SISTEM PEMBELAJARAN ELEKTRONIK UNTUK KRIPTOGRAFI RIJNDAEL 128 BIT MENGGUNAKAN METODE WEB-BASED LEARNING

Mursid
mursidjpr73@gmail.com

Staf Pengajar pada Program Studi Teknik Informatika
Fakultas Ilmu Komputer dan Manajemen
Universitas Sains dan Teknologi Jayapura

Abstraksi *- Mempelajari algoritma kriptografi Rijndael di kelas membutuhkan waktu karena tingkat kesulitan dan penjabarannya yang cukup panjang, membuat mahasiswa tidak dapat menyelesaikannya dengan maksimal. Tujuan penelitian ini menghasilkan aplikasi pembelajaran kriptografi rijndael yang dapat menampilkan teori dasar dan proses enkripsi dan dekripsi secara tahap demi tahap, sehingga dapat membantu mahasiswa dalam mempelajari atau memahami kriptografi rijndael dengan lebih mudah. Metode pembelajaran dengan Web Base Learning (WBL) dapat menyajikan materi dan tahapan konsep algoritma rijndael berbasis web, sehingga dapat diakses secara luas.*
Aplikasi yang dihasilkan dapat melakukan uji coba algoritma secara dinamis dan interaktif serta ditampilkan tahapan proses secara detail. Hasil pengujian untuk kualitas sistem aplikasi pembelajaran kriptografi terhadap responden berdasarkan hasil kuisioner yang menyatakan baik mencapai 89%.

Kata kunci: Pembelajaran Elektronik, WBL, Kriptografi, Rijndael 128 Bit, Dekripsi.

1. PENDAHULUAN

Penggunaan Teknologi Informasi dan Komunikasi (TIK) pada proses pembelajaran bukan merupakan hal yang baru dalam era globalisasi sekarang ini. Seiring dengan kemajuan teknologi paradigma sistem pendidikan yang semula berbasis konvensional mengalami perubahan ke dalam bentuk digital (Riyana, 2007).

Keterbatasan waktu belajar di kelas dan banyaknya sub pokok bahasan tentang kriptografi, serta kurangnya kemampuan matematis membuat mahasiswa tidak dapat menyelesaikan algoritma kriptografi rijndael secara maksimal. Hal ini yang menjadi penyebab atau permasalahan dalam mempelajari algoritma kriptografi.

E-learning merupakan proses dan kegiatan penerapan pembelajaran berbasis web (*web-based learning*), pembelajaran berbasis komputer (*computer based learning*), pendidikan virtual (*virtual education*) dan/atau kolaborasi digital (*digital collaboration*). Materi-materi dalam kegiatan pembelajaran elektronik tersebut kebanyakan dihantarkan melalui media internet, intranet, *tape* video atau audio, penyiaran melalui satelit, televisi (ASTD, 2009; Riyana, 2007).

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara mengubahnya menjadi suatu bentuk yang tidak dapat dikenal lagi (Ariyus, 2008). Masalah keamanan dan kerahasiaan data dan informasi merupakan salah satu aspek yang penting. Salah satu cara menjaga keamanan dan kerahasiaan data dan informasi adalah dengan teknik enkripsi dan dekripsi atau yang dikenal juga dengan kriptografi (Munir, 2006).

Web Base Learning (WBL) merupakan suatu sistem yang dapat berkomunikasi secara mudah dengan memanfaatkan fasilitas internet sehingga kegiatan berkomunikasi dapat dilakukan tanpa dibatasi oleh jarak, tempat dan waktu (Wahono, 2013).

AES (*Advanced Encryption Standard*) Rijndael adalah algoritma kriptografi yang menggantikan DES (*Data Encryption Standard*) ditetapkan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001. AES Rijndael sebagai pengganti diharapkan dapat bertahan hingga abad 21 (Kromodimoeljo, 2009). Rijndael mendukung panjang kunci 128 bit, 192 bit, 256 bit. Algoritma Rijndael

merupakan salah satu algoritma yang menggunakan teknik substitusi dan permutasi pada tiap blok yang akan di enkripsi atau dekripsi. Untuk setiap putaran algoritma rijndael menggunakan kunci yang berbeda yang merupakan hasil dari proses ekspansi kunci. Ada 4 (empat) konsep dasar untuk melakukan proses dekripsi algorintma rijndael yaitu *Invshiftrows, Invsubbytes, Addroundkeys dan Invmixcolumns* (Xintong, 2009; FIPSP, 2001).

Penelitian ini bertujuan untuk menghasilkan aplikasi pembelajaran kriptografi yang dapat melakukan proses enkripsi dan dekripsi disertai tahapan algoritma, sehingga dapat membantu mahasiswa dalam memahami algoritma kriptografi rijndael.

2. METODOLOGI PENELITIAN

2.1 Lokasi dan Rancangan Penelitian

Penelitian ini dilakukan di Universitas Hasanuddin pada laboratorium Multimedia Jurusan Teknik Elektro. Metode penelitian yang digunakan yaitu deskriptif, yang melakukan kajian studi pustaka, menganalisa dan merancang sistem pembelajaran kriptografi. Data-data yang dikumpulkan berupa teori-teori dasar kriptografi, yang dirumuskan dalam bentuk perhitungan matematis secara manual untuk proses enkripsi dan dekripsi serta di implementasikan ke dalam bahasa program.

2.2 Tahapan Pemodelan

Tahapan ini merupakan tahapan memodelkan rumus dari algoritma dan langkah-langkah proses enkripsi dan dekripsi dengan melakukan perhitungan rumus dan cara kerja algoritma kriptografi secara manual. Tahapan ini akan di implementasikan dengan program sehingga menghasilkan sebuah aplikasi yang dapat digunakan mahasiswa atau pengguna dalam memahami konsep dasar algoritma kriptografi Rijndael.

2.3 Tahapan Pengembangan Aplikasi

Tahapan pengembangan Aplikasi terdiri dari lima tahap yaitu (1) Kebutuhan sistem meliputi analisis studi pustaka tentang algoritma kriptografi (2) Analisis algoritma secara manual untuk proses enkripsi dan dekripsi (3) Perancangan sistem meliputi perancangan proses input, output dan antar muka sistem (4) Implementasi merupakan tahapan pemodelan yang dirumuskan secara matematis ke bahasa pemograman (5) Pengujian sistem meliputi uji coba dan perbaikan terhadap aplikasi yang telah dibuat.

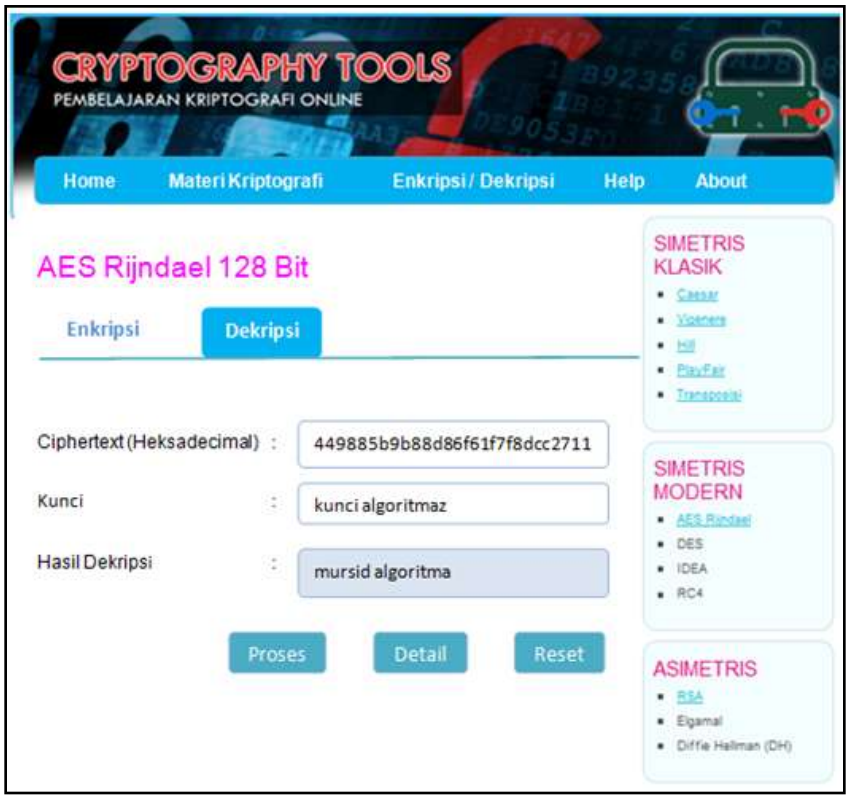
3. HASIL DAN PEMBAHASAN

Gambar 1 merupakan tampilan aplikasi kriptografi yang memuat materi dasar tentang kriptografi. Gambar 2 menunjukkan proses dekripsi algoritma kriptografi rijndael, yang menjadi inputan adalah hasil dari proses enkripsi berupa *ciphertext* dan *key*, kemudian pilih tombol *button* "Proses" untuk mendapatkan langsung hasil dekripsi berupa teks asli (*plaintext*), pilih tombol *butto*n "Detail" untuk melihat proses algoritma kriptografi rijndael secara bertahap.

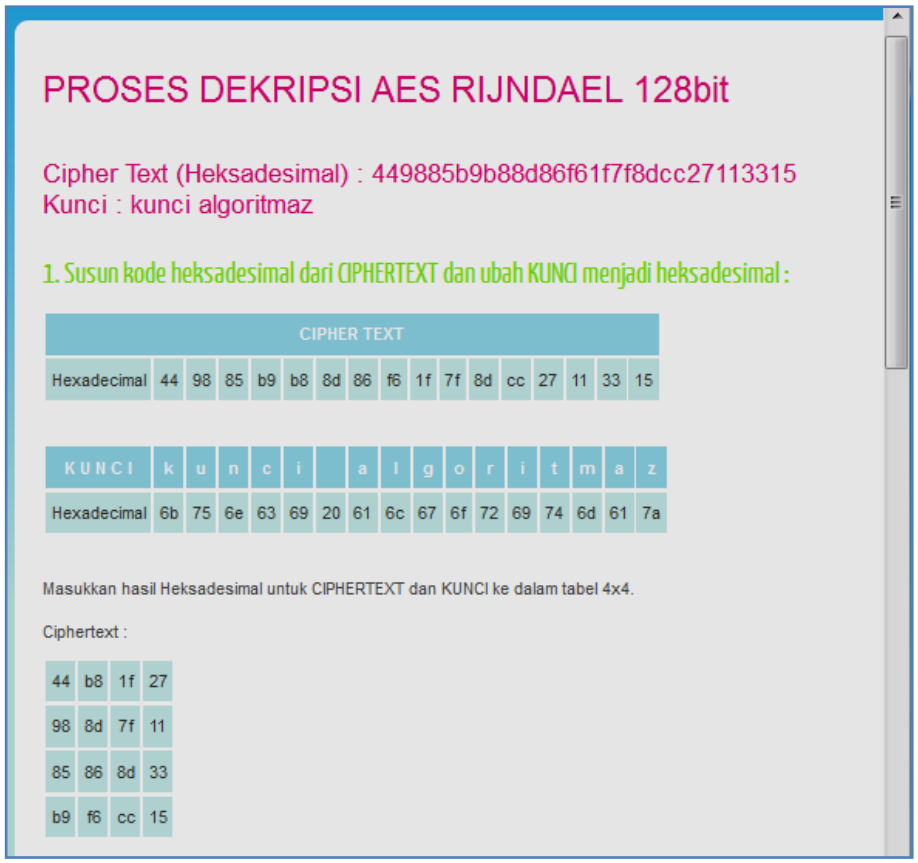
Gambar 3 menunjukkan proses XOR antara *ciphertext* dengan *addroundkey (n=10)*, sesuai dengan ketentuan jumlah putaran untuk algoritma rijndael 128 bit. Gambar 4 menunjukkan proses putaran pertama algoritma rijndael, yang setiap putarannya terdapat empat proses yang harus dilakukan yaitu *Invshiftrows, Invsubbytes, Addroundkeys dan InvMixcolumns*.

Gambar 5 menunjukkan hasil akhir proses dekripsi algoritma rijndael yang menghasilkan tekx asli (*plaintext*) semula.

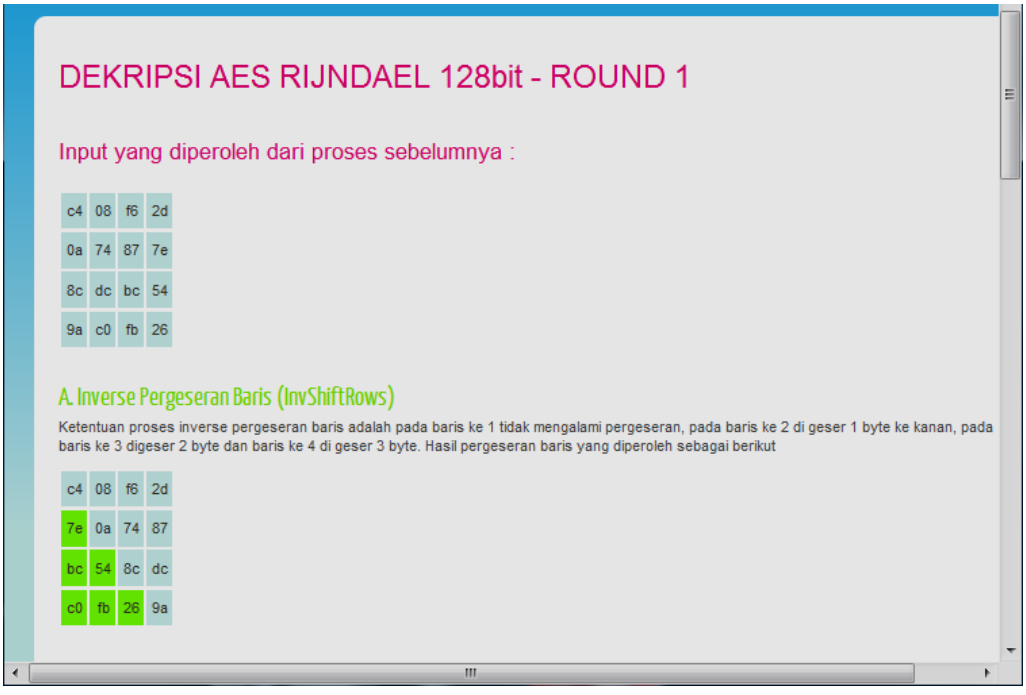
Gambar 1. Tampilan Aplikasi Kriptografi



Gambar 2. Proses awal Dekripsi AES Rijndael 128



Gambar 3. Proses awal proses XOR *Ciphertext* dengan *Addroundkey 10*



Gambar 4. Putaran Pertama Proses Dekripsi Rijndael

Gambar 5. Hasil Akhir putaran 10 Dekripsi AES Rijndael

Penelitian ini menunjukkan proses dekripsi algoritma rinjdael dapat di tampilkan secara detail sesuai algoritma. Pembahasan ini khusus untuk proses dekripsi algoritma rijndael 128 bit. Proses algoritma kriptografi rijndael terdiri dari 4 (empat) konsep dasar dalam setiap putaran yaitu *InvShiftRows, InvSubBytes, AddRoundkey* dan *InvMixColumns*. Banyaknya putaran untuk rijndael 128 bit adalah 10 kali, sebagai contoh proses hasil enkripsi dari teks asli : **mursid algoritma**, kunci : **kunci algoritmaz,** dengan *ciphertext* hasil enkripsi (dalam *hexadecimal*) : "**449885b9b88d86f61f7f8dcc27113315**".

Langkah pertama untuk proses dekripsi, ***Ciphertext*** dalam Hexadecimal di XOR dengan **Hasil penambahan kunci ke n** dari proses *expasion key*. Pada proses enkripsi yang di XOR pertama adalah kuncinya, berbeda untuk proses dekripsi yaitu dari hasil proses penambahan kunci ke n (n=10). Langkah berikutnya adalah melakukan tahapan proses *InvShiftRows, InvSubBytes, AddRoundKey* dan *InvMixColumns*.

InvShiftRows atau inverse pergeseran baris adalah pada baris pertama tidak mengalami pergeseran, baris kedua di geser 1 byte ke kanan, baris ketiga digeser 2 byte dan baris keempat di geser 3 byte.

InvSubBytes adalah proses substitusi yang menggunakan tabel inverse s-box, dimana tiap elemen pada state hasil transformasi *invshiftrows* dipetakan dengan inverse s-box.

AddRoundKey, Proses dekripsi dilakukan dari hasil putaran kunci terakhir (putaran ke n=10). Operasi ini merupakan suatu operasi penambahan kunci dengan operasi XOR dan setiap kunci putaran terdiri dari w[i], dimana w[i] merupakan kunci yang diturunkan dari putaran ke n.

Proses ekspansi kunci merupakan proses yang terpisah dimulai dari *cipherkey* dan dilakukan ekspansi kunci untuk membentuk *key schedule*. Ekspansi kunci menghasilkan total Nb (Nr+1) word, sehingga untuk AES 128 bit adalah 4 (10+1) = 40 word = 44 x 32 bit = 1408 bit sub key. Dalam proses penjadwalan kunci (*key schedule*), hanya kolom pertama saja yang perhitungannya berbeda yaitu menggunakan *s-box* dan *Rcon*, sedangkan untuk kolom 2, 3 dan 4 langsung di XOR terhadap kunci sebelumnya

InvMixColumns adalah proses perkalian XOR yang dilakukan antara inverse polinomial pada GF (2^8) dengan *InvSubBytes*. Perkalian matriks baris dan kolom pertama dapat dilihat sebagai berikut:

A' = {0E.A} XOR {0B.B} XOR {0D.C} XOR {09.D}

Proses *Inverse Mixcolumn* dilakukan dengan empat langkah yaitu pertama mengkonversi bilangan hexadecimal kedalam biner, kedua membagi bilangan dari *inverse polinomial* menjadi bit yang lebih kecil, ketiga menentukan hasil perkalian dengan bilangan hexadesimal (01,02, 04 08), dan keempat mencari hasil perkalian. Pada proses langkah ketiga, mencari hasil perkalian perlu diperhatikan beberapa ketentuan yaitu apabila di multiplikasi dengan 2 dan angka biner paling kiri dari bilangan tersebut adalah "1" digeser 1 digit kekiri dan di tambahkan "0" diakhir kemudian dimultiplikasi dengan nilai dari angka 2 (0001 1011) menggunakan fungsi XOR. Apabila angka binernya adalah "0" maka langsung dikalikan dengan bilangan tersebut. Untuk proses perkalian selanjutkan yang menjadi masukan diambil dari hasil proses sebelumnya dengan ketentuan yang sama (Xintong, 2009).

A' = {0E**.**b6} XOR {0B**.**a9} XOR {0D**.**83} XOR {09**.**2d}

- **0E.b6**

Langkah pertama, konversikan bilangan hexadecimal ke dalam biner:

0E = 0000 1110
b6 = 1011 0110

Langkah kedua, membagi bilangan dari *inverse polinomial* menjadi bit yang lebih kecil.

0E = 0000 1110 = 14 (08 xor 04 xor 02)
= (0000 1000 XOR 0000 0100 XOR 0000 0010)

Langkah ketiga, menentukan hasil perkalian dengan bilangan *hexadecimal* (01, 02, 04 dan 08).

1011 0110 x 0000 0001 = 1011 0110 (jika dikalikan 1, nilainya tetap)
1011 0110 x 0000 0010 = 0110 1100 XOR 0001 1011 = 0111 0111
(jika dikalikan 2, angka bit paling kiri adalah "1", maka dapat digeser langsung 1 digit kekiri dan ditambahkan angka "0" diakhir dan di XOR dengan nilai 2 (0001 1011)).

1011 0110 x 0000 0100 = 1110 1110
(jika dikalikan 4, hasil perkalian sebelumnya dengan 2 yang digunakan sebagai masukan dengan ketentuan yang sama dimana bit paling kiri "0" maka langsung digeser 1 digit kekiri dan ditambahkan "0" diakhir).

1011 0110 x 0000 1000 = 1101 1100 XOR 0001 1011 = 1100 0111
(jika dikalikan 8, hasil perkalian dengan 4 yang digunakan sebagai masukan dengan ketentuan yang sama dimana bit paling kiri "1" maka dapat langsung digeser 1 digit kekiri dan ditambahkan angka "0" diakhir kemudain di XOR dengan nilai 2 (0001 1011)).

Langkah keempat, menentukan hasil akhir.

0E•b6 = **{08 x b6} XOR {04 x b6} XOR {02 x b6}**
= {0000 1000 x 1011 0110} XOR {0000 0100 x 1011 0110} XOR {0000 0010 x 1011 0110}
= 1100 0111 XOR 1110 1110 XOR 0111 0111
= **0101 1110 (5e),** lakukan langkah yang sama untuk proses berikutnya.

Sehingga nilai "A" yang dihasilkan adalah:

A' = {0E.b6} XOR {0B.a9} XOR {0D.83} XOR {09.2d}
= 0101 1110 XOR 1101 1111 XOR 1100 1101 XOR 0101 1110
= **0001 0010** dalam hexadecimal **= 12**

Untuk mendapat nilai pada setiap kolom yang lain, lakukan proses yang sama. Hasil akhir yang diperoleh dari proses *Invmixcolumns* akan menjadi masukkan pada putaran berikutnya (Xintong, 2009; Satria, 2009).

4. PENUTUP

Aplikasi pembelajaran kriptografi dengan metode *web base learning* dapat mejadi alternatif model pembelajaran algoritma kriptografi. Aplikasi yang dihasilkan dapat melakukan uji coba algoritma untuk proses enkripsi dan dekripsi secara dinamis dan interaktif serta menampilkan tahapan proses algoritma secara tahap demi tahap, sehingga sangat membantu mahasiswa atau pengguna dalam memahami algoritma kriptografi Rijndael. Saran untuk pengembangan aplikasi perlu dikaji lebih mendalam dengan bahasa pemograman.

5. DAFTAR PUSTAKA

American Society for Training and Development (ASTD). (2009). Definition of e-learning. [online]. http://www.about-elearning.com/definition-of-e-learning.html. [03 Agustus 2014].

Ariyus Dony. (2008). *Pengantar Ilmu Kriptografi* (Teori Analisis dan Implementasi). Andi. Yogyakarta.

Federal Information Processing Standards Publication-197 (FIPSP). (2001). Announcing the Advanced Encryption Standard (AES).

Kromodimoeljo Sentot. (2009). Teori *dan Aplikasi Kriptogra*fi. Penerbit SPK IT Consulting.

Manullang E.V. (2013). Sistem Pembelajaran Elektronik untuk Kriptologi Simetris dan Asimetris (Studi Kasus Enkripsi). Tesis Teknik Elektro. Pascasarjana UNHAS. Makassar.

Munir R. (2006). *Kriptografi.* Penerbit Informatika. Bandung.

Riyana C. (2007). Konsep Dasar e-Learning. Dokumen presentasi pada perkuliahan e-learning di Jurusan Kurikulum dan Teknologi Pendidikan Fakultas Ilmu Pendidikan Universitas Pendidikan Indonesia. Bandung.

Satria E. (2009). Studi Algoritma Rijndael Dalam Sistem Keamanan Data. Skripsi Matematika. Universitas Sumatra Utara. Medan.

Wahono B. (2013). Perancangan Simulasi Pembelajaran Kriptografi Hill Cipher Menggunakan Metode Web Based Learning (WBL). Pelita Informatika Budi Darma volume V no.2.

Xintong Kit Choy. (2009). *Understanding AES Inverse Mix-Columns Transformation Calculation*, University of Wollongong.