Pengamanan Data dengan Metoda Kriptografi IDEA

Aditya Pratama, A.Md., Daryanto, S.Kom., Lutfi Ali M, S.Si.
Teknik Informatika
Universitas Muhammadiyah Jember

ABSTRAK

Dalam sebuah masalah kerahasian data, data yang rahasia harus diamankan terlebih dahulu dengan berbagai macam cara, salah satunya adalah dengan menggunakan metoda kriptografi. 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*). Metoda ini terdiri dari 8 putaran (*round*) dan menggunakan 64 *bit plaintext* dengan panjang kunci sebesar 128 *bit*. Yang menjadi permasalahan dalam menyusun tugas akhir (skripsi) ini adalah bagaimana merancang perangkat lunak pembelajaran metoda kriptografi IDEA yang telah dikembangkan dengan inputan *plaintext* lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit). Sehingga nantinya menghasilkan sebuah aplikasi metoda kriptografi IDEA yang telah dikembangkan dengan inputan *plaintext* lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit).

Kata kunci : Kriptografi, IDEA, Plaintext.

1. Pendahuluan

Dalam sebuah masalah kerahasian data, data yang rahasia harus diamankan terlebih dahulu dengan berbagai macam cara, salah satunya adalah dengan menggunakan metoda kriptografi. Agar data / informasi yang dikirim tidak diketahui oleh orang lain yang tidak berkepentingan. Metoda kriptografi yang digunakan untuk mengamankan data ada bermacam – macam. Masing – masing metoda memiliki kelebihan dan kekurangan. 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*).

Metoda IDEA diperkenalkan pertama kali oleh Xuejia Lai dan James Massey pada tahun 1990 dengan nama PES (*Proposed Encryption Standard*). Setelah Biham dan Shamir mendemonstrasikan *cryptanalysis* yang berbeda, sang penemu memperkuat algoritma mereka dari serangan dan algoritma hasil pengubahan tersebut dan diberi nama IPES (*Improved Proposed Encryption Algorithm*). Kemudian pada tahun 1992, IPES diganti namanya menjadi IDEA (*International Data Encryption Algorithm*).

Metoda IDEA ini menggunakan beberapa operasi dasar, seperti operasi logika *XOR* (*Exclusive – OR*), operasi perkalian mod $2^{16} + 1$ (*multiplication modulo* $2^{16} + 1$) dan operasi penambahan mod 2^{16} (*addition modulo* 2^{16}). Metoda ini terdiri dari 8 putaran (*round*) dan menggunakan 64 *bit plaintext* dengan panjang kunci sebesar 128 *bit*.

Berdasarkan uraian di atas, penulis bermaksud untuk mengambil tugas akhir (skripsi) dengan judul " Pengamanan Data dengan Metoda Kriptografi IDEA ".

2. Kriptografi

Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula dengan menggunakan berbagai macam teknik yang telah ada sehingga informasi tersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan.

Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan 4 aspek keamanan dari suatu informasi yakni kerahasiaan (*confidentiality*), integritas data (*data integrity*), otentikasi (*authentication*), dan ketiadaan penyangkalan (*non-repudiation*). (Menezes. et al,1996) (Scheiner. B., 1996). Keempat aspek tersebut merupakan tujuan utama dari suatu sistem kriptografi yang dapat dijelaskan sebagai berikut,

a. Kerahasiaan (*confidentiality*)

Kerahasiaan bertujuan untuk melindungi suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut. Terdapat beberapa cara yang dapat digunakan untuk menjaga kerahasiaan suatu informasi, mulai dari penjagaan secara fisik misalnya menyimpan data pada suatu tempat khusus sampai dengan penggunaan algoritma matematika untuk mengubah bentuk informasi menjadi tidak terbaca.

b. Integritas data (*data integrity*)

Integritas data bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut. Untuk menjamin integritas data ini kita harus mempunyai kemampuan untuk mendeteksi terjadinya manipulasi data oleh pihak-pihak yang tidak berkepentingan. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.

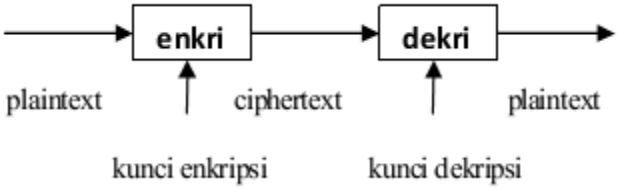
c. Otentikasi (*authentication*)

Otentikasi merupakan identifikasi yang dilakukan oleh masing – masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian dari informasi yang diterima. Identifikasi terhadap suatu informasi dapat berupa tanggal pembuatan informasi, isi informasi, waktu kirim dan hal-hal lainnya yang berhubungan dengan informasi tersebut.

d. *Non-repudiation*

Non-repudiation berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang telah dilakukan oleh pelaku aksi itu sendiri. Jika terjadi penyangkalan maka diperlukan suatu prosedur yang melibatkan pihak ketiga untuk menyelesaikan masalah tersebut.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Sepertiyang telah dijelaskan di atas, proses enkripsi mengubah plaintext menjadi ciphertext (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.



Gambar 1. Diagram proses enkripsi dan dekripsi

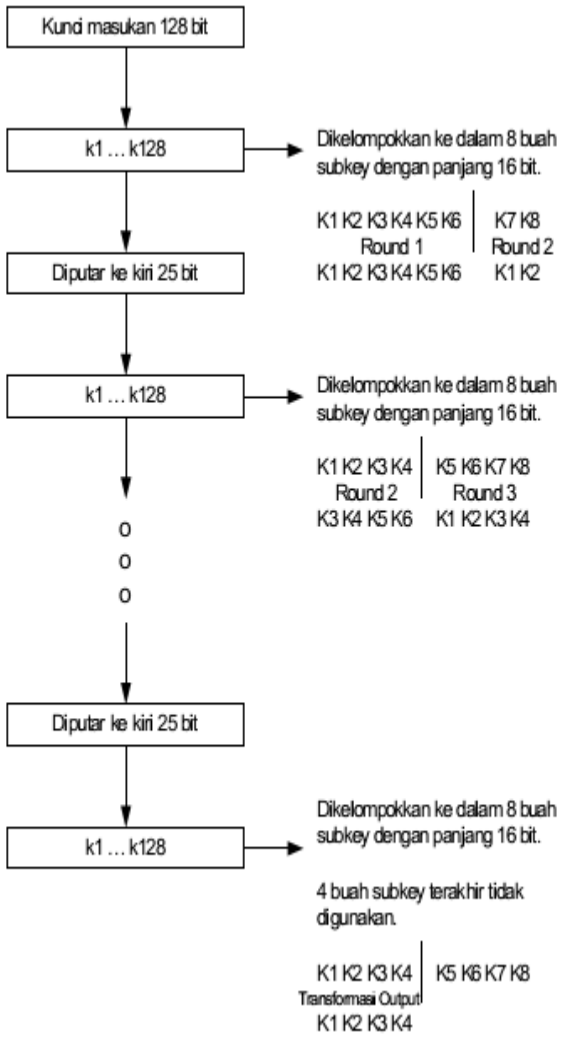
3. Algoritma IDEA (International Data Encryption Algorithm)

Metoda IDEA diperkenalkan pertama kali oleh Xuejia Lai dan James Massey pada tahun 1990 dengan nama PES (Proposed Encryption Standard). Kemudian pada tahun 1992, IPES diganti namanya menjadi IDEA (International Data Encryption Algorithm). IDEA merupakan *block cipher* (cipher blok), yang beroperasi pada blok *plaintext* 64 *bit*. Panjang kuncinya 128 *bit*. Algoritma yang sama digunakan untuk proses enkripsi dan dekripsi. IDEA menggunakan operasi aljabar yang tidak kompatibel sebagai berikut (Scheiner. B., 1996),

a. Pembentukan Kunci

Proses pembentukan ini dimulai dengan membagi 128 bit key menjadi 8 buah 16 bit subkey. Ini merupakan delapan subkey pertama untuk algoritma dengan perincian enam subkey pertama untuk putaran (round) 1 dan dua subkey terakhir untuk putaran 2. Key dirotasikan 25 bit ke kiri dan dibagi menjadi 8 subkey lagi. Ini

merupakan delapan subkey kedua untuk algoritma dengan perincian empat subkey pertama untuk putaran 2 dan empat subkey terakhir untuk putaran 3. Algoritma hanya menggunakan 52 buah subkeydengan perincian 6 buah subkey untuk 8 putaran ditambah 4 buah subkey untuk transformasi output.Proses pembentukan kunci dapat dilihat pada gambar di bawah ini :



Gambar 2. Proses Pembentukan kunci IDEA

b. Enkripsi

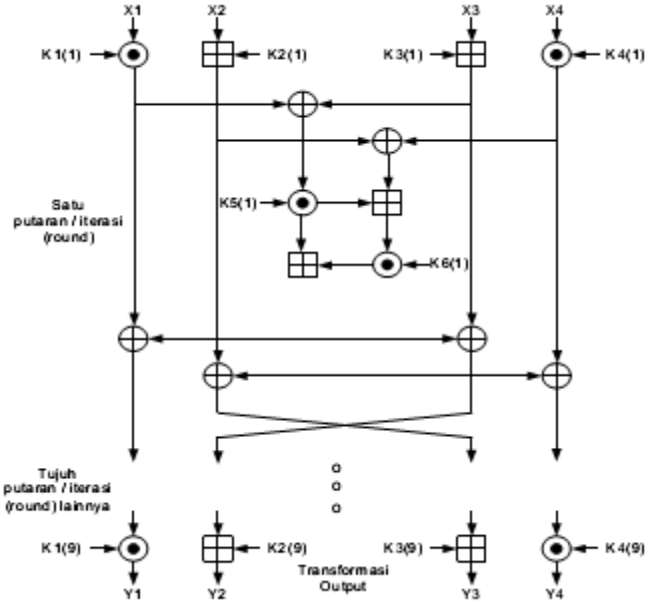
Proses enkripsi algoritma IDEA adalah sebagai berikut, Pertama – tama, plaintext 64 bit dibagi menjadi 4 buah sub blok dengan panjang 16 bit, yaitu X1, X2, X3, X4. Empat sub blok ini menjadi masukan bagi iterasi tahap pertama algoritma. Total terdapat 8 iterasi. Pada setiap iterasi, 4 sub blok di-XOR-kan, ditambahkan, dikalikan dengan yang lain dan dengan 6 buah subkey 16 bit. Diantara iterasi sub blok kedua dan ketiga saling dipertukarkan. Akhirnya 4 buah sub blok dikombinasikan dengan 4 subkey dalam transformasi output. Pada setiap tahapan, urutan berikut ini dikerjakan :

1. Kalikan X1 dengan K1 mod (216 + 1).
2. Tambahkan X2 dengan K2 mod 216.
3. Tambahkan X3 dengan K3 mod 216.
4. Kalikan X4 dengan K4 mod (216+ 1).
5. XOR hasil dari step 1 dan 3.
6. XOR hasil dari step 2 dan 4.
7. Kalikan hasil step 5 dengan K5 mod (216+ 1).
8. Tambahkan hasil step 6 dan 7 mod 216.
9. Kalikan hasil step 8 dengan K6 mod (216+ 1).
10. Tambahkan hasil dari step 7 dan 9.
11. XOR hasil dari step 1 dan 9.
12. XOR hasil dari step 3 dan 9.
13. XOR hasil dari step 2 dan 10.
14. XOR hasil dari step 4 dan 10.

Output dari setiap round adalah empat sub blok yang dihasilkan pada langkah 11, 12, 13 dan 14. Sub blok 12 dan 13 di-swap (kecuali untuk putaran terakhir) sehingga input dari putaran berikutnya adalah hasil kombinasi dari langkah 11 13 12 14.Setelah 8 putaran, akan dilakukan tranformasi output berikut :

1. Kalikan X1 dengan subkey K1 mod (216+ 1).
2. Tambahkan X2 dengan subkey K2 mod 216.
3. Tambahkan X3 dengan subkey K3 mod 216.
4. Kalikan X4 dengan subkey K4 mod (216+ 1).

Proses enkripsi algoritma IDEA dapat dilihat pada gambar berikut ini :



Gambar 3. Proses Enkripsi Algoritma IDEA

c. Dekripsi

Proses dekripsi sama persis dengan proses enkripsi. Perbedaannya hanya terletak pada aturan dari subkey-nya. Urutan subkey terbalik dengan proses enkripsi dan subkey-nya di-inverse-kan.Subkey pada langkah transformasi output pada proses enkripsi di-inverse-kan dan digunakan sebagai subkey pada putaran 1 pada proses dekripsi. Subkey pada putaran 8 di-inverse-kan dan digunakan sebagai subkey pada putaran 1 dan 2 pada proses dekripsi. Demikian seterusnya.Proses dekripsi menggunakan algoritma yang sama dengan proses enkripsi tetapi 52 buah subblok kunci yang digunakan masing-masing merupakan hasil turunan 52 buah subblok kunci enkripsi. Pada kasus ini akan diambil invers dari operasi penambahan oleh mod 216dan perkalian mod 216+1, tergantung pada operasi yang dibuat pada fase enkripsi. Setiap subkunci dekripsi adalah salah satu dari invers penambahan atau perkalian yang berkorespondensi dengan subkunci enkripsi.

4. Perangkat Lunak Pembelajaran

Seiring dengan perkembangan peradaban manusia dan kemajuan pesat di bidang teknologi, tanpa disadari komputer telah ikut berperan dalam dunia pendidikan terutama penggunaannya sebagai alat bantu pengajaran. Percobaan penggunaan komputer untuk proses belajar dimulai di Amerika Serikat pada akhir tahun 1950-an dan awal tahun 1960-an. Perangkat lunak pembelajaran dengan komputer muncul dari sejumlah disiplin ilmu, terutama ilmu komputer dan psikologi.

Dari ilmu komputer dan matematika muncul program – program yang membuat semua perhitungan dan fungsi lebih mudah dan bermanfaat. Sedangkan dari ilmu psikologi muncul pengetahuan mengenai teori belajar, teknik belajar, serta motivasi yang baik.

5. Rancangan Arsitektur

Perangkat lunak pembelajaran ini dirancang dengan menggunakan bahasa pemrograman *Microsoft Visual Basic 6.0*. Perangkat lunak pembelajaran ini dirancang dengan menggunakan beberapa *form*, antara lain :

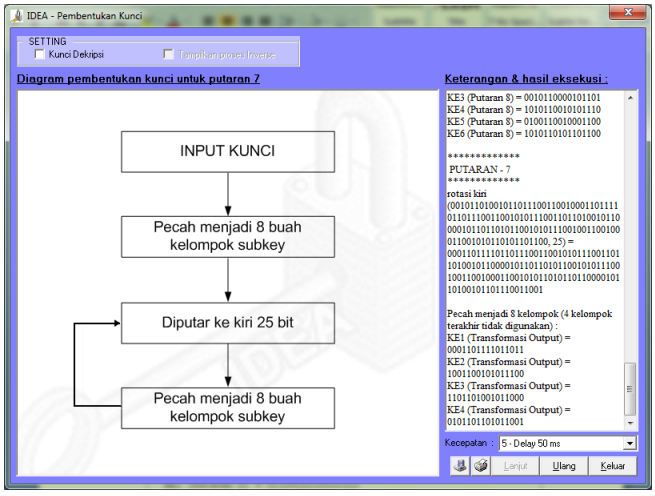
1. *Form Main*.
2. *Form* Input Proses Pembentukan Kunci.
3. *Form* Input Proses Enkripsi.
4. *Form* Input Proses Dekripsi.
5. *Form* Tampilan Proses Pembentukan Kunci.
6. *Form* Tampilan Proses Enkripsi / Dekripsi.
7. *Form* Teori.
8. *Form About*.

6. Pengujian dan Hasil

Pada proyek akhir ini dilakukan pengujian dan analisa system terhadap performansi dari kriptografi IDEA.

6.1 Pengujian dan Analisa Implementasi Proses Pembentukan Kunci

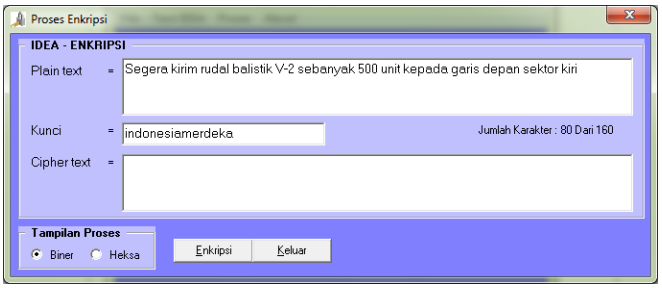
Pengujian aplikasi pada proses pembentukan kunci metoda IDEA akan menghasilkan tampilan proses pembentukan kunci beserta tahapan-tahapan dan perhitungan pada program aplikasi yang telah di bangun. Untuk lebih jelasnya dapat dilihat pada gambar dibawah.



Gambar 4. Tampilan Aplikasi Proses Pembentukan kunci Algoritma IDEA

6.2 Pengujian dan Analisa Implementasi Proses Enkripsi Metoda IDEA

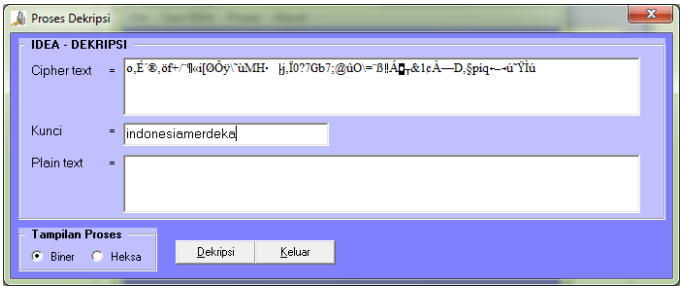
Pengujian enkripsi metoda IDEA akan dilakukan pada data string dimana tujuan dari pengujian ini adalah untuk mengetahui kebenaran dari metode enkripsi IDEA yang telah dibuat serta pengembangan dari plaintext 64 bit (8 karakter) menjadi kurang dari dan lebih dari 64 bit. Untuk lebih jelasnya dapat dilihat gambar dibawah ini.



Gambar 5. Tampilan Aplikasi Proses Enkripsi Algoritma IDEA

6.3 Pengujian dan Analisa Implementasi Proses Dekripsi Metoda IDEA

Pengujian dekripsi metoda IDEA dilakukan pada program aplikasi dimana tujuannya adalah mengembalikan teks hasil enkripsi yang telah dilakukan sebelumnya (ciphertext) menjadi plaintext sesuai dengan inputn awal. Untuk lebih jelasnya dapat dilihat gambar dibawah ini.



Gambar 6. Tampilan Aplikasi Proses Dekripsi Algoritma IDEA

6.4 Hasil Pengujian

Untuk pengujian Proses Enkripsi telah di berikan inputan berupa teks, angka maupun kombinasi teks dan angka. Agar lebih jelasnya dapat di lihat table berikut

No	Plain Text	bit	Key	bit	Cipher Text
1	abcdefgh	64	kriptografi-idea	128	KkE¿r0«c
2	abcd	32	kriptografi-idea	128	‹Ý!ÁÁÉ"
3	abcdefgh ijklmnop	128	kriptografi-idea	128	9ùyçÙ¤e bOWm#ZX
4	abcde 1234	72	kriptografi-idea	128	žœf6†¼ U~@ùS~!
5	12345678 90	80	kriptografi-idea	128	&4Å"A÷☐ ì((8'8?Ü

Tabel 1 Hasil pengujian Proses Enkripsi

Untuk pengujian Proses Dekripsi di berikan inputan berupa Cipher text dari pengujian Proses Enkripsi. Agar lebih jelasnya dapat di lihat table berikut

No	Cipher Text	Key	bit	Plain Text	bit
1	KkE¿r0«c	kriptografi-idea	128	abcdefgh	64
2	‹Ý!ÁÁÉ"	kriptografi-idea	128	abcd	32
3	9ùyçÙ¤e bOWm#ZX	kriptografi-idea	128	abcdefgh ijklmnop	128
4	žœf6†¼ U~@ùS~!	kriptografi-idea	128	abcde 1234	72
5	&4Å"A÷☐ ì((8'8?Ü	kriptografi-idea	128	12345678 90	80

Tabel 2 Hasil pengujian Proses Dekripsi