PERANCANGAN APLIKASI KRIPTOGRAFI DENGAN METODE IDEA *(INTERNATIONAL DATA ENCRYPTION ALGORITHM)*

Fathur Rahman, Wagino, Dan Nur Alamsyah

Fakultas Teknologi Informasi Universitas Islam Kalimantan MAB
Email: Fathur@fti.uniska-bjm.ac.id

ABSTRAK

Dalam Penggunaan Kriptografi ada metode yang digunakan dalam penelitian ini yaitu Metode **IDEA (International Data Encryption Algorithm)** dimana metode IDEA ini ditujukan untuk mensimulasikan kriptografi denganmetodeIDEA yaitu untuk membantu pembelajaran metoda kriptografi IDEA dan perangkat lunak dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar.Hasil Penelitian ini untuk dapatmempelajaridan membantu tentang pemahaman Kriptografi dengan metodeIDEA, dimana hasil aplikasinya dapat di gunakan sebagai media pembelajaran bagi penguna program untuk mempelajari secara aplikasi/program sehingga pengguna paham dan mengerti materi pembelajaran tersebut.Sistem ini harus dapat memberikan informasi tentang pembelajaran kriptografi khususnya metode IDEA. Metode IDEA yang digunakan sangat membantu dalam memudahkan dalam proses Kriptografi sehingga dapat mudah dipelajari.

Kata Kunci : Kriptografi, IDEA, keamanan data

PENDAHULUAN

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu : Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas

atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data

lain kedalam data yang sebenarnya. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain. Non-repudiasi, atau nir penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman / terciptanya suatu informasi oleh yang mengirimkan / membuat.(Andri K., 2003)

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya yaituAlgoritma Simetris, Algoritma Asimetris dan Fungsi Hash. Salah satu metoda kriptografi yang dianggap sebagai algoritma *block cipher* yang terbaik dan teraman yang tersedia untuk publik sampai saat ini adalah metoda kriptografi IDEA (*International Data Encryption Algorithm*) dimana IDEA termasuk jenis Algoritma Simetris berdasarkan kunci yang dipakainya (Andi,2003)

International Data Encryption Algorithm (IDEA) adalah algoritma yang dikembangkan oleh Dr X. Lai dan Prof J. Massey di Swiss pada awal 1990 untuk menggantikan standar DES. Menggunakan tombol yang sama untuk enkripsi dan dekripsi, seperti DES beroperasi pada tanggal 8 byte pada suatu waktu. Tidak seperti DES meskipun menggunakan kunci 128-bit. Panjang kunci ini tidak memungkinkan untuk istirahat oleh hanya mencoba setiap kunci, dan tidak ada cara lain serangan dikenal. Ini adalah algorighm cepat, dan juga telah diimplementasikan dalam chipset perangkat keras, membuatnya lebih cepat. (Jusuf K., 2004)

Data Encryption Algoritma Internasional (IDEA) adalah blok cipher yang dirancang oleh James Massey dari ETH Zurich dan Xuejia Lai dan pertama kali dijelaskan pada 1991. Sebagai blok cipher, juga simetris. Algoritma ini dimaksudkan sebagai pengganti Data Encryption Standard (DES). IDEA merupakan revisi kecil dari Standar, cipher sebelumnya Enkripsi Usulan (PES); IDEA awalnya disebut Improved PES (IPES).

IDEA beroperasi pada 64-bit blok dengan menggunakan kunci 128-bit, dan terdiri dari serangkaian delapan transformasi identik (bulat, lihat ilustrasi) dan transformasi keluaran (setengah bulat). Proses untuk enkripsi dan dekripsi adalah sama. IDEA berasal banyak dari keamanan dengan interleaving operasi dari kelompok yang berbeda - Selain modular dan perkalian, dan bitwise exclusive OR (XOR) - yang secara aljabar "kompatibel" dalam arti tertentu. (Wikipedia, 2015)

Tujuan penyusunan penelitian ini adalah untuk mengembangkan suatu perangkat lunak yang mampu mensimulasikan kriptografi denganmetodeIDEA sehingga dapat digunakan sebagai bahan ajar berbasis digital.

METODE PENELITIAN

Perancangan dan Pembuatan aplikasi metode kriptografi IDEA memiliki langkah-langkah sebagai berikut :

1. Aplikasi dapat menginformasikan hasil proses pembentukan kunci, enkripsi dan dekripsi.
2. Masukan data dari user yaitu menerima *plaintext* sepanjang 8 karakter dan kunci sepanjang 16 karakter.
3. Adanya Materi dasar mengenai metode IDE pada Aplikasi tersebut
4. Hasil proses pada perangkat lunak dapat disesuaikan dengan cepat lambatnya banyaknya data yang diproses
5. *User* diasumsikan telah memahami dasar matematika kriptografi seperti operasi XOR, perkalian modulo, penjumlahan modulo, *Left Rotate*, dan konversi antar basis bilangan dan konversi dari bilangan ke *ASCII Code* yaitu mencakup biner ke desimal, heksadesimal ke desimal, biner ke heksadesimal, biner ke *ASCII Code*, heksadesimal ke *ASCII Code* dan sebaliknya.
6. Aplikasi dapat menampilkan tahapan proses perhitungan dalam biner dan heksadesimal.

HASIL DAN PEMBAHASAN

Perancangan dan Pembuatan aplikasi metode kriptografi IDEA memiliki langkah-langkah sebagai berikut :

1. Aplikasi dapat menginformasikan hasil proses pembentukan kunci, enkripsi dan dekripsi.
2. Masukan data dari user yaitu menerima *plaintext* sepanjang 8 karakter dan kunci sepanjang 16 karakter.
3. Adanya Materi dasar mengenai metode IDE pada Aplikasi tersebut
4. Hasil proses pada perangkat lunak dapat disesuaikan dengan cepat lambatnya banyaknya data yang diproses

5. *User* diasumsikan telah memahami dasar matematika kriptografi seperti operasi XOR, perkalian modulo, penjumlahan modulo, *Left Rotate*, dan konversi antar basis bilangan dan konversi dari bilangan ke *ASCII Code* yaitu mencakup biner ke desimal, heksadesimal ke desimal, biner ke heksadesimal, biner ke *ASCII Code*, heksadesimal ke *ASCII Code* dan sebaliknya.
6. Aplikasi dapat menampilkan tahapan proses perhitungan dalam biner dan heksadesimal.

1. Implementasi Sistem

Implementasi Aplikasi / program ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*).

2. Spesifikasi Perangkat Keras dan Perangkat Lunak

Program ini direkomendasikan untuk dijalankan dengan menggunakan perangkat keras (*hardware*) yang mempunyai spesifikasi berikut :

1. Prosesor Intel atau AMD Processor
2. Memory minimal 1GB.
3. Harddisk minimal 250 GB.
4. VGA *card*.
5. Monitor dengan minimal resolusi 1024 × 768 *pixel*.
6. *Keyboard* dan *Mouse*.

Adapun perangkat lunak (*software*) yang digunakan untuk menjalankan aplikasi ini adalah sistem operasi miniaml MS-Windows 7 atau MS-Windows terbaru / kompatibel.

3. Pengujian Program

Sebagai contoh, penggunaan atau simulasi aplikasi kriptografi dengan metode IDEA dengan melakukan menginput salah satu data untuk di coba di aplikasi yang telah selesai dibuat.

Untuk lebih memahami proses pembentukan kunci pada metoda IDEA, diberikan sebuah contoh berikut ini.

Misalkan : *Input* kunci = ‘METODA IDEA’

Proses pembentukan kuncinya adalah sebagai berikut :

KUNCI ENKRIPSI

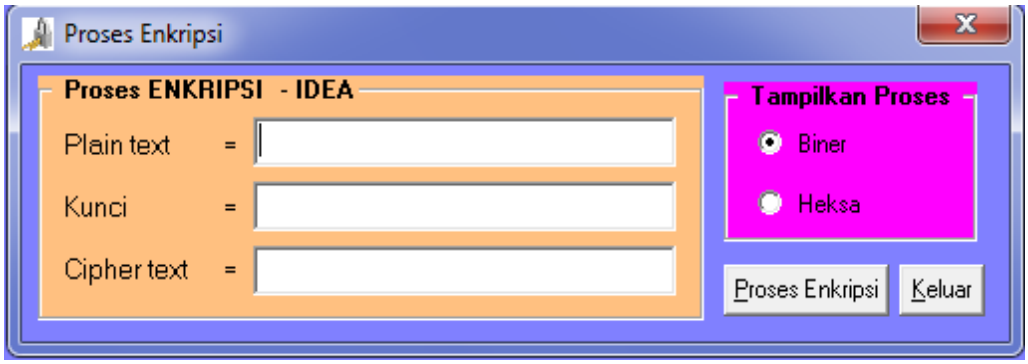
PUTARAN - 1
INPUT KUNCI :

0100110101000101010101000100111101000100010000010010000001001001010001
0001000101010000010010000001000110010001010101001001001001

Pecah menjadi 8 kelompok :

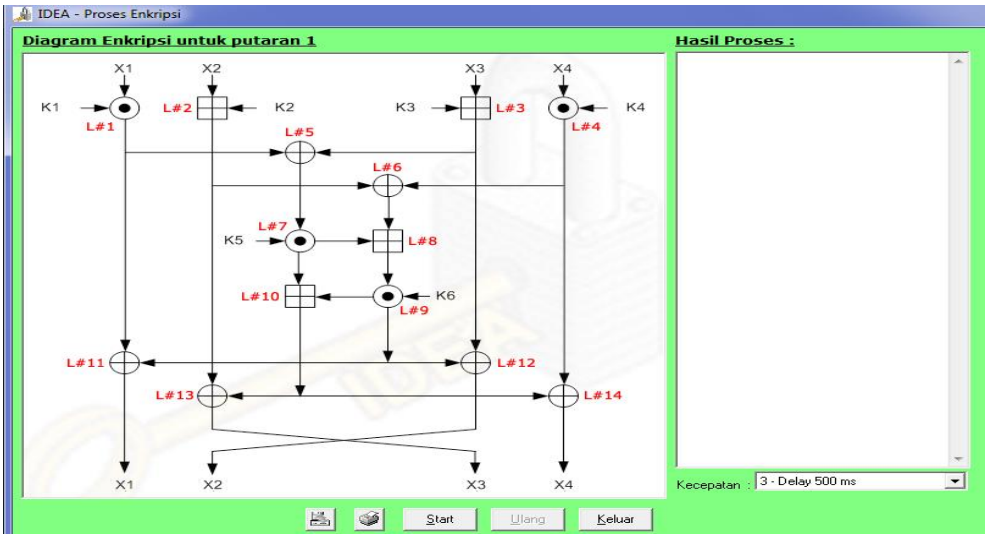
KE1 (Putaran 1) = 0100110101000101
KE2 (Putaran 1) = 0101010001001111
KE3 (Putaran 1) = 0100010001000001
KE4 (Putaran 1) = 0010000001001001
KE5 (Putaran 1) = 0100010001000101
KE6 (Putaran 1) = 0100000100100000
KE1 (Putaran 2) = 0100011001000101
KE2 (Putaran 2) = 0101001001001001

Setelah itu, bentuk muncul'proses enkripsiinput data'. Masukkanformat teksyang diinginkandalam kotak teks"teks biasa" dankunci dalamkotak teks"kunci enkripsi".



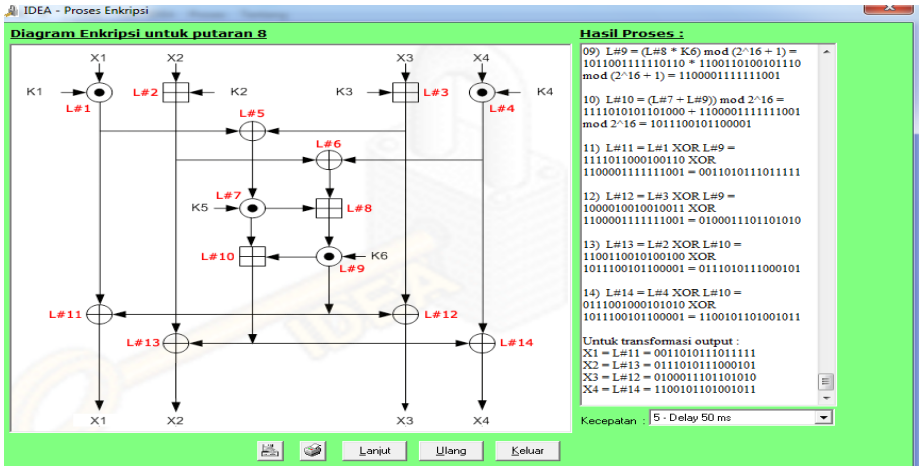
Gambar Prosedur untuk proses enkripsi

Pilih carauntuk melihathasil yang diinginkan. Setelah itu, klik"Process", bentuk'proses enkripsi' berikut akan ditampilkan :



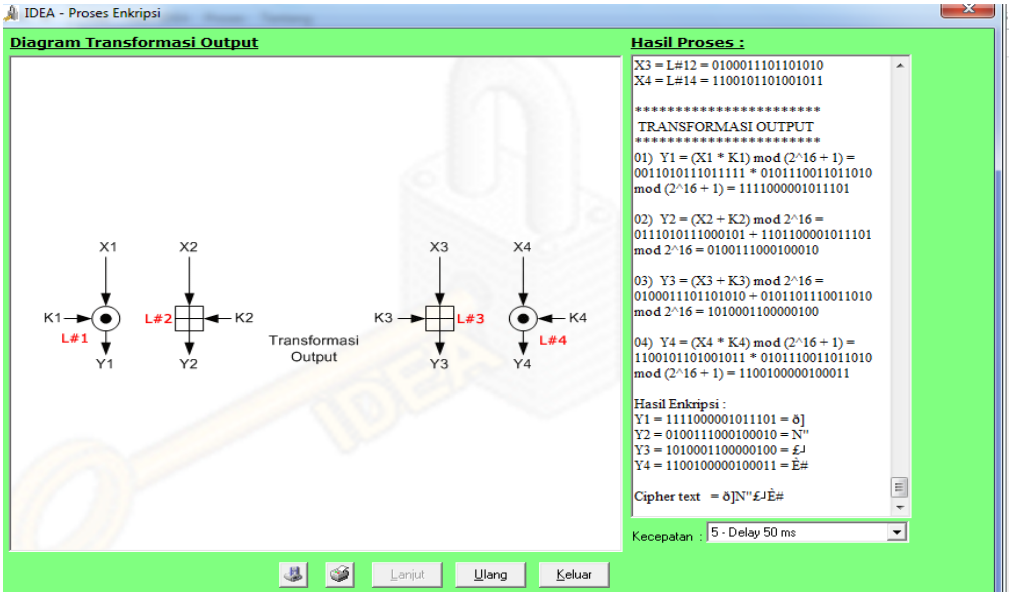
Gambar *Langkah proses enkripsi*

Kliktombol"Start / Mulai" untuk memulai prosesenkripsi. Hasilproses iniditunjukkan pada gambarberikut:



Gambar Prosedur untuk proses enkripsi

JikaAndamelanjutkan ketahap berikutnyadariprosesmengklik tombol'Next', maka prosesakan berlanjut.Jikaproses ini selesai, makatombol'Next' tidak dapat diakses.



Gambar Prosedur untuk proses enkripsi

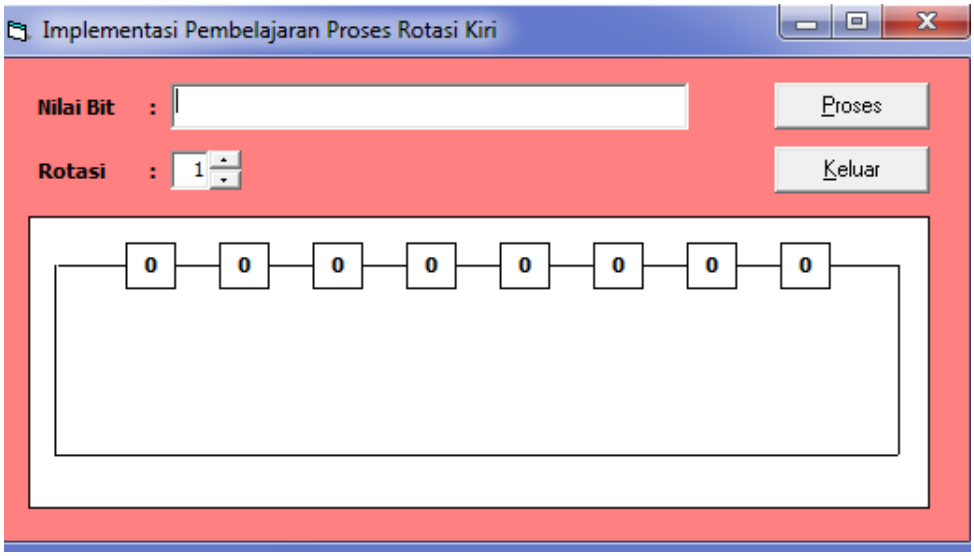
Prosedur pembentukan proses rotasi kiri, lakukan langkah berikut ini :

a. Klik pada menu ‘Proses’, pilih sub menu ‘Rotasi Kiri’ seperti terlihat pada gambar berikut ini :

b.

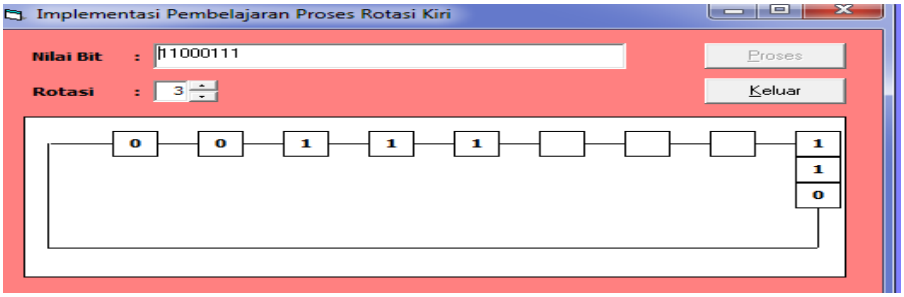
Gambar Prosedur untuk proses rotasi kiri

c. Setelah itu, akan muncul *form* ‘Rotasi Kiri’, seperti terlihat pada gambar berikut ini :

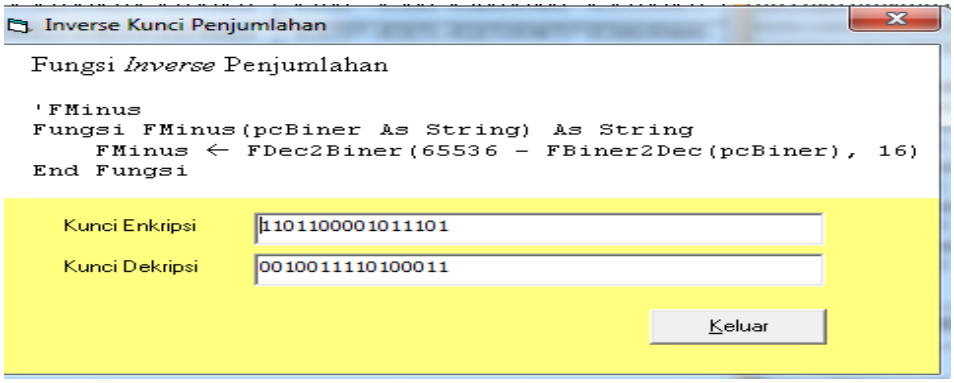


Gambar Prosedur untuk proses rotasi kiri

Masukkan nilaibitdaribitkotak teksdanlebarAnda ingin memutar. Klik"Process" untuk memulai prosesrotasikiridanbit outputakan ditampilkandalam kotak teks.

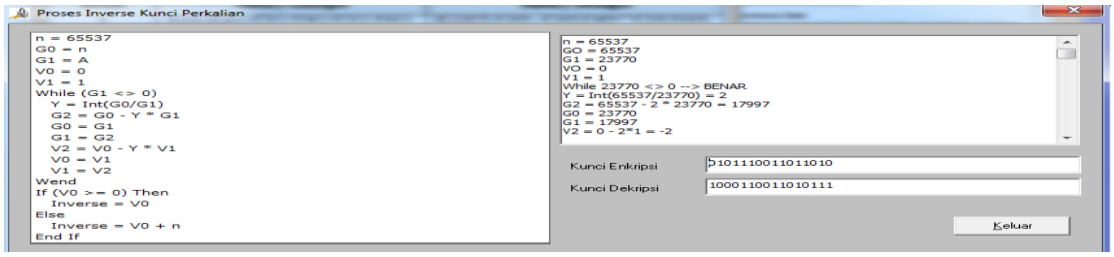


Gambar Prosedur untuk proses rotasi kiri



Gambar *Proses pembentukan kunci inverse penjumlahan*

Untuk contoh proses pembentukan kunci *inverse* perkalian, maka di *input* data ‘1101100001011101’.



Gambar 4. *Proses pembentukan kunci inverse perkalian*

KESIMPULAN

Berdasarkan uraian dari dari hal-hal di atas, maka hasil penelitian dapat diambil kesimpulan bahwa metode IDEA menyediakan kemudahan dalam proses pembelajaran tentang pemahaman Kriptografi dimana hasil aplikasinya dapat di gunakan sebagai media pembelajaran bagi penguna program untuk mempelajari secara aplikasi/program sehingga pengguna paham dan mengerti materi pembelajaran tersebut.

DAFTAR PUSTAKA

ANDI. (2003), ***Memahami Model Enskripsi dan Security Data***, Yogyakarta. Wahana Komputer.

Diffie, Whitfield, Martin E Hellman. 1998. ***New Directions in Cryptography***. IEEE Trans. Info. Theory IT-22.

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

Kristanto, Andri, ***Keamanan Data Pada Jaringan Komputer***, Gaya Media, 2003

Pranata, Antony. 2003. ***Pemograman Borland delphi 6***. Andi: Yogyakarta.

Trape and Washington. 2006***. Introduction to Cryptography with Coding Theory.*** USA : Pearson Education Inc.

https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm. Diakses tanggal : 13 Desember 2015