caesar terdapat pada proses pembentukan kunci. Kunci pada caesar lebih sederhana yaitu hanya melakukan pergeseran posisi huruf A – Z seperti ditunjukkan pada Gambar 4.11.



Gambar 4.11. Tampilan caesar cipher

Pada gambar 4.11 apabila tombol geser ke kiri ditekan satu kali maka Huruf B pada baris cipher akan bergeser satu kolom sehingga posisi B berada di bawah Alphabet A. pergeseran ke kiri atau ke kanan ditentukan berapa kali pengguna menekan tombol geser “<” dan “>”. Setelah melakukan pergeseran kunci maka teks asli akan diubah sesuai dengan huruf cipher di

bawah baris alphabet. Selain menggunakan teknik substitusi ada juga teknik transposisi seperti ditunjukkan Gambar 4.12.



Gambar 4.12. Tampilan transposisi cipher

Pada teknik transposisi terdapat beberapa pola transposisi namun dalam implementasi penulis baru membuat pola baris menurun. misalnya teks asli “NAMA SAYA EVANITA MANULLANG” maka apabila pengguna memilih 3 baris, kata tersebut disusun dalam 3 baris dan akan dibaca mendatar.

1	N	A	Y	V	I	M	U	A
2	A	S	A	A	T	A	L	N
3	M	A	E	N	A	N	L	G

Maka sususan hasil transposisi yaitu : “NAYVIMUA ASAATALN MAENANLG”.

.

B. PEMBAHASAN

1. Analisis Kebutuhan

Pembuatan sistem perangkat lunak ini didasarkan pada teori CAL (*Computer Aided Learning*) dan metode psikologi belajar yang telah dijelaskan pada bab 2. Oleh karena itu, pembuatan sistem perangkat lunak ini membutuhkan suatu analisis sistem agar sistem ini dapat diterima dan bermanfaat. Untuk mendukung analisis sistem, diberikan (Lampiran 1) Garis Besar Program Perkuliahan (GBPP) mata kuliah kriptografi dan keamanan komputer yang menunjukkan bahwa aplikasi pembelajaran ini dibutuhkan oleh mahasiswa.

2. Pengujian Sistem

Pada bagian ini akan dijelaskan mengenai pengujian perangkat lunak yang telah selesai dibuat. Secara garis besar pengujian yang dilakukan dibagi menjadi tiga bagian, antara lain:

a) Pengujian dasar teori.

Pengujian ini dilakukan untuk membandingkan kekurangan dan kelebihan dari aplikasi pembelajaran kriptologi yang telah dibuat dengan perangkat lunak pembelajaran lain yang sejenis, misalnya adalah animasi rijndael, cryptool, Perangkat lunak pembelajaran GOST. Aplikasi Pembelajaran sebelumnya memiliki beberapa kelemahan, diantaranya adalah:

1. Pemaparan proses matematis kriptografi kurang detail, hanya menampilkan hasil-hasil dari prosesnya saja (cryptool,animasi rijndael)
2. hanya terdapat satu algoritma saja dalam satu aplikasi pembelajaran. (GOST)
3. Tidak disertakannya teori yang menyangkut kriptografi. (cryptool,animasi rijndael)

Dalam perangkat lunak yang dibuat ini, dasar penekanan ini ditekankan pada prosesnya yang dinamis dengan interaktif pemakai. Hal ini berguna untuk menghilangkan kesan statis pada aplikasi tersebut. Materi yang ada berupa pemaparan dalam bentuk teks dan gambar bagan. Untuk mengatasi kelemahan pada perangkat lunak lain yang telah ada tersebut, maka perangkat lunak ini dilengkapi dengan beberapa fasilitas yang tidak dimiliki oleh perangkat lunak lain tersebut.

b) Pengujian kesesuaian fungsi dan proses aplikasi.

Pengujian dilakukan terhadap proses dan fungsi-fungsi yang ada pada aplikasi pembelajaran.

Tabel 4.1. Pengujian fungsi dan proses aplikasi

NO	Point Pengujian	Benar	Salah
1.	Kesesuaian pengelompokan menu dengan pengelompokan kriptologi	✓	
2.	Kesesuaian content teori dengan buku sumber	✓	
3.	Hasil perhitungan aplikasi dengan hitungan manual	✓	
4.	Pemberian input sesuai paramater	✓	
5.	Proses yang ditampilkan sesuai dengan algoritma	✓	
6.	Penanganan error apabila tidak ada inputan salah satu parameter		✓

c). Pengujian Kualitas Sistem.

Pengujian kualitas sistem dilakukan dengan menyebarkan kuisioner menyangkut peranan sistem terhadap aktifitas pembelajaran kriptografi. Responden diambil 20 orang mahasiswa teknik informatika yang mengambil mata kuliah Keamanan Komputer, dimana mereka merupakan sasaran pengguna aplikasi ini.

Berikut daftar pertanyaan untuk mengukur peranan sistem terhadap pembelajaran kriptografi :

1) Apakah pengaturan tulisan, warna dan posisi tulisan padaperangkat lunak teratur dan mudah dibaca.
2) Apakah uraian proses yang ada pada perangkat lunak mampu membantu Anda memahami materi.
3) Apakah materi yang ada pada perangkat lunak sesuai dengan materi yang disampaikan dikelas.
4) Apakah pemaparan proses matematis yang ada dalam perangkat lunak sangat jelas.
5) Apakah pengoperasian perangkat lunak mudah bagi pengguna.
6) Apakah program saat dijalankan tidak terjadi error atau kesalahan.
7) Apakah belajar dari perangkat lunak ini lebih mudah dibanding belajar dari buku atau media lain.

Bentuk jawaban dari pertanyaan yang diajukan berupa skala penilalian antara 1 (satu) sampai 5 (lima) dengan deskripsi sebagai berikut :

(a) Angka 1 (satu) sangat buruk.

(b) Angka 2 (buruk)

(c) Angka 3 (cukup)

(d) Angka 4 (baik)

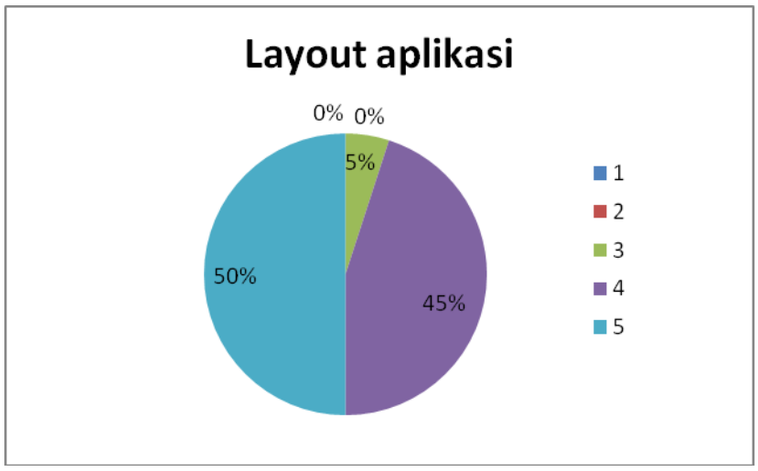
(e) Angka 5 (sangat baik)

Hasil nilai dari kuisioner yang diberikan adalah sebagai berikut :

Tabel 4.2. Hasil Kuisioner

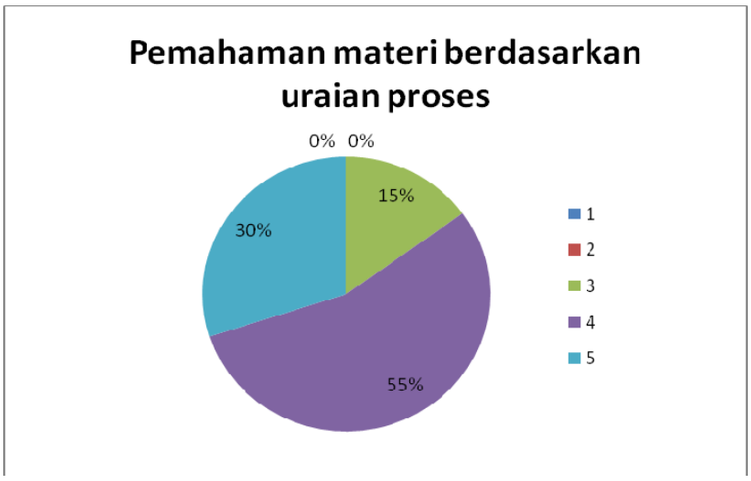
NO	Partisipan	Pertanyaan						
		1	2	3	4	5	6	7
1	Pengguna 1	4	3	4	4	5	5	5
2	Pengguna 2	4	3	4	4	5	5	5
3	Pengguna 3	5	4	4	4	4	5	5
4	Pengguna 4	4	4	4	4	4	5	5
5	Pengguna 5	5	5	4	4	4	5	4
6	Pengguna 6	3	3	4	3	4	5	4
7	Pengguna 7	4	4	5	4	4	4	5
8	Pengguna 8	4	4	5	5	4	4	5
9	Pengguna 9	5	5	4	5	4	4	4
10	Pengguna 10	4	4	4	4	3	4	5
11	Pengguna 11	4	5	4	4	3	5	5
12	Pengguna 12	5	4	4	5	3	5	5
13	Pengguna 13	4	4	4	4	3	4	5
14	Pengguna 14	5	4	4	4	4	3	4
15	Pengguna 15	5	5	4	5	4	4	5
16	Pengguna 16	5	5	4	5	4	4	5
17	Pengguna 17	5	5	4	4	4	4	4
18	Pengguna 18	4	4	4	5	4	3	4
19	Pengguna 19	5	4	4	5	4	3	5
20	Pengguna 20	5	4	4	5	4	4	4

Dari hasil kuisioner diatas dapat dibuat grafik berdasarkan pertanyaan yang diberikan adalah



Gambar 4.13. Hasil kuisioner layout aplikasi

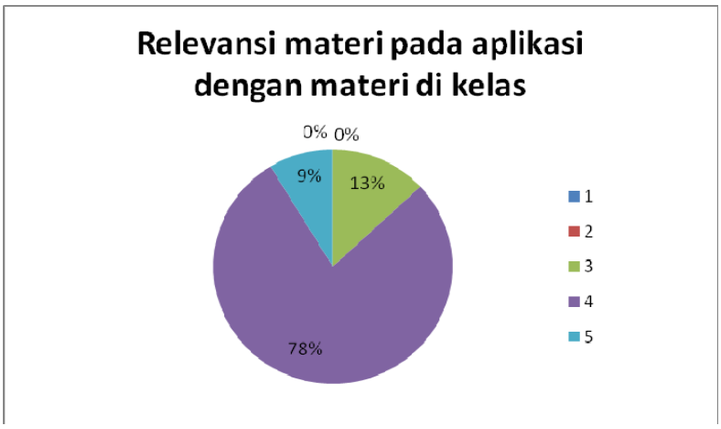
Gambar 4.13 menunjukkan 50% pengguna memberikan penilaian sangat baik terhadap desain layout dari aplikasi, sedangkan 45% menyatakan baik dan 5% menyatakan cukup baik.



Gambar 4.14. Hasil Kuisioner Uraian Proses

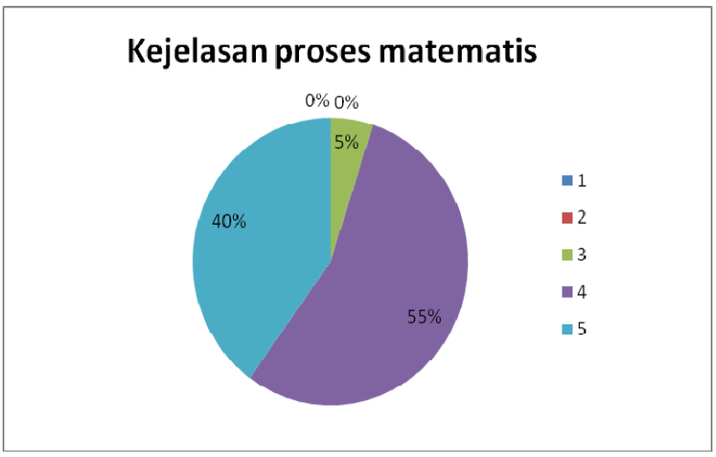
Gambar 4.14 menunjukkan 30% pengguna memberikan penilaian sangat baik terhadap pemahaman materi berdasarkan uraian proses pada

aplikasi pembelajaran, sedangkan 55% menyatakan baik dan 15% menyatakan cukup.



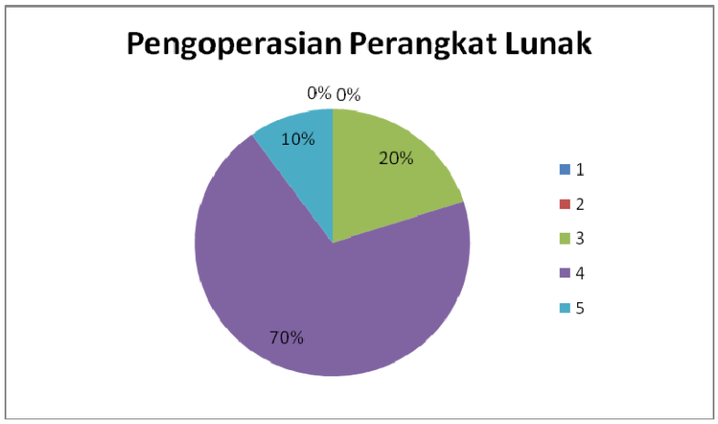
Gambar 4.15. Hasil Kuisioner Relevansi Terhadap Materi di Kelas

Gambar 4.15 menunjukkan 9% pengguna menyatakan bahwa materi yang disajikan pada aplikasi pembelajaran sangat relevan dengan materi yang dipelajari di kelas, sedangkan 78% menyatakan relevan, dan 13% menyatakan cukup relevan.



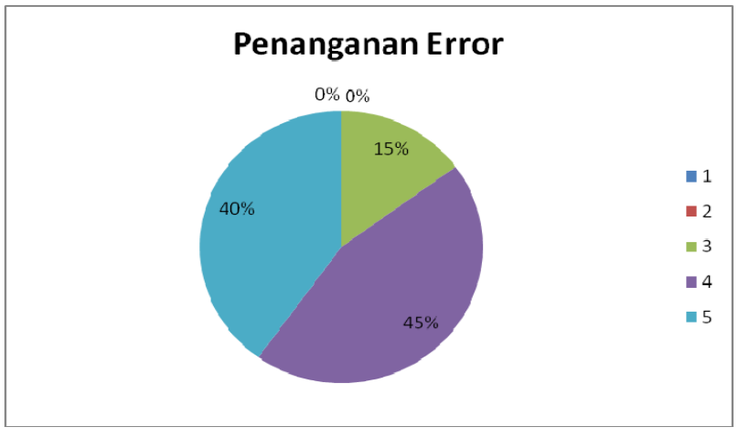
Gambar 4.16. Hasil Kuisioner Kejelasan Proses Matematis

Gambar 4.16 menunjukkan 40% pengguna menyatakan bahwa proses matematis yang disajikan pada aplikasi sangat jelas, dan 55% pengguna menyatakan jelas, sedangkan 5% pengguna menyatakan cukup jelas.



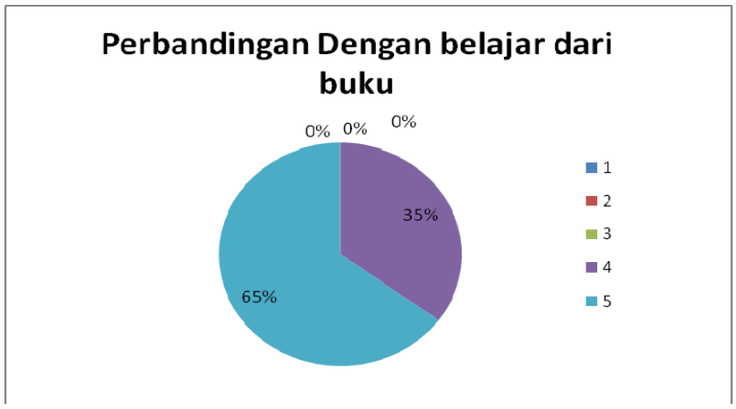
Gambar 4.17. Hasil Kuisioner Pengoperasian Perangkat Lunak

Gambar 4.17 menunjukkan 10% pengguna menyatakan bahwa cara mengoperasikan atau menggunakan aplikasi pembelajaran sangat mudah, sedangkan 70% pengguna menyatakan mudah, dan 20% menyatakan cukup mudah.



Gambar 4.18. Hasil Kuisioner Penanganan Eror pada Aplikasi

Gambar 4.18 menunjukkan 40% pengguna menyatakan penanganan error pada aplikasi sudah sangat baik, sedangkan 45 % pengguna menyatakan baik dan 15% pengguna menyatakan cukup baik.



Gambar 4.19. Hasil Kuisioner Perbandingan Belajar

Gambar 4.19 menyatakan 65% pengguna sangat setuju bahwa lebih mudah mempelajari algoritma kriptografi menggunakan aplikasi pembelajaran dibandingkan menggunakan buku, sedangkan 35% pengguna menyatakan setuju.

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan sebelumnya, maka dapat ditarik kesimpulan sebagai berikut:

1. Dari penelitian ini dihasilkan sebuah aplikasi baru pembelajaran kriptologi. Aplikasi yang dibangun menguraikan proses matematis dari kriptografi simetris dan asimetris yang dapat membantu mahasiswa mempelajari algoritma kriptologi.
2. Aplikasi yang dibuat belum sempurna dan belum lengkap dikarenakan keterbatasan waktu dan penulis sehingga diharapkan aplikasi pembelajaran ini tidak berhenti sampai disini tetapi semakin dikembangkan secara luas, karena aplikasi ini akan dipublikasikan sehingga lebih mudah untuk dikembangkan.

B. Saran

Penulis ingin memberikan beberapa saran yang mungkin dapat membantu dalam pengembangan aplikasi pembelajaran kriptologi agar menjadi lebih baik, yaitu :

1. Penambahan berbagai jenis algoritma sehingga semakin baik dalam proses pembelajaran, proses enkripsi asimetris dan dekripsi.

2. Pembuatan teori matematika yang berkaitan dengan kriptologi serta proses pengujiannya.
3. Pembuatan game-game sederhana yang mengandung kriptografi.
4. Studi lanjut guna pengembangan penelitian.

DAFTAR PUSTAKA

Moeis Dikwan, 2011, Perangkat Lunak Penunjang Pembelajaran dengan Metode GOST, Jurnal Tesis Informatika UNHAS.

Nufus Hayatun, 2009, Pembuatan Aplikasi Kriptografi Algoritma Base64 Menggunakan Java jdk 1.6, *Jurnal Universitas Gunadarma*.

Satria Eko, 2009, Studi Algoritma Rijndael Dalam Sistem Keamanan Data, *Jurnal Skripsi Universitas Sumatera Utara*.

Zelviana Anandia, Efendy Syahril, Arisandy Dedy, 2012, Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa, Jurnal Dunia Teknologi Informasi Vol1.

Ariyus Dony, 2008, Pengantar Ilmu Kriptografi, Penerbit Andi, Yogyakarta.

Berman Pamela, 2006, E-Learning Concepts and Techniques, Bloomsburg University of Pennsylvania, USA.

Henk C.A van Tilborg, 2000, Fundamentals Of Cryptology, Kluwer Academic Publisher, London.

Menezes, Oorschot and Vanstone,1997, Handbook of Applied Cryptography, CRC Press, Inc.

Pressman Roger S, 2005, *"Software Engineering", 6th Edition*, The MacGraw-Hill Companies, Inc., Newyork.

Schneier Bruce, 1996, Applied Cryptography, www.schneier.com, Second Edition.

Sommerville Ian, 2003, *"Software Engineering", 6th Edition*, Erlangga, Jakarta.

Stalling William, 2011, Cryptography and Network Security Principles and Practice Fifth Edition, Prentice Hall.

www.cryptool.org (diakses 20 November 2012)

GARIS-GARIS BESAR PROGRAM PERKULIAHAN
(GBPP)

Mata Kuliah: Kriptografi;
Kode/Bobot: TSK 411 / 3 sks;
Deskripsi Mata Kuliah: Mata kuliah ini membahas tentang arti kriptografi dan tujuan dari kriptografi; kriptografi kunci publik dan kriptografi kunci rahasia; algoritma-algoritma kriptografi klasik; *Block Cipher*; Data Encryption Standard (DES); *fast exponentiation;* RSA; Rabin-Williams Cryptosystem; El Gamal Encryption; Advanced Encryption Standard (AES); *Hash function* dan MD5; Kriptografi dan *e-commerce*; serta *Watermarking* dan steganografi.
Standar Kompetensi: Mahasiswa akan dapat memahami pilar konsep kriptografi dalam menyelesaikan, menganalisis masalah, dan dan dapat menjelaskan aplikasi kriptografi dalam keamanan komputer dan jaringan.

No	Kompetensi Dasar Hard Skill	Pokok Bahasan	Sub-pokok Bahasan	Kompetensi Dasar Soft Skills	Metode	Media	Waktu (menit)	Daftar
1	2	3	4	5	6			
1	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan definisi tentang kriptografi, enkripsi, dekripsi, kriptografi kunci publik dan kriptografi kunci rahasia paling sedikit 80% tepat.	1. Pendahuluan tentang Kriptografi	1.1 Pengertian tentang Kriptografi: enkripsi dan dekripsi 1.2 Kriptografi kunci publik 1.3 kriptografi kunci rahasia.	Responsif dan komunikatif	Ceramah Diskusi	LCD dan notebook	3 x 50	[1] [2] [4]
2	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat mengerjakan soal-soal algoritma kriptografi klasik: *Caesar cipher, playfair, matrix*	2. Algoritma kriptografi klasik	2.1 Caesar cipher 2.2 Playfair 2.3 Matrix encryption 2.4 Vigenere cipher 2.5 Vernam cipher	Kreatif Inovasi Analisis Inisiatif	Discover Learning Diskusi	LCD dan notebook	3 x 50	[1] [2]

	encrypt-ion, vigenere cipher, dan *vernam cipher*							
3.	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan dan mengerjakan soal-soal tentang *Block Cipher*: ECB, CBC, CFB, OFB, dan *Feistel Cipher* paling sedikit 80% tepat.	3. *Block Cipher*	3.1 Electronic Codebook (ECB) 3.2 Cipher Block Chainning (CBC) 3.3 Cipher Feedback Mode (CFB) 3.4 Output Feedback (OFB) 3.5 Feistel Cipher	Kemandirian Kreatif Bertanggung jawab Percaya diri ketekunan	Ceramah Diskusi	LCD dan notebook	6 x 50	[1] [2]
4.	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan konsep tentang algoritma Data Encryption Standard (DES) paling sedikit 80% tepat.	4. Data Encryption Standard (DES)	4.1 Latar belakang dan tujuan DES 4.2 *Initial Permutation*, Permutasi, substitusi pada DES 4.3 *Inner function* pada DES 4.4 Enkripsi DES 4.5 Dekripsi dan keamanan DES	Apresiasi Analogi/ imajinasi Empati Kreativitas Pengalaman, trampil	Ceramah Diskusi Latihan soal	LCD dan notebook	3 x 50	[1] [2] [3]
5	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan dan mengerjakan soal-soal tentang *Fast Exponentiation* dan algoritma RSA paling sedikit 80% tepat.	5. *Fast Exponentiation* dan Algoritma RSA.	5.1 Konsep modulo 5.2 Model *fast exponentiation* untuk menyelesaikan soal-soal modulo 5.3 Pembangkitan kunci dengan RSA 5.4 Enkripsi dengan RSA 5.5 Dekripsi dengan RSA	Apresiasi Analogi/ imajinasi Empati Kreativitas Pengalaman, trampil	Simulasi Diskusi Latihan soal	LCD dan notebook	3 x 50	[1] [2] [3]

6	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat mengerjakan soal-soal yang berhubungan dengan algoritma Rabin-Williams Cryptosystem dan paling sedikit 80% tepat.	6. Rabin-Williams Cryptosystem.	6.1 Enkripsi dengan Rabin-Williams Cryptosystem 6.2 Penentuan akar dan dekripsi pada Rabin-Williams.	▯ Apresiasi ▯ Analogi/ imajinasi ▯ Empati ▯ Kreativitas ▯ Pengalaman, trampil	▯ Simulasi ▯ Diskusi	LCD dan notebook	3 x 50	[1] [2] [4]
7.	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat mengerjakan soal-soal yang berhubungan dengan algoritma El-Gamal Encryption. paling sedikit 80% tepat.	7. El-Gamal Encryption.	7.1 Kunci publik dan kunci rahasia pada El-Gamal 7.2 Enkripsi dengan El-Gamal 7.3 Dekripsi pada El-Gamal	▯ Apresiasi ▯ Analogi/ imajinasi ▯ Empati ▯ Kreativitas ▯ Pengalaman, trampil	▯ Simulasi ▯ Diskusi	LCD dan notebook	3 x 50	[1] [3]
8	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan konsep dan mengerjakan soal-soal tentang algoritma Advanced Encryption Standard (AES-Rijndael) paling sedikit 80% tepat.	8. Advanced Encryption Standard (AES-Rijndael)	8.1 Alasan pengguna-an AES 8.1 Panjang kunci dan panjang blok 8.2 Enkripsi AES 8.3 Dekripsi AES 8.4 Keamanan AES	▯Sintesis ▯Analisis ▯Responsif ▯Apresiasi ▯Pengalaman	▯ Ceramah ▯ Diskusi ▯ Latihan soal	LCD dan notebook	6 x 50	[1] [2] [3]
9	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan konsep dan mengerjakan soal-soal tentang Fungsi Hash satu arah dan Message Digest 5 (MD5) paling sedikit 80% tepat.	9. Fungsi Hash satu arah dan Message Digest 5 (MD5)	9.1 Arti dan Tujuan Fungsi Hash 9.2 Aspek keamanan Fungsi Hash 9.3 Enkripsi dengan Algoritma MD5	▯ Prioritas ▯ Mengambil keputusan ▯ Berfikir kritis ▯ Selektif ▯ Tanggung jawab	▯ Problem Based Learning ▯ Ceramah ▯ Latihan soal	LCD dan notebook	6 x 50	[1] [2] [3]

10	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan dan mengerjakan soal-soal tentang aplikasi kriptografi dalam e-Commerce paling sedikit 80% tepat.	10. Kriptografi dan *e-Commerce*	10.1 Aplikasi kriptografi dalam *e-commerce* 10.2 Tanda tangan digital 10.3 Tanda tangan buta 10.4 Kontrak Digital 10.5 Protokol SET	Sintesis Analisis Responsif Apresiasi Pengalaman	Problem Based Learning Ceramah Latihan soal	LCD dan notebook	6 x 50	[1] [2] [3]
11	Setelah menyelesaikan pokok bahasan ini, mahasiswa Program Studi Sistem Komputer akan dapat menjelaskan dan mengerjakan soal-soal tentang Steganografi paling sedikit 80% tepat.	11. *Watermarking* (tanda-air) dan Steganografi	11.1 Beda kriptografi dan steganografi 11.2 Aplikasi water-marking dan steganografi 11.3 Cara penyembunyian informasi dalam steganografi	Apresiasi Analogi/ imajinasi Empati Kreativitas Pengalaman, trampil	Problem Based Learning Ceramah Latihan soal	LCD dan notebook	3 x 50	[1] [2]

Referensi

1. Menezes, A.J., P.C. van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1996.
2. Pfleeger, C.P., *Security in Computing, 2nd ed.*, Prentice-Hall International, Inc., New Jersey, 1997
3. Schneider, B. *Applied Cryptography*, John Wiley & Sons, New York, 1994.
4. Tanenbaum, A.S., *Jaringan Komputer* (Edisi Indonesia Dari Computer Network) Edisi III, Prenhallindo, Jakarta, 1997

GARIS–GARIS BESAR PROGRAM PENGAJARAN (GBPP)

PROGRAM STUDI : MANAJEMEN INFORMATIKA D-3
JUDUL MATA KULIAH : **KEAMANAN SISTEM INFORMASI**
NOMOR KODE / SKS : / 3
DESKRIPSI SINGKAT : MEMBAHAS PENTINGNYA TEKNOLOGI INFORMASI DAN KEAMANAN SISTEM INFORMASI, MENYUSUN MANAJEMEN, RENCANA DAN KEBIJAKAN KEAMANAN SISTEM INFORMASI DALAM ORGANISASI SERTA IMPLIKASINYA TERHADAP HUKUM DAN ETIKA.

TUJUAN INSTRUKSIONAL UMUM : MAHASISWA DAPAT MENJELASKAN DAN MENYUSUN PERENCANAAN KEAMANAN, MENYUSUN KEBIJAKAN KEAMANAN, MEMBANGUN PROGRAM PENGAMANAN, MEMPERKIRAKAN DAN MENGELOLA RISIKO, MENYUSUN MEKANISME PROTEKSI KEAMANAN, MENGENAL METODE DAN TEKNIK ENKRIPSI DAN MENGETAHUI HUKUM DAN ETIKA PADA KEAMANAN SIFO

NO	TUJUAN INSTRUKSIONAL KHUSUS	POKOK BAHASAN	SUB POKOK BAHASAN	ES. WAKTU	SUMBER KEPUSTAKAAN
1	2	3	4	5	6
1	Mahasiswa dapat menjelaskan pentingnya IT dan ketertarikan masyarakat terhadap keamanan sistem informasi	Keamanan Sistem Informasi	1. Pengantar Keamanan Sistem Informasi 2. Area spesialisasi dari keamanan 3. Komponen Keamanan Sifo	150	Buku 1, Hal 1
2-3	Mahasiswa dapat menyusun rencana keamanan dan konsep pengelolaan keamanan sistem informasi	Managemen Keamanan Sistem dan Perencanaan	1. Pengantar Managemen Keamanan Informasi a. Perbedaan antara leadership dan managemen b. Prinsip managemen keamanan sistem 2. Perencanaan (*Planning*) untuk Keamanan a. Komponen perencanaan keamanan informasi 3. Pendekatan implementasi keamanan informasi a. Pendekatan Top-Down dan Bottom-Up b. SDLC dan SecSDLC	300	Buku 1, Hal 1 Buku 1, Hal 25
4-5	Mahasiswa dapat menjelaskan kemungkinan2 yang mempengaruhi keamanan sistem serta dapat menyusun rencana, menerapkan dan memelihara kebijakan keamanan sistem	Perencanaan Terhadap Kemungkinan & Kebijakan Keamanan Sistem	*1.* Perencanaan *Contingencies* a. Komponen Perencanaan *Contingency* a.1.Incident Response a.2.Disaster recovery	300	Buku 1, Hal 63 Buku 8, SP800-34

NO	TUJUAN INSTRUKSIONAL KHUSUS	POKOK BAHASAN	SUB POKOK BAHASAN	ES. WAKTU	SUMBER KEPUSTAKAAN
1	2	3	4	5	6
	informasi		a.3.Business Continuity b. Testing Perencanaan *Contingency* 2. Kebijakan Keamanan Sistem a. Kebijakan keamanan sistem enterprise b. Isu seputar kebijakan keamanan c. Kebijakan sistem spesifik d. Panduan untuk kebijakan managemen e. Access Control List (ACL)		Buku 1, Hal 105
6-7	Mahasiswa dapat membangun program keamanan sistem dan memodel serta mengelola keamanan dalam penerapannya dalam sebuah oragnisasi	Program Keamanan, Model dan Penerapannya	1. Membangun Program Keamanan a. Variabel struktur program infosec (information security) b. Merancang struktur laporan untuk program infosec c. Komponen program keamanan d. Aturan keamanan informasi e. Implementasi program SETA 2. Model Managemen Keamanan dan Penerapannya a. Model managemen keamanan - ISO/IEC 17799 - NIST b. Penerapan keamanan informasi	300	Buku 1, Hal 155 Buku 1, Hal 209 http://iso17799world.com/auth.htm
8	Mahasiswa dapat mengetahui dan memahami bahaya, dampak dan mencegah spyware	Spyware	1. Pengertian Spyware 2. Pengolongan Spyware 3. Dampak Spyware 4. Pencegahan spyware	150	Internet
9-10	Mahasiswa dapat menjelaskan risiko serta mengelola risiko yang mungkin muncul dalam keamanan sistem	Manajemen Risiko	1. Mengidentifikasi dan Memperkirakan Risiko a. Manajemen risiko b. Identifikasi risiko c. Perkiraan risiko	300	Buku 1, Hal 285 Buku 8, SP800-30

NO	TUJUAN INSTRUKSIONAL KHUSUS	POKOK BAHASAN	SUB POKOK BAHASAN	ES. WAKTU	SUMBER KEPUSTAKAAN
1	2	3	4	5	6
			2. Memperkirakan dan Mengelola Risiko a. Strategi pengelolaan risiko b. Kategori kontrol c. *Feasibility Studi* dan *cost-benefit* analysis d. Penerapan pengelolaan risiko e. Metode OCTAVE		Buku 1, Hal 319 Buku 8, SP800-30
11-12	Mahasiswa dapat menyusun mekanisme proteksi	Mekanisme Proteksi	1. Mekanisme Proteksi a. Akses kontrol b. *Firewall* c. *Dial-up protection* d. *Intrusion detection system* e. *Cryptografi*	150	Buku 1, Hal 361
13	Mahasiswa dapat menjelaskan teknik teknik dan membuat enkripsi	Keamanan sistem dan kriptografi	1. Enkripsi dan dekripsi a. Pengertian enkripsi dan dekripsi b. Metode enkripsi c. Teknik-teknik enkripsi	150	Buku 2, Hal 31 Buku 6, hal. 61 Buku 9, hal. 43 Buku 10, hal. 21
14	Mahasiswa dapat menyusun personil yg profesional yang terlibat dalam posisi keamanan sistem informasi dalam sebuah organisasi	Personil dan Keamanan	1. Personil dan Keamanan a. Staf dan fungsi keamanan b. Profesional kemananan informasi c. Penetapan kebijakan	150	Buku 1, Hal 413
15	Mahasiswa dapat mengetahui hukum tentang teknologi informasi dan hukum informasi transaksi elektronik (ITE)	Hukum dan Etika	1. Hukum dan Etika Keamanan Sistem a. Hukum dan Etika b. Hukum TI c. Hukum ITE	150	Buku 1, Hal 451 Internet

Referensi Utama :

1. Whitman & Mattord,2004, **Management of Information Security**, Thomson Course Technology.

Referensi Tambahan :

2. Budi rahardjo,2005, **Keamanan sistem informai berbasis internet versi 5.3**, http://budi.insan.co.id
3. Dieter Gollmann, 2000, **Computer Security**, John Wiley & Sons, England
4. Internet dalam berbagai sumber referensi di mesin pencarian
5. ISO 17799 and BS7799 : http://iso17799world.com/auth.htm
6. Jennifer Sebery & Josef Pieprzyk,1989, **Cryptography : An Introduction to Computer Security**, Prentice Hall
7. Linda volonino and Stephen Robinson, 2004, **Principel and practice of information security**, Prentice hall
8. NIST, **SP800-12,26,30,34,100**, NIST Publications (http://csrc.nist.gov/publications/nistpubs/index.html)
9. Wahana, 2003, **Memahami model enkripsi dan security data**, Wahana Komputer dan Andi, Yogyakarta
10. William stallings, 1995, **Network dan internetwork security Principles and practice**, Prentice hall

WEBSITE :
http://afenprana.wordpress.com

Dosen Pengasuh,

Afen Prana, S.T

1. GARIS BESAR PROGRAM PENGAJARAN (GBPP)

Mata Kuliah : Keamanan Komputer
Kode / Bobot SKS : TKC165 / 3
Deskripsi Mata Kuliah : Mata kuliah ini membahas mengenai konsep dasar pengamanan komputer sebagai sistem *stand-alone* sekaligus lebih memfokuskan pada pengamanan jaringan komputer, protokol komunikasi TCP/IP, jaringan Internet, Malware/ *Malicious software*, jenis-jenis serangan pada sistem komputer, paradigma hacker dan teknik kriptografi.
TIU : Mahasiswa mempunyai pemahaman terhadap 3 konsep menyeluruh mengenai pengamanan pada sistem komputer berkaitan dengan *People*, *Process*, dan *Technology* (PPT)

No	TIK	Pokok Bahasan	Sub Pokok Bahasan	Estimasi Waktu	Metoda Pembelajaran	Media Pembelajaran	Pustaka
1	2	3	4	5	6	7	8
1	Menjelaskan konsep dasar keamanan pada sistem dan jaringan komputer serta trend keamanan sistem informasi dan *cybercrime*	Pendahuluan	• Definisi • Tujuan Perkuliahan • Komponen dari keamanan komputer • X.800 standar OSI • Ancaman-ancaman • Mekanisme dan Kebijakan (SOP)	3x50'	Ceramah, dan diskusi	• Hand out • Laptop/komputer • LCD	• 1,2,3,4,5,6 BAB 1
2	Menjelaskan konsep akses control dan mempraktekkan teori matrik akses kontrol (ACM)	Access Control Matrix (ACM)	• Overview • Model Access Control Matrix • Peralihan Protection State • Perintah-perintah dasar Ms.Windows dan Linux	3x50'	Ceramah, diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• 1, Bab 3 • 2, Bab 4.3 • 4, Bab 3
3	Mendemontrasikan paradigma teknik hacking : *foot printing, scanning target*	*Foot printing* dan *scanning target*	• Port dan Socket • Inner Footprinting • Outer Footprinting • Fase pengintaian • Fase *scanning*	3x50'	Ceramah, diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• 4,Bab 5 & 6 • 5,Bab 2 & 3 • 6, BAB 3 & 4
4	Mendemontrasikan paradigma teknik	•Memperoleh akses	• *Script Kiddies Exploit* • Password Attacks	3x50'	Ceramah, diskusi, tanya	• Hand out • Laptop/komputer	• 4, BAB 7,8,9,10,11

	hacking : cara memperoleh akses & mempertahankan hak akses dan cara menutupi jejak serta mempertahankan akses	•Mempertahankan hak akses •Menutupi jejak serta mempertahankan akses	• IP Address Spoofing • Netcat: A General-Purpose Network Tool • Denial-of-Service Attacks • Menutupi jejak serta mempertahankan akses		jawab dan latihan	• LCD	• 6, BAB 5,6 & 7
5	Menjelaskan jenis serangan tipe *Denial of Service Attack* (DoS), Buffer overflow & lubang keamanan pada *software* (*software vulnerabilities*)	• DoS • Buffer-overflow	• *Denial of Service Attack* (DoS) • Buffer overflow • *Software vulnerabilities*	3x50'	Ceramah, diskusi, dan tanya jawab	• Hand out • Laptop/kompute • LCD	• 2, BAB 3 • 4, BAB 7,9 • 5, BAB 8, 20
6	Menjelaskan jenis serangan tipe *Malware : Virus, Worm, Rootkit*	*Malware*	• *Virus* • *Worm* • *Rootkit* • Trojans • Backdoors	3x50'	Ceramah, diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• 2, BAB 6, 16 • 4, BAB 9, 10
7	Menjelaskan dan mempraktekan *Web Based Password Cracking Techniques*	*Web Based Password Cracking Techniques*	• Kelemahan umum aplikasi web • Metode • Memanipulasi input • Authentication dan Session Management • *Tools*	3x50'	Ceramah, diskusi, dan tanya jawab	• Hand out • Laptop/komputer • LCD	• 5, BAB 12
8	Menjelaskan dan mempraktekan SQL *Injection*	SQL *Injection*	• Pengenalan umum • *Kelemahan Server Side Scripting* • *SQL Injection* untuk mendapatkan akses sistem • *Scripts SQL Injection*	3x50'	Ceramah, Demonstrasi diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• 2, BAB 12
9	Menjelaskan dan mempraktekan *Hacking Wireless*	*Hacking Wireless Networks*	• Introduction to 802.11 • WEP • Cracking WEP Keys	3x50'	Ceramah, diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• 5, BAB 15

	Networks		• Sniffing Traffic • Wireless DoS attacks • WLAN Scanners • WLAN Sniffers				
10	Menjelaskan konsep dan desain penanganan pengamanan sistem	Desain penanganan pengamanan sistem	• Hardware • Software • Human Factor • Factors lain	3x50'	Ceramah, diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• 2, BAB 5
11	Mempraktekan teknik enkripsi metode klasikal	Enkripsi metode klasikal	• Definisi • Sejarah • Kriptografi dalam kehidupan sehari-hari • Algoritma kriptografi klasik berbasis karakter(Substitusi) • kriptografi kunci-simetri	3x50'	Ceramah, diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• 2, BAB 12 • 7, Bag.1 BAB 2 •
12	Mempraktekan teknik enkripsi metode moderen	Enkripsi metode moderen	• Blok Kriptografi Modern • Operasi bit xor • Operasi XOR Bitwise	3x50'	Ceramah, diskusi dan Tanya-jawab	• Hand out • Laptop/komputer • LCD	• 2, BAB 12.3 • 5, BAB 21 • 7, Bag.2 BAB 9,12
13	Menjelaskan mengenai *Watermarking* dan *Steganography*	*Watermarking* dan *Steganography*	• *Steganography* • *Spatial (time) domain* • *Frequency domain* • *Watermarking* • Visible Watermarking • Invisible Watermarking	3x50'	Ceramah, diskusi, dan latihan	• Hand out • Laptop/komputer • LCD	• www.outguess.org • www.demcom.com • www.cl.cam.ac.uk/~fapp2/steganography/index.html • www.digimarc.com
14	Menjelaskan jenis-jenis penipuan, kejahatan Internet dengan Social *Engineering*	Social *Engineering*	• Social *Engineering* • Faktor • Metode • Contoh	3x50'	Demonstrasi, diskusi dan praktik	• Hand out • Laptop/komputer • LCD	• 4, BAB 5 • 5, BAB 9 •

Lampiran Struktur file dan Coding dalam aplikasi

Struktur file aplikasi yaitu

Folder Utama diberi nama **tesis**,

sub folder dan file yang terdapat dalam folder tesis yaitu

Nama	Jenis	fungsi
Images	folder	sebagai tempat menyimpan file yang berupa gambar
css	folder	berisi file-file css yang digunakan oleh aplikasi
js	folder	berisi file-file javascript yang juga berguna untuk aplikasi
klasik	folder	berisi algoritma-algortima Simetris Klasis
modern	folder	berisi algoritma-algortima Simetris Modern
asimetris	folder	berisi algoritma-algortima Asimetris
kriptanalisis	folder	berisi algoritma kriptanalisis
index	file php	sebagai halaman utama program
home	file html	sebagai isi pada content awal program

Source Code

indek.php

```
<html>
<head>
<link rel="stylesheet" href="css/reset.css" type="text/css" media="all">
<link rel="stylesheet" href="css/grid.css" type="text/css" media="all">
<link rel="stylesheet" href="css/style.css" type="text/css" media="all">
<style type="text/css">
body {
	background-image: url(images/bg.jpeg);
}
</style>
<script type="text/javascript" src="js/jquery-1.4.2.min.js" ></script>
<script type="text/javascript" src="js/cufon-yui.js"></script>
<script type="text/javascript" src="js/Myriad_Pro_italic_400-
Myriad_Pro_italic_600.font.js"></script>
<script type="text/javascript" src="js/cufon-replace.js"></script>
<script type="text/javascript" src="js/jquery.faded.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<!--[if lt IE 7]>
<script type="text/javascript" src="js/ie_png.js"></script>
<script type="text/javascript">ie_png.fix('.png, .logo, .extra-
banner');</script>
<![endif]-->
<!--[if lt IE 9]><script type="text/javascript"
src="js/html5.js"></script><![endif]-->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

```
</head>
<body>
 <div id="wrap">
 <div id="header"><img src="images/header.jpg"></div>
       <div id="menuatas">
       <ul id="menu">
<li><a href="index.php?id=hm">Home</a></li>
<li>
<a href="#">kriptografi</a>
<ul>
<li><a href="index.php?id=cls">Simetris Klasik</a></li>
<li><a href="index.php?id=mod">Simetris Moderen</a></li>
</li>
<li><a href="index.php?id=as">Asimetris</a></li>
</ul>
</li>
<li><a href='kriptanalisis/kriptanalisisteori.php'
target='utama'>kriptanalisis</a></li>
</ul>
       </div>

<div id="tengah">
  <section id="content">
  <table width="960" height="0" border="0">
    <tr>
      <td width="200" height="0" align="center" bgcolor="#0FCD57"><table
cellpadding="5" cellspacing="5" class="menu">
        <?php
        if (isset($_GET['id']))
       {
      $id = $_REQUEST['id'];
         if ($id == 'as')
         {
        echo "
        <tr align = 'center'><td><img src='images/asimetris.jpg'></td></tr>
        <tr align = 'center' cellpadding='5' cellspacing='5'><td><a
href='asimetris/rsa/rsateori.php' target='utama'>RSA</a></td></tr>
        <tr align = 'center' cellpadding='5' cellspacing='5'><td><a
href='asimetris/elgamal/elgamalteori.php'
target='utama'>ELGAMAL</a></td></tr>
        <tr align = 'center' cellpadding='5' cellspacing='5'><td><a
href='asimetris/ecc/eccteori.php' target='utama'>ECC</a></td></tr>";
         }
         elseif ($id == 'cls'){
               echo "
               <tr align = 'center'><td><img
src='images/klasik.jpg'></td></tr>
        <tr align = 'center'><td><a href='klasik/vigenere/vigenereteori.php'
target='utama'>Vigenere</a></td></tr>
        <tr align = 'center'><td><a href='klasik/caesar/caesarteori.php'
target='utama'>Caesar</a></td></tr>
        <tr align = 'center'><td><a
href='klasik/kodegeser/kodegeserteori.php'
target='utama'>KodeGeser</a></td></tr>
        <tr align = 'center'><td><a href='klasik/hill/hillteori.php' 72 |
Page target='utama'>Hill</a></td></tr>
        <tr align = 'center'><td><a href='klasik/playfair/playfairteori.php'
target='utama'>Playfair</a></td></tr>
        <tr align = 'center'><td><a
href='klasik/transposisi/transposisiteori.php'
target='utama'>Transposisi</a></td></tr>";
         }
         elseif ($id == 'mod'){
```

```
          echo "
        <tr align = 'center'><td><img src='images/modern.jpg'></td></tr>
        <tr align = 'center'><td><a href='modern/des/desteori.php'
target='utama'>DES</a></td></tr>
        <tr align = 'center'><td><a href='modern/rijndael/rijndaelteori.php'
target='utama'>AES RIJNDAEL</a></td></tr>
        <tr align = 'center'><td><a href='modern/idea/ideateori.php'
target='utama'>IDEA</td></tr>
        <tr align = 'center'><td><a href='modern/a5/a5teori.php'
target='utama'>A5</td></tr>
        <tr align = 'center'><td><a href='modern/rc4/rc4teori.php'
target='utama'>RC4</td></tr>
                    ";
         }
         }
           ?></table></td>
      <td width="760">
         <script type="text/javascript" src="jquery-1.6.2.js"></script>
         <script type="text/javascript" src="jquery.iframe-auto-
height.plugin.js"></script>
        <iframe name="utama" width="760" height="" frameborder="0"
src="home.html" scrolling="yes"> </iframe>
        <script type="text/javascript">
      jQuery('iframe').iframeAutoHeight();
</script></td>
    </tr>
  </table>
</section>
</div>
    <div id="footer"><h1><center>Copyright &copy Evanita Manullang
2013</center></h></div>
</div>
</body>
</html>
```

Caesar Cipher

```
//-------------------- CAESAR CIPHER ---------------------//
function cc_Encipher()
{
    var cc_validChars = 'abcdefghijklmnopqrstuvwxyz ';
    var cc_plainText;
    var cc_cipherText;
    var cc_id;
    var cc_newText = '';

    cc_plainText = document.getElementById('cc-plainText').value;
    cc_cipherText = '';

    for (cc_a = 0; cc_a < cc_plainText.length; cc_a++)
    {
   if (cc_validChars.indexOf(cc_plainText.charAt(cc_a).toLowerCase()) != -1)
   {
   cc_id = 'cc-cipher-' + cc_plainText.charAt(cc_a).toLowerCase();
   cc_newText = cc_newText + cc_plainText.charAt(cc_a).toUpperCase();
   cc_cipherText = cc_cipherText + document.getElementById(cc_id).value;
        }
        else
        {
            cc_cipherText = cc_cipherText + '?';
        }
```

```
    }
    document.getElementById('cc-plainText').value = cc_newText;
    document.getElementById('cc-cipherText').value = cc_cipherText;
}
function cc_num2alpha(cc_n)
{

    var cc_alphabet = new Array(26);
    cc_alphabet[0] = 'a';
    cc_alphabet[1] = 'b';
    cc_alphabet[2] = 'c';
    cc_alphabet[3] = 'd';
    cc_alphabet[4] = 'e';
    cc_alphabet[5] = 'f';
    cc_alphabet[6] = 'g';
    cc_alphabet[7] = 'h';
    cc_alphabet[8] = 'i';
    cc_alphabet[9] = 'j';
    cc_alphabet[10] = 'k';
    cc_alphabet[11] = 'l';
    cc_alphabet[12] = 'm';
    cc_alphabet[13] = 'n';
    cc_alphabet[14] = 'o';
    cc_alphabet[15] = 'p';
    cc_alphabet[16] = 'q';
    cc_alphabet[17] = 'r';
    cc_alphabet[18] = 's';
    cc_alphabet[19] = 't';
    cc_alphabet[20] = 'u';
    cc_alphabet[21] = 'v';
    cc_alphabet[22] = 'w';
    cc_alphabet[23] = 'x';
    cc_alphabet[24] = 'y';
    cc_alphabet[25] = 'z';

    return cc_alphabet[cc_n];
}
function cc_shiftLeft()
{
    var cc_currentAlphabet = new Array(26);
    var cc_shiftAlphabet = new Array(26);
    var cc_temp_a;

    for (cc_b = 0; cc_b < 26; cc_b++)
    {
    cc_currentId = 'cc-cipher-' + cc_num2alpha(cc_b);
    cc_currentAlphabet[cc_b]= document.getElementById(cc_currentId).value;
    }
    cc_temp_a = cc_currentAlphabet[0];
    for(cc_c = 0; cc_c < 26; cc_c++)
    {
        cc_shiftAlphabet[cc_c] = cc_currentAlphabet[cc_c+1];
        if (cc_c == 25)
        {
          cc_shiftAlphabet[cc_c] = cc_temp_a;
        }
        cc_id = 'cc-cipher-' + cc_num2alpha(cc_c);
        document.getElementById(cc_id).value = cc_shiftAlphabet[cc_c];
    }
    cc_Encipher();
}
function cc_shiftRight()
{
```

```
    var cc_currentAlphabet = new Array(26);
    var cc_shiftAlphabet = new Array(26);
    var cc_temp_z;
    for (cc_d = 0; cc_d < 26; cc_d++)
    {
        cc_currentId = 'cc-cipher-' + cc_num2alpha(cc_d);
        cc_currentAlphabet[cc_d]=
document.getElementById(cc_currentId).value;
    }
    cc_temp_z = cc_currentAlphabet[25];
    for(cc_e = 0; cc_e < 26; cc_e++)
    {
        cc_shiftAlphabet[cc_e] = cc_currentAlphabet[cc_e-1];
        if (cc_e == 0)
        {
          cc_shiftAlphabet[cc_e] = cc_temp_z;
        }
        cc_id = 'cc-cipher-' + cc_num2alpha(cc_e);
        document.getElementById(cc_id).value = cc_shiftAlphabet[cc_e];
    }
    cc_Encipher();
}
function cc_Clear()
{
    document.getElementById('cc-plainText').value = '';
    document.getElementById('cc-cipherText').value = '';
}
</script>
<style type="text/css">
</style>
</head>
<body >

             <div id="pageFrame">
               <div id="masthead">

               <div id="masthead2">Klik tombol Geser ke kiri atau ke kanan
untuk mengubah posisi cipher, kemudian masukkan teks asli, setelah itu klik
tombol enkripsi. Proses enkripsi dilakukan dengan cara mengubah huruf pada
teks asli sesuai dengan cipher. </div>
               </div>
               <div id="contentColumn">
                 <div id="innerContentColumn">
                   <p> </p>
                   <table cellpadding="1">
  <tr>
<td>Alphabet:</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>M</td>
<td>N</td>
<td class="cc-app-heading">O</td>
<td class="cc-app-heading">P</td>
```

```
<td class="cc-app-heading">Q</td>
<td class="cc-app-heading">R</td>
<td class="cc-app-heading">S</td>
<td class="cc-app-heading">T</td>
<td class="cc-app-heading">U</td>
<td class="cc-app-heading">V</td>
<td class="cc-app-heading">W</td>
<td class="cc-app-heading">X</td>
<td class="cc-app-heading">Y</td>
<td class="cc-app-heading">Z</td>
</tr>
<tr>
<input id="cc-cipher- " type="hidden" value=" ">
<td>Cipher:</td>
<td><input type="text" id="cc-cipher-a" value="A" size="1"></td>
<td><input type="text" id="cc-cipher-b" value="B" size="1"></td>
<td><input type="text" id="cc-cipher-c" value="C" size="1"></td>
<td><input type="text" id="cc-cipher-d" value="D" size="1"></td>
<td><input type="text" id="cc-cipher-e" value="E" size="1"></td>
<td><input type="text" id="cc-cipher-f" value="F" size="1"></td>
<td><input type="text" id="cc-cipher-g" value="G" size="1"></td>
<td><input type="text" id="cc-cipher-h" value="H" size="1"></td>
<td><input type="text" id="cc-cipher-i" value="I" size="1"></td>
<td><input type="text" id="cc-cipher-j" value="J" size="1"></td>
<td><input type="text" id="cc-cipher-k" value="K" size="1"></td>
<td><input type="text" id="cc-cipher-l" value="L" size="1"></td>
<td><input type="text" id="cc-cipher-m" value="M" size="1"></td>
<td><input type="text" id="cc-cipher-n" value="N" size="1"></td>
<td><input type="text" id="cc-cipher-o" value="O" size="1"></td>
<td><input type="text" id="cc-cipher-p" value="P" size="1"></td>
<td><input type="text" id="cc-cipher-q" value="Q" size="1"></td>
<td><input type="text" id="cc-cipher-r" value="R" size="1"></td>
<td><input type="text" id="cc-cipher-s" value="S" size="1"></td>
<td><input type="text" id="cc-cipher-t" value="T" size="1"></td>
<td><input type="text" id="cc-cipher-u" value="U" size="1"></td>
<td><input type="text" id="cc-cipher-v" value="V" size="1"></td>
<td><input type="text" id="cc-cipher-w" value="W" size="1"></td>
<td><input type="text" id="cc-cipher-x" value="X" size="1"></td>
<td><input type="text" id="cc-cipher-y" value="Y" size="1"></td>
<td><input type="text" id="cc-cipher-z" value="Z" size="1"></td>
</tr>
</table>
<br>
<table align="center">
<tr>
<td        class="cc-app-shift"><input         type="submit"         value="<"
onclick="cc_shiftLeft();"></td>
<td    class="cc-app-shift"><div    align="center"><strong>    Klik    untuk
geser</strong></div></td>
<td        class="cc-app-shift"><input         type="submit"         value=">"
onclick="cc_shiftRight();"></td>
</tr>
</table>
<p><br>

</p>
<table id="cc-app-2" align="center" cellspacing="3">
  <tr>
<td class="cc-app-heading-2">Plaintext:</td>
<td class="cc-app-element">Masukkan Plain Text:<br>
  <textarea id="cc-plainText" class="cc-textarea"></textarea></td>
</tr>
<tr><td></td><td><center>
```

```
<input type="submit" value="enkripsi" onclick="cc_Encipher();">
 
<input type="submit" value="bersihkan" onclick="cc_Clear();">
</center></td></tr>
<tr>
<td class="cc-app-heading-2">Ciphertext:</td>
<td class="cc-app-element">Hasil / Cipher Text::<br>
  <textarea id="cc-cipherText" class="cc-textarea"></textarea></td>
</tr>
</table>
<br>

<h3></h3>
<p> </p>
<br>
                      </div>
                    </div>
                    <div id="footer">
                           <div id="innerFooter">
                      </div>
                    </div>
             </div>
       <script               src="http://www.google-analytics.com/urchin.js"
type="text/javascript"></script>
<script type="text/javascript">
_uacct = "UA-2036050-1";
urchinTracker();
</script>
</body>
</html>
```

Vigenere Cipher

```
<script language="javascript">
function buildSquare()
{
var squaretext = document.getElementById('squaretext').value.toUpperCase();
var    squarehtml    =    '<table    id="vs-app-square-table"    align="center"
cellspacing="1"        cellpadding="4"><tr        class="vs-app-square-alpha"
bgcolor="#28E415"><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</t
d><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td><td>
N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td>
<td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr>';
    var numStart;
    var alphabetKeys = new Array(6);
    var alphabets = new Array(6);

    if (squaretext != '')
    {

        document.getElementById('vs-plainText').disabled = false;
        document.getElementById('vs-plainText').value = '';
        document.getElementById('vs-cipherText').disabled = false;

        for(a = 0; a < squaretext.length; a++)
        {
            alphabets[a] = squaretext.charAt(a);
            alphabets[squaretext.charAt(a)] = new Array(26);
            squarehtml = squarehtml + '<tr><td class="vs-app-square-text"
bgcolor="#F95725">' + squaretext.charAt(a) + '</td>';
            alphabets[squaretext.charAt(a)][0] = squaretext.charAt(a);
            numStart = alpha2num(squaretext.charAt(a)) + 1;
```

```
            for(b = numStart, c = 1; b < numStart + 25; b++, c++)
            {
                if (b > 25)
                {
                    d = b - 26;
                }
                else
                {
                    d = b;
                }
                alphabets[squaretext.charAt(a)][c] = num2alpha(d);
                squarehtml = squarehtml + '<td class="vs-app-square-
elements">' + num2alpha(d) + '</td>';
            }
            squarehtml = squarehtml + '</tr>';
        }
        squarehtml = squarehtml + '</table>';
        document.getElementById('square').innerHTML = '';
        document.getElementById('square').innerHTML = squarehtml;
        document.getElementById('vs-plainText').focus();
        return alphabets;
    }
    else
    {
        window.alert('You must enter a Keyword');
        document.getElementById('squaretext').focus();
    }
}
function resetSquare()
{
    document.getElementById('square').innerHTML='';
    document.getElementById('squaretext').value='';
    document.getElementById('vs-plainText').disabled=true;
    document.getElementById('vs-plainText').value='First you must build your
Vigenere Square';
    document.getElementById('vs-cipherText').value='';
    document.getElementById('vs-cipherText').disabled=true;
    document.getElementById('squaretext').focus();
}
function writeCipher()
{
    var ValidChars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ';
    var text = document.getElementById('vs-plainText').value;
    var squaretextlength =
document.getElementById('squaretext').value.length;
    var cipher = '';
    var newtext = '';
    var alphabets = buildSquare();
    for (e = 0, f = 0; e < text.length; e++, f++)
    {
        if (ValidChars.indexOf(text.charAt(e).toUpperCase()) != -1)
        {
            if (f == squaretextlength)
            {
                f = 0;
            }
            newtext = newtext + text.charAt(e).toUpperCase();
            cipher = cipher +
alphabets[alphabets[f]][alpha2num(text.charAt(e).toUpperCase())];
        }
        else
        {
        }
```

```
   }
    document.getElementById('vs-plainText').value = newtext;
    document.getElementById('vs-cipherText').value = cipher;
}
function alpha2num(alpha)
{
    var alphabet_a = new Array(26);
    alphabet_a['A'] = 0;
    alphabet_a['B'] = 1;
    alphabet_a['C'] = 2;
    alphabet_a['D'] = 3;
    alphabet_a['E'] = 4;
    alphabet_a['F'] = 5;
    alphabet_a['G'] = 6;
    alphabet_a['H'] = 7;
    alphabet_a['I'] = 8;
    alphabet_a['J'] = 9;
    alphabet_a['K'] = 10;
    alphabet_a['L'] = 11;
    alphabet_a['M'] = 12;
    alphabet_a['N'] = 13;
    alphabet_a['O'] = 14;
    alphabet_a['P'] = 15;
    alphabet_a['Q'] = 16;
    alphabet_a['R'] = 17;
    alphabet_a['S'] = 18;
    alphabet_a['T'] = 19;
    alphabet_a['U'] = 20;
    alphabet_a['V'] = 21;
    alphabet_a['W'] = 22;
    alphabet_a['X'] = 23;
    alphabet_a['Y'] = 24;
    alphabet_a['Z'] = 25;

    return alphabet_a[alpha];
}
function num2alpha(n)
{
    var alphabet_n = new Array(26);
    alphabet_n[0] = 'A';
    alphabet_n[1] = 'B';
    alphabet_n[2] = 'C';
    alphabet_n[3] = 'D';
    alphabet_n[4] = 'E';
    alphabet_n[5] = 'F';
    alphabet_n[6] = 'G';
    alphabet_n[7] = 'H';
    alphabet_n[8] = 'I';
    alphabet_n[9] = 'J';
    alphabet_n[10] = 'K';
    alphabet_n[11] = 'L';
    alphabet_n[12] = 'M';
    alphabet_n[13] = 'N';
    alphabet_n[14] = 'O';
    alphabet_n[15] = 'P';
    alphabet_n[16] = 'Q';
    alphabet_n[17] = 'R';
    alphabet_n[18] = 'S';
    alphabet_n[19] = 'T';
    alphabet_n[20] = 'U';
    alphabet_n[21] = 'V';
    alphabet_n[22] = 'W';
    alphabet_n[23] = 'X';
```

```
    alphabet_n[24] = 'Y';
    alphabet_n[25] = 'Z';

    return alphabet_n[n];
}
</script>
</head>
<body >

             <div id="pageFrame">
               <div id="masthead">

               <div id="masthead2">
                 <p>Masukkan Kunci terlebih dahulu, kemudian pembentukan
kunci dilakukan dengan cara menyusun abjad kunci perbaris kemudian tiap
huruf pada kunci akan diteruskan sesuai abjad sehingga perubahan huruf
sesuai dengan urutan kunci.</p>
                 <p>Baris Pertama pembentukan kunci adalah SUSUNAN abjad
ASLI, baris selanjutnya adalah SUSUNAN abjad sesuai KUNCI.</p>
               </div>
               </div>
               <div id="contentColumn">
                 <div id="innerContentColumn">
                   <p>
<table id="vs-app" align="center" cellspacing="3">
  <tr>
<td class="vs-app-heading">Kunci:</td>
<td  class="vs-app-element"><input  id="squaretext"  type="text"  value=""
class="vs-app-keyword"></td>
</tr>
</table>

<br>
<center>
<input type="submit" value="BENTUK KUNCI" onclick="buildSquare();">
 
<input type="submit" value="RESET" onclick="resetSquare();">
</center>

<br>
<span id="square"></span>
<br>

<table width="388" align="center" cellspacing="3" id="vs-app">
<tr>
<td width="151" class="vs-app-heading">Plaintext:</td>
<td  width="224"  class="vs-app-element">Masukkan  text  asli:<br><textarea
id="vs-plainText"  class="vs-textarea"  disabled>BENTUK  KUNCI  TERLEBIH
DAHULU</textarea></td>
</tr>
<tr><td colspan="2"><center>
  <p>
    <input type="submit" value="ENKRIPSI" onclick="writeCipher();">
  </p>
  <p align="justify">Enkripsi dilakukan dengan cara mengubah huruf pada teks
asli seperti kunci yang dibentuk, huruf pertama disesuaikan dengan kunci
pada baris pertama, huruf ke dua pada baris kedua, demikian selanjutnya
sampai berulang kembali ke baris awal.</p>
</center></td></tr>
<tr>
<td class="vs-app-heading">Ciphertext:</td>
<td class="vs-app-element">Hasil enkripsi / Cipher:<br><textarea id="vs-
cipherText" class="vs-textarea" disabled></textarea></td>
```

```
</tr>
</table>

<br>

                  </div>
                     </div>
                     <div id="footer">
                            <div id="innerFooter"></div>
                     </div>
              </div>
       <script               src="http://www.google-analytics.com/urchin.js"
type="text/javascript"></script>
<script type="text/javascript">
_uacct = "UA-2036050-1";
urchinTracker();
</script>
</body>
</html>
```

TRANSPOSISI

```
<script language="javascript">
function writeRailFenceCipher()
{
    var lines;
    var text;
    var cipher = '';
    var cipherArray = new Array(lines);
    var railfencehtml = '';
    var newtext = '';

    lines = document.getElementById("lines").value;
    text = document.getElementById("rf-plainText").value;
    if (text != '')
    {
        for (p = 0; p < lines; p++)
        {
            cipherArray[p] = '';
        }
        for(n = 0, arr = 0; n < text.length; n++)
        {
            if (text.charAt(n) != ' ')
            {
                newtext = newtext + text.charAt(n).toUpperCase();
                if (arr == lines-1)
                {
                    arr = 0;
                }
                else
                {
                    if (n != 0)
                    {
                        arr++;
                    }
                }
        cipherArray[arr] = cipherArray[arr] + text.charAt(n).toUpperCase();
            }
        }
        for (o = 0; o < lines; o++)
        {
            cipher = cipher + cipherArray[o];
```

```
            railfencehtml = railfencehtml + cipherArray[o] + '<br>';
        }
        railfencehtml = railfencehtml;
        document.getElementById('railfence-view').innerHTML = railfencehtml;
        document.getElementById('rf-plainText').value = newtext;
        document.getElementById('rf-cipherText').value = cipher;
    }
}
function clearRailFenceCipher()
{
   document.getElementById('rf-plainText').value = '';
   document.getElementById('railfence-view').innerHTML = '';
   document.getElementById('rf-cipherText').value = '';
}
function minusOne()
{
    num_lines = document.getElementById('lines').value;
    if (num_lines < 3)
    {
        window.alert('The number of lines must be larger than 1');
        num_lines = 2;
    }
    else
    {
        num_lines--;
    }
    document.getElementById('lines').value = num_lines;
//    writeRailFenceCipher();
}
function plusOne()
{
    num_lines = document.getElementById('lines').value;
    num_lines++;
    document.getElementById('lines').value = num_lines;
//    writeRailFenceCipher();
}
function scytalePuzzle(q, a)
{
    if (q == 1)
    {
        if (a == 1) { writeAnswer(1, 'too-slim', 'too slim'); }
        if (a == 2) { writeAnswer(1, 'correct', 'CORRECT!'); }
        if (a == 3) { writeAnswer(1, 'too-large', 'too large'); }
    }
    if (q == 2)
    {
        if (a == 1) { writeAnswer(2, 'correct', 'CORRECT!'); }
        if (a == 2) { writeAnswer(2, 'too-large-1', 'too large'); }
        if (a == 3) { writeAnswer(2, 'too-large-2', 'too large'); }
    }
    if (q == 3)
    {
        if (a == 1) { writeAnswer(3, 'too-slim-1', 'too slim'); }
        if (a == 2) { writeAnswer(3, 'too-slim-2', 'too slim'); }
        if (a == 3) { writeAnswer(3, 'correct', 'CORRECT!'); }
    }
}
function writeAnswer(id, text, text2)
{
    var td_id = 'scytale-puzzle-' + id;
    var imagepath = 'images/scytale/scytale-puzzle/';
    var image1 = 'puz-' + id + '-' + text + '.gif';
    var image2 = 'puz-' + id + '-' + text + '-text.gif';
```

```
    document.getElementById(td_id).innerHTML = '<br><p><strong>The rod is '
+ text2 + '</strong></p><img src="' + imagepath + image1 + '"><br><br><img
src="' + imagepath + image2 + '"><br><br>';
}   </script>
</head>

       <body >

              <div id="pageFrame">
                <div id="masthead">

                <div id="masthead2">Pilih banyaknya baris yang akan dibentuk
untuk cipher transposisi ini. </div>
                </div>
                <div id="contentColumn">
                  <div id="innerContentColumn"> <br>

<table align="center">
<tr>
<td        class="rf-app-lines"><input         type="submit"         value="-"
onclick="minusOne();"></td>
<td    class="rf-app-lines"><input    type="text"    name="lines"    id="lines"
class="rf-app-lines-input" value="4" readonly></td>
<td        class="rf-app-lines"><input         type="submit"         value="+"
onclick="plusOne();"></td>
</tr>
<tr>
<td colspan="3" class="rf-app-lines">BANYAKNYA BARIS</td>
</tr>
</table>

<br>

<table width="410" align="center" cellspacing="4" id="rf-app">
<tr>
<td width="163" class="rf-app-heading">Plaintext:</td>
<td     width="196"     class="rf-app-element"><textarea     id="rf-plainText"
class="rf-textarea"></textarea></td>
</tr>
<tr>
  <td colspan="2"><center>
            <input      type="submit"
value="proses" onclick="writeRailFenceCipher();">
      
    <input                     type="submit"                     value="reset"
onclick="clearRailFenceCipher();"><br>
  </center>  </td></tr>
<tr>
  <td colspan="2">Teks asli akan disusun dalam dalam baris yang terbentuk
secara menurun kemudian akan di baca menjadi cipher secara mendatar.</td>
</tr>
<tr>
<td class="rf-app-heading">Susunan teks dalam baris.:</td>

<td class="rf-app-railfence" id="railfence-view"></td>
</tr>
<tr>
<td class="rf-app-heading">Ciphertext:</td>
<td     class="rf-app-element"><textarea     id="rf-cipherText"     class="rf-
textarea"></textarea></td>
</tr>
</table>
```

```
                </div>
              </div>
              <div id="footer">
                  </div>
            </div>
      <script               src="http://www.google-analytics.com/urchin.js"
type="text/javascript"></script>
<script type="text/javascript">
_uacct = "UA-2036050-1";
urchinTracker();
</script>
</body>
</html>
```

RIJNDAEL

Fungsi Ascii ke Hexadesimal

```
<?php
function ascii2hex($str) {
$result = '';
for($i=0; $i<strlen($str); $i++) {
$hex = strtoupper(dechex(ord($str[$i])));
$hex = str_pad($hex, 2, '0', STR_PAD_LEFT);
$result .= $hex;
}return $result;
}
?>
```

Fungsi Hexadesimal ke Ascii

```
<?php
function hex2ascii($str) {
$hex = str_split($str, 2);
$jml = ((strlen($str)/2)-1);
for($i=0; $i<=$jml; $i++){
$ubah = str_split($hex[$i]);
if ($ubah[0] == '0' or $ubah[0] == '1'){
$ubah[0] = 'A';
}
$hex[$i] = $ubah[0].$ubah[1];
$ascii[$i] = chr(hexdec($hex[$i]));
}
$result                                                                    =
$ascii[0]." ".$ascii[1]." ".$ascii[2]." ".$ascii[3]." ".
$ascii[4]." ".$ascii[5]." ".$ascii[6]." ".$ascii[7]." ".
$ascii[8]." ".$ascii[9]." ".$ascii[10]." ".$ascii[11]." 
".$ascii[12]." ".$ascii[13]." ".$ascii[14]." ".$ascii[15];
return $result;
}
?>
```

Proses Sebelum Putaran (Mengubah teks asli dan kunci menjadi hexadesimal dan melakukan proses XOR Teks asli dalam hexadesimal terhadap kunci dalam hexadesimal)

```
<?php
include 'binhex.php';
include'asc2hex.php';
include 'heksabin.php';
$in = $_REQUEST['in'];
$key = $_REQUEST['key'];
```

```
$in = ascii2hex($in); //in to bin
$inH = str_split($in,2);
$jml = (strlen($in)/2-1);
for ($i=0; $i<=$jml; $i++){
$inhex[$i] = hexbin($inH[$i]);
}
$in                                                                    =
$inhex[0].$inhex[1].$inhex[2].$inhex[3].$inhex[4].$inhex[5].$inhex[6].$inhex
[7].$inhex[8].$inhex[9].$inhex[10].$inhex[11].$inhex[12].$inhex[13].$inhex[1
4].$inhex[15]; //end in to bin
session_start();
$key = ascii2hex($key); //key to bin
$_SESSION['key'] = $key;
$keyH = str_split($key,2);
$jml = (strlen($key)/2-1);
for ($i=0; $i<=$jml; $i++){
$keyhex[$i] = hexbin($keyH[$i]);
}
$key                                                                   =
$keyhex[0].$keyhex[1].$keyhex[2].$keyhex[3].$keyhex[4].$keyhex[5].$keyhex[6]
.$keyhex[7].$keyhex[8].$keyhex[9].$keyhex[10].$keyhex[11].$keyhex[12].$keyhe
x[13].$keyhex[14].$keyhex[15]; //end key to bin
$a = str_split($key);
$b = str_split($in);
$jml = (strlen($key)-1);
for ($i=0; $i<=$jml; $i++){
if ($a[$i] == $b[$i]){
       $hasil[$i] = '0';
       }
       elseif ($a[$i] != $b[$i]){
       $hasil[$i] = '1';
       }
}
$hasilx                                                                =
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7].$hasil[8].$hasil[9].$hasil[10].$hasil[11].$hasil[12].$hasil[13].$hasil[1
4].$hasil[15].$hasil[16].$hasil[17].$hasil[18].$hasil[19].$hasil[20].$hasil[
21].$hasil[22].$hasil[23].$hasil[24].$hasil[25].$hasil[26].$hasil[27].$hasil
[28].$hasil[29].$hasil[30].$hasil[31].$hasil[32].$hasil[33].$hasil[34].$hasi
l[35].$hasil[36].$hasil[37].$hasil[38].$hasil[39].$hasil[40].$hasil[41].$has
il[42].$hasil[43].$hasil[44].$hasil[45].$hasil[46].$hasil[47].$hasil[48].$ha
sil[49].$hasil[50].$hasil[51].$hasil[52].$hasil[53].$hasil[54].$hasil[55].$h
asil[56].$hasil[57].$hasil[58].$hasil[59].$hasil[60].$hasil[61].$hasil[62].$
hasil[63].$hasil[64].$hasil[65].$hasil[66].$hasil[67].$hasil[68].$hasil[69].
$hasil[70].$hasil[71].$hasil[72].$hasil[73].$hasil[74].$hasil[75].$hasil[76]
.$hasil[77].$hasil[78].$hasil[79].$hasil[80].$hasil[81].$hasil[82].$hasil[83
].$hasil[84].$hasil[85].$hasil[86].$hasil[87].$hasil[88].$hasil[89].$hasil[9
0].$hasil[91].$hasil[92].$hasil[93].$hasil[94].$hasil[95].$hasil[96].$hasil[
97].$hasil[98].$hasil[99].$hasil[100].$hasil[101].$hasil[102].$hasil[103].$h
asil[104].$hasil[105].$hasil[106].$hasil[107].$hasil[108].$hasil[109].$hasil
[110].$hasil[111].$hasil[112].$hasil[113].$hasil[114].$hasil[115].$hasil[116
].$hasil[117].$hasil[118].$hasil[119].$hasil[120].$hasil[121].$hasil[122].$h
asil[123].$hasil[124].$hasil[125].$hasil[126].$hasil[127];

$a = str_split($hasilx,8);
$jml = (strlen($hasilx)/8-1);
for ($i=0; $i<=$jml; $i++){
$hasilakhir[$i] = binhex($a[$i]);
}
$hasilakhir                                                            =
$hasilakhir[0].$hasilakhir[1].$hasilakhir[2].$hasilakhir[3].$hasilakhir[4].$
hasilakhir[5].$hasilakhir[6].$hasilakhir[7].$hasilakhir[8].$hasilakhir[9].$h
```

```
asilakhir[10].$hasilakhir[11].$hasilakhir[12].$hasilakhir[13].$hasilakhir[14
].$hasilakhir[15];
$arr2 = str_split($hasilakhir,2);
```

Proses 1 (Substitusi Byte terhadap S-Box)

```
<?php
function pr1($angka){
$angka = str_split($angka,2);
$sbox = array
(
array("63","7c","77","7b","f2","6b","6f","c5","30","01","67","2b","fe","d7","ab","76"),
array("ca","82","c9","7d","fa","59","47","f0","ad","d4","a2","af","9c","a4","72","c0"),
array("b7","fd","93","26","36","3f","f7","cc","34","a5","e5","f1","71","d8","31","15"),
array("04","c7","23","c3","18","96","05","9a","07","12","80","e2","eb","27","b2","75"),
array("09","83","2c","1a","1b","6e","5a","a0","52","3b","d6","b3","29","e3","2f","84"),
array("53","d1","00","ed","20","fc","b1","5b","6a","cb","be","39","4a","4c","58","cf"),
array("d0","ef","aa","fb","43","4d","33","85","45","f9","02","7f","50","3c","9f","a8"),
array("51","a3","40","8f","92","9d","38","f5","bc","b6","da","21","10","ff","f3","d2"),
array("cd","0c","13","ec","5f","97","44","17","c4","a7","7e","3d","64","5d","19","73"),
array("60","81","4f","dc","22","2a","90","88","46","ee","b8","14","de","5e","0b","db"),
array("e0","32","3a","0a","49","06","24","5c","c2","d3","ac","62","91","95","e4","79"),
array("e7","c8","37","6d","8d","d5","4e","a9","6c","56","f4","ea","65","7a","ae","08"),
array("ba","78","25","2e","1c","a6","b4","c6","e8","dd","74","1f","4b","bd","8b","8a"),
array("70","3e","b5","66","48","03","f6","0e","61","35","57","b9","86","c1","1d","9e"),
array("e1","f8","98","11","69","d9","8e","94","9b","1e","87","e9","ce","55","28","df"),
array("8c","a1","89","0d","bf","e6","42","68","41","99","2d","0f","b0","54","bb","16")
);
for ($j=0; $j<=15; $j++){
$a = substr($angka[$j],0,1);
switch ($a){
case "A": $a = 10; break;
case "B": $a = 11; break;
case "C": $a = 12; break;
case "D": $a = 13; break;
case "E": $a = 14; break;
case "F": $a = 15; break;
default: $a = $a; break;
}
$b = substr($angka[$j],-1);
switch ($b){
case "A": $b = 10; break;
case "B": $b = 11; break;
case "C": $b = 12; break;
case "D": $b = 13; break;
case "E": $b = 14; break;
case "F": $b = 15; break;
default: $b = $b; break;
}
$hasil[$j] = $sbox[$a][$b];
}
?>
<table border="1">
<?php
echo "
Proses Substitusi Byte dilakukan dengan cara mensubtitusi hasil dari proses
sebelumnya terhadap s-box. Cara melakukan substitusi yaitu dengan
memperhatikan xy, misalnya A9, maka x =A dan y=9, maka cari di dalam s-box
baris A kolom 9.<br><tr><td><input name='a1' type='text' size='2'
maxlength='2' value=".$hasil[0]." readonly='readonly' /></td>
<td><input type='text' name='a2' size='2' maxlength='2' value=".$hasil[1]."
readonly='readonly' /></td>
```

```
<td><input type='text' name='a3' size='2' maxlength='2' value=".$hasil[2]."
readonly='readonly'/></td>
<td><input type='text' name='a4' size='2' maxlength='2' value=".$hasil[3]."
readonly='readonly'/></td></tr>
<tr><td><input     type='text'     name='b1'     size='2'     maxlength='2'
value=".$hasil[4]." readonly='readonly'/></td>
<td><input type='text' name='b2' size='2' maxlength='2' value=".$hasil[5]."
readonly='readonly'/></td>
<td><input type='text' name='b3' size='2' maxlength='2' value=".$hasil[6]."
readonly='readonly'/></td>
<td><input type='text' name='b4' size='2' maxlength='2' value=".$hasil[7]."
readonly='readonly'/></td></tr>
<tr><td><input     type='text'     name='c1'     size='2'     maxlength='2'
value=".$hasil[8]." readonly='readonly'/></td>
<td><input type='text' name='c2' size='2' maxlength='2' value=".$hasil[9]."
readonly='readonly'/></td>
<td><input type='text' name='c3' size='2' maxlength='2' value=".$hasil[10]."
readonly='readonly'/></td>
<td><input type='text' name='c4' size='2' maxlength='2' value=".$hasil[11]."
readonly='readonly'/></td></tr>
<tr><td><input     type='text'     name='d1'     size='2'     maxlength='2'
value=".$hasil[12]." readonly='readonly'/></td>
<td><input type='text' name='d2' size='2' maxlength='2' value=".$hasil[13]."
readonly='readonly'/></td>
<td><input type='text' name='d3' size='2' maxlength='2' value=".$hasil[14]."
readonly='readonly'/></td>
<td><input type='text' name='d4' size='2' maxlength='2' value=".$hasil[15]."
readonly='readonly'/></td></tr>
<tr><td colspan = '4' align = 'center'>Hasil Sub Bytes</td></tr>
";
?>
</table>
<?php
$return                                                                    =
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7].$hasil[8].$hasil[9].$hasil[10].$hasil[11].$hasil[12].$hasil[13].$hasil[1
4].$hasil[15];
return $return;
}
?>
```

Proses 2 (Shift Rows atau pergeseran kolom)

```
<?php
function pr2($angka){
$angka = str_split($angka,2);
echo " <br> Shift Rows atau pergeseran baris dilakukan dengan cara : baris
pertama tidak terjadi pergeseran, baris ke dua di geser 1 kolom ke kiri dan
posisi paling kiri berpindah ke sebelah kanan, baris ke tiga digeser
sebanyak 2 kolom, dan baris ke empat sebanyak 3 kolom.
<table   border   =   '1'><tr><td><input   name='a1'   type='text'   size='2'
maxlength='2' value=".$angka[0]." readonly='readonly' /></td>
<td><input type='text' name='a2'  size='2' maxlength='2' value=".$angka[1]."
readonly='readonly' /></td>
<td><input type='text' name='a3' size='2' maxlength='2' value=".$angka[2]."
readonly='readonly'/></td>
<td><input type='text' name='a4' size='2' maxlength='2' value=".$angka[3]."
readonly='readonly'/></td></tr>
<tr><td><input     type='text'     name='b1'     size='2'     maxlength='2'
value=".$angka[5]." readonly='readonly'/></td>
<td><input type='text' name='b2' size='2' maxlength='2' value=".$angka[6]."
readonly='readonly'/></td>
```

```
<td><input type='text' name='b3' size='2' maxlength='2' value=".$angka[7]."
readonly='readonly'/></td>
<td><input type='text' name='b4' size='2' maxlength='2' value=".$angka[4]."
readonly='readonly'/></td></tr>
<tr><td><input     type='text'     name='c1'     size='2'     maxlength='2'
value=".$angka[10]." readonly='readonly'/></td>
<td><input type='text' name='c2' size='2' maxlength='2' value=".$angka[11]."
readonly='readonly'/></td>
<td><input type='text' name='c3' size='2' maxlength='2' value=".$angka[8]."
readonly='readonly'/></td>
<td><input type='text' name='c4' size='2' maxlength='2' value=".$angka[9]."
readonly='readonly'/></td></tr>
<tr><td><input     type='text'     name='d1'     size='2'     maxlength='2'
value=".$angka[15]." readonly='readonly'/></td>
<td><input type='text' name='d2' size='2' maxlength='2' value=".$angka[12]."
readonly='readonly'/></td>
<td><input type='text' name='d3' size='2' maxlength='2' value=".$angka[13]."
readonly='readonly'/></td>
<td><input type='text' name='d4' size='2' maxlength='2' value=".$angka[14]."
readonly='readonly'/></td></tr>
<tr><td colspan = '4' align = 'center'>Hasil SiftRows</td></tr>
</table>
";
$hasil[0]=$angka[0];
$hasil[1]=$angka[5];
$hasil[2]=$angka[10];
$hasil[3]=$angka[15];
       $hasil[4]=$angka[1];
       $hasil[5]=$angka[6];
       $hasil[6]=$angka[11];
       $hasil[7]=$angka[12];
$hasil[8]=$angka[2];
$hasil[9]=$angka[7];
$hasil[10]=$angka[8];
$hasil[11]=$angka[13];
       $hasil[12]=$angka[3];
       $hasil[13]=$angka[4];
       $hasil[14]=$angka[9];
       $hasil[15]=$angka[14];
$return                                                                    =
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7].$hasil[8].$hasil[9].$hasil[10].$hasil[11].$hasil[12].$hasil[13].$hasil[1
4].$hasil[15];
return $return;
}
?>
```

Proses 3 (Mix Kolom atau Pencampuran Kolom)

```
<?php
function pr3($angka){
$angka = str_split($angka,2);
include "binhex.php";
$dua[0] = "0";  $dua[1] = "0";  $dua[2] = "0";  $dua[3] = "1";
$dua[4] = "1";  $dua[5] = "0";  $dua[6] = "1";  $dua[7] = "1";
$nol[0] = "0";  $nol[1] = "0";  $nol[2] = "0";  $nol[3] = "0";
$nol[4] = "0";  $nol[5] = "0";  $nol[6] = "1";  $nol[7] = "0";
$sbox = array
(
array("2","3","1","1"),
array("1","2","3","1"),
array("1","1","2","3"),
array("3","1","1","2")
```

```
);
//looping untuk kolom
for ($c=0; $c<=3; $c++){
//lopping untuk isi kolom
for ($b=0; $b<=3; $b++){
//potong bilangan
$str = strtoupper($angka[$b]);
$a = str_split($str);

for ($j=0; $j<=1; $j++){
switch ($a[$j]){ case "0": $a[$j] = '0000'; break;
case "1": $a[$j] = '0001'; break;
case "2": $a[$j] = '0010'; break;
case "3": $a[$j] = '0011'; break;
case "4": $a[$j] = '0100'; break;
case "5": $a[$j] = '0101'; break;
case "6": $a[$j] = '0110'; break;
case "7": $a[$j] = '0111'; break;
case "8": $a[$j] = '1000'; break;
case "9": $a[$j] = '1001'; break;
case "A": $a[$j] = '1010'; break;
case "B": $a[$j] = '1011'; break;
case "C": $a[$j] = '1100'; break;
case "D": $a[$j] = '1101'; break;
case "E": $a[$j] = '1110'; break;
case "F": $a[$j] = '1111'; break;
}
$hasil[$j] = $a[$j];
}
$hasilbiner = $hasil[0].$hasil[1];
$hasil = str_split($hasilbiner);
$jml = (strlen($hasilbiner))-1;

if (($sbox[$c][$b])==1){ //kalo yang di sbox 1
$hasilF = $hasilbiner;
}
elseif (($sbox[$c][$b])==2){ //kalo yang di sbox 2
       if ($hasil[0] == 1){  //(Geser.arr2)
       for ($i=0; $i <= $jml; $i++)
       {
       $hasil[8] = 0;
       $hasil[$i] = $hasil[$i+1];
       if ($hasil[$i] == $dua[$i]){
                     $hasil[$i] = '0';
                     }
                     elseif ($hasil[$i] != $dua[$i]){
                     $hasil[$i] = '1';
                     }
       }      }
       elseif ($hasil[0] == 0){ //kalo awal =0
              for ($l=0; $l <= $jml; $l++)
              {
                     $hasil[8] = 0;
                     $hasil[$l] = $hasil[$l+1];
              }
}      }
elseif (($sbox[$c][$b])==3){ //kalo yang di sbox 3
$hasil1 = str_split($hasilbiner);
if ($hasil[0] == 1){  //(Geser.arr3)
       for ($i=0; $i <= $jml; $i++)
       {
       $hasil[8] = 0;
       $hasil[$i] = $hasil[$i+1];
```

```
	if ($hasil[$i] == $dua[$i]){
			$hasil2[$i] = '0';
			}
			elseif ($hasil[$i] != $dua[$i]){
			$hasil2[$i] = '1';
			}
	if ($hasil1[$i] == $hasil2[$i]){
	$hasil[$i] = '0';
	}
	elseif ($hasil1[$i] != $hasil2[$i]){
	$hasil[$i] = '1';
	}
	}
}
	elseif ($hasil[0] == 0){ //kalo akhirnya =0
		for ($l=0; $l <= $jml; $l++)
		{
			$hasil[8] = 0;
			$hasil2[$l] = $hasil[$l+1];
	if ($hasil1[$l] == $hasil2[$l]){
	$hasil[$l] = '0';
	}
	elseif ($hasil1[$l] != $hasil2[$l]){
	$hasil[$l] = '1';
	}
		}
}
}
$hasilS[$b]=    $hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].
$hasil[6].$hasil[7];
}
$hasil1 = str_split($hasilS[0]);
$hasil2 = str_split($hasilS[1]);
$hasil3 = str_split($hasilS[2]);
$hasil4 = str_split($hasilS[3]);
		for ($l=0; $l <= $jml; $l++)
		{
	if ($hasil1[$l] == $hasil2[$l]){
	$hasil1[$l] = '0';
	}
	elseif ($hasil1[$l] != $hasil2[$l]){
	$hasil1[$l] = '1';
	}
		if ($hasil3[$l] == $hasil4[$l]){
		$hasil2[$l] = '0';
		}
		elseif ($hasil3[$l] != $hasil4[$l]){
		$hasil2[$l] = '1';
		}
	if ($hasil1[$l] == $hasil2[$l]){
	$hasil[$l] = '0';
	}
	elseif ($hasil1[$l] != $hasil2[$l]){
	$hasil[$l] = '1';
	}
			}
$hasilC[$c]=    $hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].
$hasil[6].$hasil[7];

$hexhex[$c] = binhex($hasilC[$c]);
			}
			$angka[0] = $hexhex[0];    $angka[1]             =
$hexhex[1];$angka[2] = $hexhex[2];$angka[3] = $hexhex[3];
```

```
//looping untuk kolom
for ($c=0; $c<=3; $c++){
//lopping untuk isi kolom
for ($b=0; $b<=3; $b++){
//potong bilangan
$str = strtoupper($angka[$b+4]);
$a = str_split($str);

for ($j=0; $j<=1; $j++){
switch ($a[$j]){
case "0": $a[$j] = '0000'; break;
case "1": $a[$j] = '0001'; break;
case "2": $a[$j] = '0010'; break;
case "3": $a[$j] = '0011'; break;
case "4": $a[$j] = '0100'; break;
case "5": $a[$j] = '0101'; break;
case "6": $a[$j] = '0110'; break;
case "7": $a[$j] = '0111'; break;
case "8": $a[$j] = '1000'; break;
case "9": $a[$j] = '1001'; break;
case "A": $a[$j] = '1010'; break;
case "B": $a[$j] = '1011'; break;
case "C": $a[$j] = '1100'; break;
case "D": $a[$j] = '1101'; break;
case "E": $a[$j] = '1110'; break;
case "F": $a[$j] = '1111'; break;
}
$hasil[$j] = $a[$j];
}
$hasilbiner = $hasil[0].$hasil[1];
$hasil = str_split($hasilbiner);
$jml = (strlen($hasilbiner))-1;
if (($sbox[$c][$b])==1){ //kalo yang di sbox 1
$hasilF = $hasilbiner;
}
elseif (($sbox[$c][$b])==2){ //kalo yang di sbox 2
       if ($hasil[0] == 1){  //(Geser.arr2)
       for ($i=0; $i <= $jml; $i++)
       {
       $hasil[8] = 0;
       $hasil[$i] = $hasil[$i+1];
       if ($hasil[$i] == $dua[$i]){
                     $hasil[$i] = '0';
                     }
                     elseif ($hasil[$i] != $dua[$i]){
                     $hasil[$i] = '1';
                     }
       }      }
       elseif ($hasil[0] == 0){ //kalo awal =0
              for ($l=0; $l <= $jml; $l++)
              {
                     $hasil[8] = 0;
                     $hasil[$l] = $hasil[$l+1];
              }
}      }
elseif (($sbox[$c][$b])==3){ //kalo yang di sbox 3
$hasil1 = str_split($hasilbiner);
if ($hasil[0] == 1){  //(Geser.arr3)
       for ($i=0; $i <= $jml; $i++)
       {
       $hasil[8] = 0;
       $hasil[$i] = $hasil[$i+1];
       if ($hasil[$i] == $dua[$i]){
```

```
                    $hasil2[$i] = '0';
                    }
                    elseif ($hasil[$i] != $dua[$i]){
                    $hasil2[$i] = '1';
                    }
       if ($hasil1[$i] == $hasil2[$i]){
       $hasil[$i] = '0';
       }
       elseif ($hasil1[$i] != $hasil2[$i]){
       $hasil[$i] = '1';
       }
       }
}
       elseif ($hasil[0] == 0){ //kalo akhirnya =0
              for ($l=0; $l <= $jml; $l++)
              {
                    $hasil[8] = 0;
                    $hasil2[$l] = $hasil[$l+1];
       if ($hasil1[$l] == $hasil2[$l]){
       $hasil[$l] = '0';
       }
       elseif ($hasil1[$l] != $hasil2[$l]){
       $hasil[$l] = '1';
       }
              }
}
}
$hasilS[$b]                                                                    =
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7];
}
$hasil1 = str_split($hasilS[0]);
$hasil2 = str_split($hasilS[1]);
$hasil3 = str_split($hasilS[2]);
$hasil4 = str_split($hasilS[3]);
              for ($l=0; $l <= $jml; $l++)
              {
       if ($hasil1[$l] == $hasil2[$l]){
       $hasil1[$l] = '0';
       }
       elseif ($hasil1[$l] != $hasil2[$l]){
       $hasil1[$l] = '1';
       }
              if ($hasil3[$l] == $hasil4[$l]){
              $hasil2[$l] = '0';
              }
              elseif ($hasil3[$l] != $hasil4[$l]){
              $hasil2[$l] = '1';
              }
       if ($hasil1[$l] == $hasil2[$l]){

       $hasil[$l] = '0';
       }
       elseif ($hasil1[$l] != $hasil2[$l]){
       $hasil[$l] = '1';
       }
                           }
                    $hasilC[$c]=
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7];

$hexhex[$c] = binhex($hasilC[$c]);
                           }
```

```
                              $angka[4] = $hexhex[0];    $angka[5]              =
$hexhex[1];$angka[6] = $hexhex[2];$angka[7] = $hexhex[3];
//looping untuk kolom
for ($c=0; $c<=3; $c++){
//lopping untuk isi kolom
for ($b=0; $b<=3; $b++){
//potong bilangan
$str = strtoupper($angka[$b+8]);
$a = str_split($str);

for ($j=0; $j<=1; $j++){
switch ($a[$j]){
case "0": $a[$j] = '0000'; break;
case "1": $a[$j] = '0001'; break;
case "2": $a[$j] = '0010'; break;
case "3": $a[$j] = '0011'; break;
case "4": $a[$j] = '0100'; break;
case "5": $a[$j] = '0101'; break;
case "6": $a[$j] = '0110'; break;
case "7": $a[$j] = '0111'; break;
case "8": $a[$j] = '1000'; break;
case "9": $a[$j] = '1001'; break;
case "A": $a[$j] = '1010'; break;
case "B": $a[$j] = '1011'; break;
case "C": $a[$j] = '1100'; break;
case "D": $a[$j] = '1101'; break;
case "E": $a[$j] = '1110'; break;
case "F": $a[$j] = '1111'; break;
}
$hasil[$j] = $a[$j];
}
$hasilbiner = $hasil[0].$hasil[1];
$hasil = str_split($hasilbiner);
$jml = (strlen($hasilbiner))-1;

if (($sbox[$c][$b])==1){ //kalo yang di sbox 1
$hasilF = $hasilbiner;
}
elseif (($sbox[$c][$b])==2){ //kalo yang di sbox 2
       if ($hasil[0] == 1){  //(Geser.arr2)
       for ($i=0; $i <= $jml; $i++)
       {
       $hasil[8] = 0;
       $hasil[$i] = $hasil[$i+1];
       if ($hasil[$i] == $dua[$i]){
                     $hasil[$i] = '0';
                     }
                     elseif ($hasil[$i] != $dua[$i]){
                     $hasil[$i] = '1';
                     }
       }      }
       elseif ($hasil[0] == 0){ //kalo awal =0
              for ($l=0; $l <= $jml; $l++)
              {
                     $hasil[8] = 0;
                     $hasil[$l] = $hasil[$l+1];
              }
}      }
elseif (($sbox[$c][$b])==3){ //kalo yang di sbox 3
$hasil1 = str_split($hasilbiner);
if ($hasil[0] == 1){  //(Geser.arr3)
       for ($i=0; $i <= $jml; $i++)
       {
```

```
	$hasil[8] = 0;
	$hasil[$i] = $hasil[$i+1];
	if ($hasil[$i] == $dua[$i]){
			$hasil2[$i] = '0';
			}
			elseif ($hasil[$i] != $dua[$i]){
			$hasil2[$i] = '1';
			}
	if ($hasil1[$i] == $hasil2[$i]){
	$hasil[$i] = '0';
	}
	elseif ($hasil1[$i] != $hasil2[$i]){
	$hasil[$i] = '1';
	}
	}
}
	elseif ($hasil[0] == 0){ //kalo akhirnya =0
		for ($l=0; $l <= $jml; $l++)
		{
			$hasil[8] = 0;
			$hasil2[$l] = $hasil[$l+1];
	if ($hasil1[$l] == $hasil2[$l]){
	$hasil[$l] = '0';
	}
	elseif ($hasil1[$l] != $hasil2[$l]){
	$hasil[$l] = '1';
	}
		}
}
}
$hasilS[$b]                                                                    =
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7];

}
$hasil1 = str_split($hasilS[0]);
$hasil2 = str_split($hasilS[1]);
$hasil3 = str_split($hasilS[2]);
$hasil4 = str_split($hasilS[3]);
		for ($l=0; $l <= $jml; $l++)
		{
	if ($hasil1[$l] == $hasil2[$l]){
	$hasil1[$l] = '0';
	}
	elseif ($hasil1[$l] != $hasil2[$l]){
	$hasil1[$l] = '1';
	}
		if ($hasil3[$l] == $hasil4[$l]){
		$hasil2[$l] = '0';
		}
		elseif ($hasil3[$l] != $hasil4[$l]){
		$hasil2[$l] = '1';
		}
	if ($hasil1[$l] == $hasil2[$l]){
	$hasil[$l] = '0';
	}
	elseif ($hasil1[$l] != $hasil2[$l]){
	$hasil[$l] = '1';
	}
			}
			$hasilC[$c]=
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7];
```

```
$hexhex[$c] = binhex($hasilC[$c]);
                            }
                            $angka[8] = $hexhex[0];    $angka[9]              =
$hexhex[1];$angka[10] = $hexhex[2];$angka[11] = $hexhex[3];
//looping untuk kolom
for ($c=0; $c<=3; $c++){
//lopping untuk isi kolom
for ($b=0; $b<=3; $b++){
//potong bilangan
$str = strtoupper($angka[$b+12]);
$a = str_split($str);

for ($j=0; $j<=1; $j++){
switch ($a[$j]){
case "0": $a[$j] = '0000'; break;
case "1": $a[$j] = '0001'; break;
case "2": $a[$j] = '0010'; break;
case "3": $a[$j] = '0011'; break;
case "4": $a[$j] = '0100'; break;
case "5": $a[$j] = '0101'; break;
case "6": $a[$j] = '0110'; break;
case "7": $a[$j] = '0111'; break;
case "8": $a[$j] = '1000'; break;
case "9": $a[$j] = '1001'; break;
case "A": $a[$j] = '1010'; break;
case "B": $a[$j] = '1011'; break;
case "C": $a[$j] = '1100'; break;
case "D": $a[$j] = '1101'; break;
case "E": $a[$j] = '1110'; break;
case "F": $a[$j] = '1111'; break;
}
$hasil[$j] = $a[$j];
}
$hasilbiner = $hasil[0].$hasil[1];
$hasil = str_split($hasilbiner);
$jml = (strlen($hasilbiner))-1;

if (($sbox[$c][$b])==1){ //kalo yang di sbox 1
$hasilF = $hasilbiner;
}
elseif (($sbox[$c][$b])==2){ //kalo yang di sbox 2
       if ($hasil[0] == 1){  //(Geser.arr2)
       for ($i=0; $i <= $jml; $i++)
       {
       $hasil[8] = 0;
       $hasil[$i] = $hasil[$i+1];
       if ($hasil[$i] == $dua[$i]){
                     $hasil[$i] = '0';
                     }
                     elseif ($hasil[$i] != $dua[$i]){
                     $hasil[$i] = '1';
                     }
       }      }
       elseif ($hasil[0] == 0){ //kalo awal =0
              for ($l=0; $l <= $jml; $l++)
              {
                     $hasil[8] = 0;
                     $hasil[$l] = $hasil[$l+1];
              }
}      }
elseif (($sbox[$c][$b])==3){ //kalo yang di sbox 3
$hasil1 = str_split($hasilbiner);
```

```
if ($hasil[0] == 1){  //(Geser.arr3)
       for ($i=0; $i <= $jml; $i++)
       {
       $hasil[8] = 0;
       $hasil[$i] = $hasil[$i+1];
       if ($hasil[$i] == $dua[$i]){
                     $hasil2[$i] = '0';
                     }
                     elseif ($hasil[$i] != $dua[$i]){
                     $hasil2[$i] = '1';
                     }

       if ($hasil1[$i] == $hasil2[$i]){
       $hasil[$i] = '0';
       }
       elseif ($hasil1[$i] != $hasil2[$i]){
       $hasil[$i] = '1';
       }
       }
}
       elseif ($hasil[0] == 0){ //kalo akhirnya =0
              for ($l=0; $l <= $jml; $l++)
              {
                     $hasil[8] = 0;
                     $hasil2[$l] = $hasil[$l+1];
       if ($hasil1[$l] == $hasil2[$l]){
       $hasil[$l] = '0';
       }
       elseif ($hasil1[$l] != $hasil2[$l]){
       $hasil[$l] = '1';
       }
              }
}
}
$hasilS[$b]                                                                    =
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7];

}
$hasil1 = str_split($hasilS[0]);
$hasil2 = str_split($hasilS[1]);
$hasil3 = str_split($hasilS[2]);
$hasil4 = str_split($hasilS[3]);
              for ($l=0; $l <= $jml; $l++)
              {
       if ($hasil1[$l] == $hasil2[$l]){
       $hasil1[$l] = '0';
       }
       elseif ($hasil1[$l] != $hasil2[$l]){
       $hasil1[$l] = '1';
       }
              if ($hasil3[$l] == $hasil4[$l]){
              $hasil2[$l] = '0';
              }
              elseif ($hasil3[$l] != $hasil4[$l]){
              $hasil2[$l] = '1';
              }
       if ($hasil1[$l] == $hasil2[$l]){

       $hasil[$l] = '0';
       }
       elseif ($hasil1[$l] != $hasil2[$l]){
       $hasil[$l] = '1';
```

```
	}
                        }
                    $hasilC[$c]=
$hasil[0].$hasil[1].$hasil[2].$hasil[3].$hasil[4].$hasil[5].$hasil[6].$hasil
[7];

$hexhex[$c] = binhex($hasilC[$c]);
                        }
                        $angka[12] = $hexhex[0];   $angka[13]            =
$hexhex[1];$angka[14] = $hexhex[2];$angka[15] = $hexhex[3];
	echo "Dalam proses mix colums atau pencampuran kolom ada beberapa
aturan khusus. Transformasi yang dilakukan yaitu dengan proses seperti
perkalian matriks namun dengan menggunakan XOR. Aturan selengkapnya dalam
proses perhitungan mix kolom dapat dilihat pada bagian teori rijndael.
	<table border = '1'><tr><td><input name='a1' type='text' size='2'
maxlength='2' value=".$angka[0]." readonly='readonly' /></td>
<td><input type='text' name='a2'  size='2' maxlength='2' value=".$angka[1]."
readonly='readonly' /></td>
<td><input type='text' name='a3' size='2' maxlength='2' value=".$angka[2]."
readonly='readonly'/></td>
<td><input type='text' name='a4' size='2' maxlength='2' value=".$angka[3]."
readonly='readonly'/></td></tr>
<tr><td><input	type='text'	name='b1'	size='2'	maxlength='2'
value=".$angka[5]." readonly='readonly'/></td>
<td><input type='text' name='b2' size='2' maxlength='2' value=".$angka[6]."
readonly='readonly'/></td>
<td><input type='text' name='b3' size='2' maxlength='2' value=".$angka[7]."
readonly='readonly'/></td>
<td><input type='text' name='b4' size='2' maxlength='2' value=".$angka[4]."
readonly='readonly'/></td></tr>
<tr><td><input	type='text'	name='c1'	size='2'	maxlength='2'
value=".$angka[10]." readonly='readonly'/></td>
<td><input type='text' name='c2' size='2' maxlength='2' value=".$angka[11]."
readonly='readonly'/></td>
<td><input type='text' name='c3' size='2' maxlength='2' value=".$angka[8]."
readonly='readonly'/></td>
<td><input type='text' name='c4' size='2' maxlength='2' value=".$angka[9]."
readonly='readonly'/></td></tr>
<tr><td><input	type='text'	name='d1'	size='2'	maxlength='2'
value=".$angka[15]." readonly='readonly'/></td>
<td><input type='text' name='d2' size='2' maxlength='2' value=".$angka[12]."
readonly='readonly'/></td>
<td><input type='text' name='d3' size='2' maxlength='2' value=".$angka[13]."
readonly='readonly'/></td>
<td><input type='text' name='d4' size='2' maxlength='2' value=".$angka[14]."
readonly='readonly'/></td></tr>
<tr><td colspan = '4' align = 'center'>Hasil Mix Coloumns</td></tr>
</table>";
$return                                                                 =
$angka[0].$angka[1].$angka[2].$angka[3].$angka[4].$angka[5].$angka[6].$angka
[7].$angka[8].$angka[9].$angka[10].$angka[11].$angka[12].$angka[13].$angka[1
4].$angka[15];

return $return;
}
?>
```