ISSN : 1978-6603

JURNAL Ilmiah SAINTIKOM Sains dan Komputer

PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI SIMETRI IDEA

Iskandar Zulkarnain, Ramenra Sinaga, Saniman

Program Studi Sistem Komputer, STMIK Triguna Dharma
Jl. A.H. Nasution No. 73 F-Medan
iskandar.z@gmail.com

Abstrak

Banyak algoritma kriptografi modern yang walaupun menyediakan keamanan tinggi, namun sangat susah dimengerti dan dipelajari masyarakat awam. Tujuan dari penelitian ini adalah untuk membangun suatu perangkat lunak yang tidak hanya bisa menjaga keamanan data dengan kuat dan handal, tapi juga mudah dimengerti banyak orang. Untuk itu algoritma IDEA dipilih, karena algoritma ini termasuk algoritma yang memuaskan user selain dengan kekuatan dan kehandalannya dari berbagai serangan para *kript analis*, dengan kemudahannya dipelajari semua orang. Sistem ini dikembangkan menggunakan bahasa pemrograman Visual Basic 6.0. Analisis kebutuhan perangkat lunak algoritma IDEA dilakukan dengan menentukan nama perangkat lunak yang akan dibangun, mengetahui siapa yang akan menggunakan perangkat lunak tersebut, memahami konsep teknologi yang akan dipakai, membuat tampilan antar muka yang mendidik, menentukan teknik yang dipergunakan untuk membentuknya, serta menguji hasil perangkat lunak tersebut. Simpulan dari paparan diatas bahwa Pengamanan data tersebut selain bertujuan meningkatkan keamanan, juga berfungsi untuk: Melindungi data agar tidak dapat dibaca oleh orang-orang yang tidak berhak, menyisipkan atau menghapus data. Algoritma ini menyediakan keamanan yang cukup tinggi dengan tidak didasarkan atas kerahasiaan algoritmanya akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan.

Kata Kunci: Perancangan, sistem keamanan data, algoritma kriptografi simetri idea

Abstrack

Many modern cryptographic algorithms that even provide high security, but it is very difficult to understand and learn the general public. The purpose of this study is to develop a software that not only can keep your data secure with strong and reliable, but also easy to understand a lot of people. For the IDEA algorithm chosen, because these algorithms includes algorithms that satisfy the user than with the strength and reliability of the various attacks of the cryptanalyst, with studied ease everyone. This system was developed using Visual Basic 6.0. Software needs analysis conducted by IDEA algorithm specifies the name of the software to be built, knowing who is going to use the software, understand the concept of technology that will be used, making the interface that educates, a technique used to determine the shape, as well as test results of software. The conclusions from the above that the exposure to data security in addition aims to increase security, also serves to: Protect your data so it can not be read by people who are not entitled to, insert or delete data. This algorithm provides high security with the algorithm based on secrecy but with more emphasis on the security/confidentiality of the key used.

Key Words: Design, data security systems, cryptography algorithms symmetry idea

PENDAHULUAN

Sistem keamanan pengiriman data (komunikasi data yang aman) dipasang untuk mencegah pencurian, kerusakan, dan penyalahgunaan data yang terkirim melalui jaringan komputer. Dalam praktek, pencurian data berwujud pembacaan oleh pihak yang tidak berwenang biasanya dengan menyadap saluran publik. Teknologi jaringan komputer telah dapat mengurangi bahkan membuang kemungkinan adanya kerusakan data akibat buruknya konektivitas fisik, namun gangguan tetap bisa terjadi karena ada unsur kesengajaan yang mengarah ke penyalah gunaan sistem dari pihak-pihak tertentu.

IDEA (International Data Encryption Algorithm) merupakan sebuah algoritma kriptografi simetri yang diciptakan pada awalnya sebagai pengganti *Data Encryption Standard* (DES). IDEA adalah sebuah revisi kecil dari cipher yang lebih awal, yakni PES (*Proposed Encryption Standard*). Pada awalnya, IDEA disebut IPES (*Improved PES*). Algoritma IDEA terbilang sederhana karena hanya melibatkan 3 proses utama dan 9 putaran.

Algoritma ini merupakan algoritma yang menyediakan keamanan cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya (algoritma *restricted*), akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan (algoritma *kriptografi modern*). Algoritma *restricted* biasanya digunakan oleh sekelompok orang untuk bertukar pesan satu sama lain, mereka membuat suatu algoritma enkripsi yang hanya diketahui oleh anggota kelompok itu saja, sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma *restricted* tersebut harus diganti karena kemungkinan anggota kelompok yang keluar itu dapat membocorkan algoritmanya.

Namun algoritma *kriptografi modern,* seperti algoritma IDEA ini, dapat mengatasi masalah tersebut dengan menggunakan kunci, yang dalam hal ini algoritmanya tidak lagi dirahasiakan, tetapi kunci harus dijaga kerahasiaannya. Sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma yang dipakai tidak perlu diganti, namun cukup mengganti kuncinya saja.

Perumusan Masalah

Beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah sebagai berikut:

1. Bagaimana aspek kerahasiaan pada algoritma kriptografi simetri IDEA yang ditinjau berdasarkan: kompleksitas algoritma, karakteristik penyandian *plaintext* terhadap *chipertext*.
2. Bagaimana membangun sistem yang dapat menjaga kerahasiaan data menggunakan *algoritma kriptografi simetri IDEA* menggunakan Bahasa pemrograman Visual basic 6.0.

Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Menganalisis bagaimana cara kerja algoritma kriptografi simetri IDEA dalam memberi layanan kerahasiaan data.
2. Membangun suatu program yang dapat menjaga keamanan data menggunakan algoritma kriptografi simetri IDEA

Metodologi Penelitian

Langkah-langkah yang dilakukan penulis antara lain dengan melakukan studi pustaka yang diantaranya :

1. Penelitian Pustaka (*library research*)
   Studi pustaka yang dilakukan penulis dengan membaca, mengumpulkan materi serta menjadikan referensi dari buku-

buku yang berkaitan dengan algoritma kriptografi simetri IDEA.

2. Penelitian literatur (*literature study research*)
   Pada penelitian lapangan dilakukan dengan langsung melakukan analisis terhadap algoritma kriptografi simetri IDEA.

LANDASAN TEORI

Kriptografi

Kriptografi berasal dari dua suku kata yaitu *kripto* dan *grafi*. Kripto artinya menyembunyikan, sedangkan grafi artinya ilmu seni. Kriptografi (*Cryptography*) adalah suatu ilmu yang mempelajari sistem sandi untuk menjamin kerahasiaan dan keamanan data, yang kegiatannya dilakukan oleh seorang *kriptographer*.

Kriptografi secara umum merupakan ilmu dan seni untuk menjaga kerahasian berita (*Scheiner*. B.,1996). Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes. et al,1996).

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi (Menezes. et al,1996) (Scheiner. B., 1996), yaitu:

1. Kerahasiaan (*Confidentiality*), adalah layanan yang digunakan untuk menjaga isi informasi dari siapapun, kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.

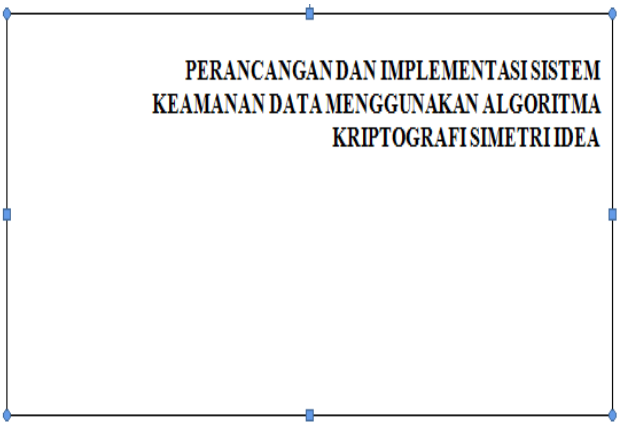
Pembahasan Proses IDEA

Proses penyelesaian metoda kriptografi IDEA ini dapat dibagi menjadi 3 tahapan yaitu :

1. Proses Pembentukan Kunci.
2. Proses Enkripsi.
3. Proses Deskripsi.

Proses Pembentukan Kunci

Metoda IDEA memiliki *input* 128 bit kunci (*key*) yang identik dengan 32 digit heksadesimal ataupun 16 karakter yang diproses untuk menghasilkan 52 buah *subkey* dengan perincian masing-masing 6 buah *subkey* akan digunakan pada 8 putaran dan 4



buah *subkey* untuk transformasi output.

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

Misalkan: *Input* kunci = ‘METODA IDEA FERI’

Proses Enkripsi

Proses enkripsi dari metoda IDEA terdiri dari 8 iterasi (putaran) ditambah satu putaran transformasi output. Proses ini memiliki *input* data *plaintext* 64 bit yang identik dengan 16 digit heksadesimal atau 8 karakter.

Proses enkripsi dari metoda IDEA dapat dilihat pada contoh berikut ini.

Misalkan *plaintext* = 'FERIFERI' dengan kunci yang dihasilkan di atas.

Perancangan

Perangkat lunak pembelajaran ini dirancang dengan menggunakan bahasa pemrograman *Microsoft Visual Basic 6.0* dan menggunakan fasilitas menu editor untuk membuat dan mengatur tampilan menu *pull down*.

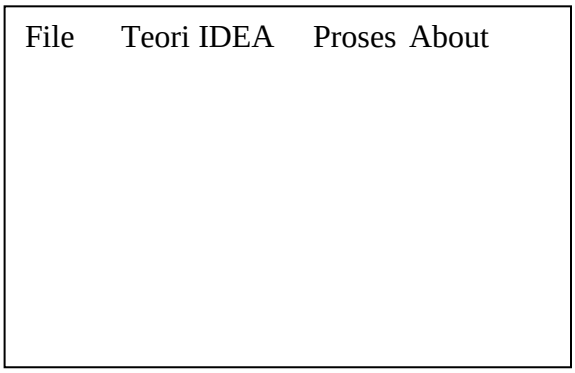
Perangkat lunak pembelajaran ini dirancang dengan menggunakan beberapa *form*, antara lain :

1. *FormSplash Screen* sebagai tampilan awal (pembuka).
2. *Form Main*.
3. *Form* Input Proses Pembentukan Kunci.
4. *Form* Input Proses Enkripsi.
5. *Form* Input Proses Dekripsi.
6. *Form* Tampilan Proses Pembentukan Kunci.
7. *Form* Tampilan Proses Enkripsi / Dekripsi.
8. *Form* Teori.
9. *Form About*.

Form Splash Screen

Gambar 3.1 Rancangan Form Splash Screen

Form Main

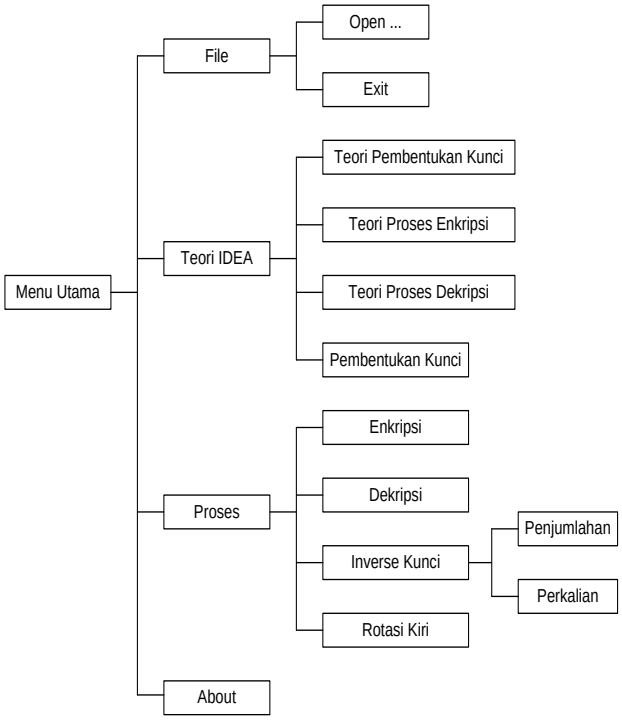


Gambar 3.2 Rancangan Form Main

Keterangan :

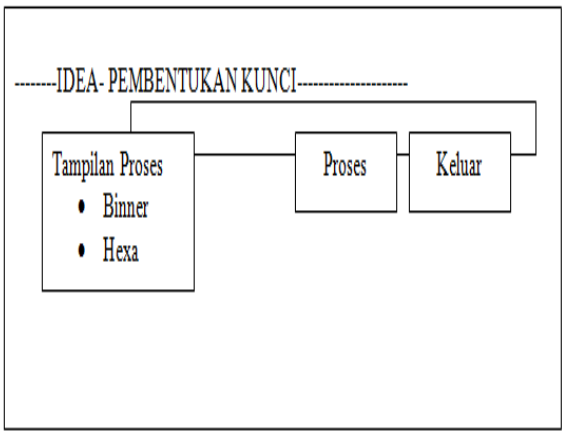
1. *Title bar*, berisi tulisan 'Perangkat Lunak Pembelajaran Kriptografi Metode IDEA'.
2. Tombol 'Minimize', berfungsi untuk memperkecil *form*.
3. Tombol 'Maximize', berfungsi untuk memperbesar *form*.
4. tombol 'Close', berfungsi untuk menutup *form*.
5. *Menu bar*, berisi menu-menu sebagai berikut :
   a. 'File' terdiri dari sub menu :
      i. 'Open …', berfungsi untuk membuka *file* hasil eksekusi yang telah disimpan sebelumnya.
      ii. 'Exit', berfungsi untuk keluar dari perangkat lunak.
   b. 'Teori IDEA' terdiri dari sub menu :
      i. 'Pembentukan Kunci', berfungsi untuk menampilkan teori mengenai proses pembentukan kunci pada metode IDEA.
      ii. 'Proses Enkripsi', berfungsi untuk menampilkan teori mengenai proses enkripsi pada metode IDEA.
      iii. 'Proses Dekripsi', berfungsi untuk menampilkan teori mengenai proses dekripsi pada metode IDEA.
   c. 'Pembelajaran', terdiri dari sub menu :
      i. 'Proses Pembentukan Kunci', berfungsi untuk memanggil *form* 'Input Proses Pembentukan Kunci'.
      ii. 'Proses Enkripsi', berfungsi untuk memanggil *form* 'Input Proses Enkripsi'.
      iii. 'Proses Dekripsi', berfungsi untuk memanggil *form* 'Input Proses Dekripsi'.
   d. 'About', berfungsi untuk memanggil *form* 'About'.

6. badan *form*
   Rancangan menu dari perangkat lunak ditunjukkan oleh gambar berikut ini :



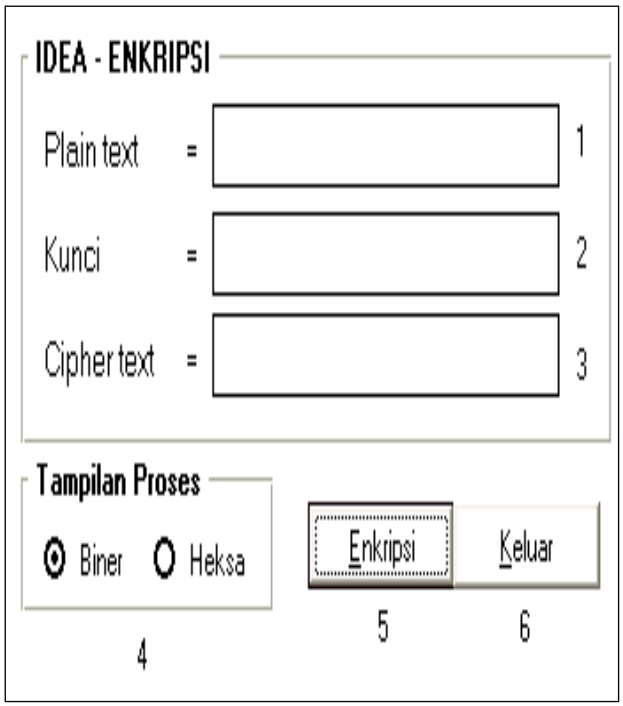
Gambar 3.3 Rancangan menu dari perangkat lunak

Form Input Proses Pembentukan Kunci



Gambar 3.4 Rancangan Form Input Proses Pembentukan Kunci

Form Input Proses Enkripsi

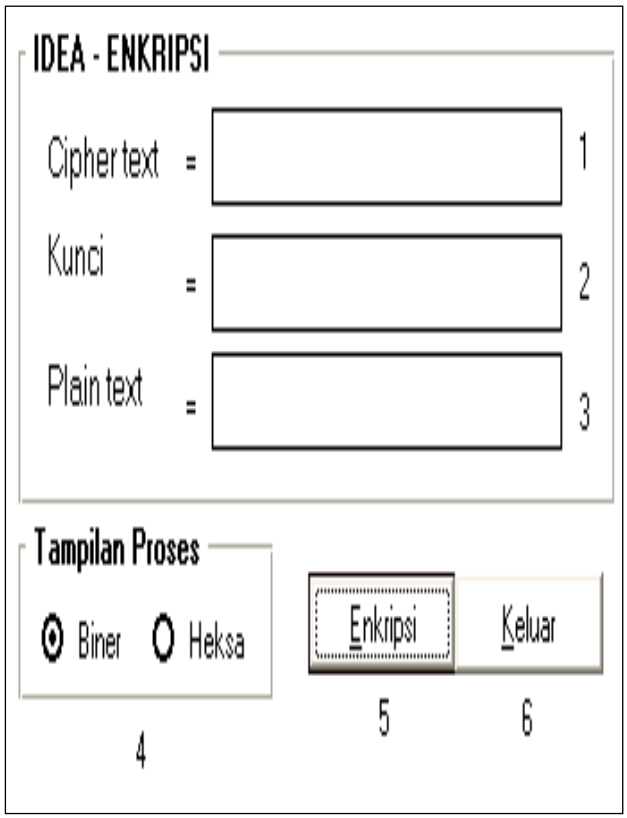


Gambar 3.5 Rancangan Form Input Proses Enkripsi

Keterangan :

1. *Text box*, berfungsi untuk meng-*input plaintext*.
2. *Text box*, berfungsi untuk meng-*input* kunci.
3. *Text box*, berfungsi untuk menampilkan hasil *ciphertext*.
4. Daerah 'Tampilan Proses', berisi *option button* 'Biner' dan 'Heksa' untuk mengatur tampilan proses yang diinginkan.
5. Tombol 'Enkripsi', berfungsi untuk menampilkan *form* 'Proses Enkripsi /Dekripsi'.
6. tombol 'Keluar', berfungsi untuk keluar dari perangkat lunak.

Form Input Proses Dekripsi

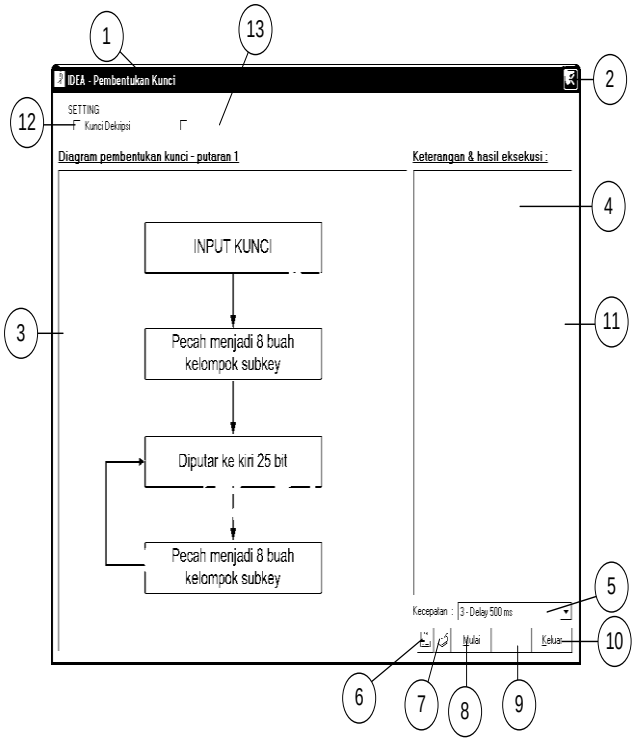


Gambar 3.6 Rancangan Form Input Proses Dekripsi

Keterangan :

1. *Text box*, berfungsi untuk meng-*input ciphertext*.
2. *Text box*, berfungsi untuk meng-*input* kunci.
3. *Text box*, berfungsi untuk menampilkan hasil *plaintext*.
4. Daerah 'Tampilan Proses', berisi *option button* 'Biner' dan 'Heksa' untuk mengatur tampilan proses yang diinginkan.
5. Tombol 'Dekripsi', berfungsi untuk menampilkan *form* 'Proses Enkripsi / Dekripsi'.
6. Tombol 'Keluar', berfungsi untuk keluar dari perangkat lunak.

3.3.1. Form Proses Pembentukan Kunci



Gambar 3.7 Rancangan Form Proses Pembentukan Kunci

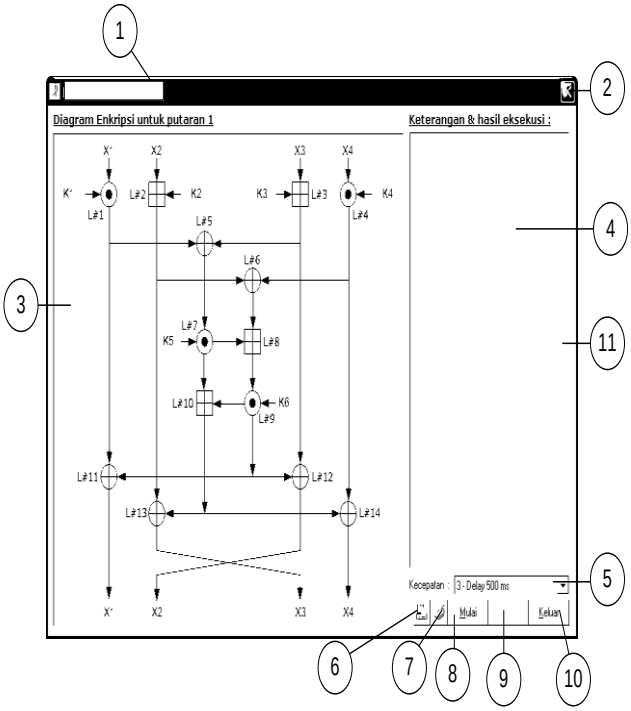
Keterangan :

1. *Title bar*, berisi tulisan 'IDEA - Proses Pembentukan Kunci'.
2. Tombol 'Close', berfungsi untuk menutup *form*.
3. Daerah tampilan diagram dari algoritma.
4. daerah tampilan hasil eksekusi.
5. *Combo box* 'Kecepatan', berfungsi untuk mengatur kecepatan algoritma.
6. Tombol 'Simpan', berfungsi untuk menyimpan hasil proses eksekusi.
7. Tombol 'Cetak', berfungsi untuk mencetak hasil proses eksekusi.
8. Tombol 'Mulai', berfungsi untuk memulai proses pembentukan kunci.
9. Tombol 'Ulangi', berfungsi untuk mengulangi proses pembentukan kunci.

10. Tombol ‘Keluar’, berfungsi untuk keluar dari *form*.
11. *Vertical scrollbar*.
12. *Checkbox*‘Kunci Dekripsi’, jika dipilih maka akan menampilkan proses kuncidekripsi.
13. *Checkbox* ‘Tampilkan proses Inverse’, jika dipilih maka akan menampilkan

proses inverse kunci.

Form Proses Enkripsi / Dekrips

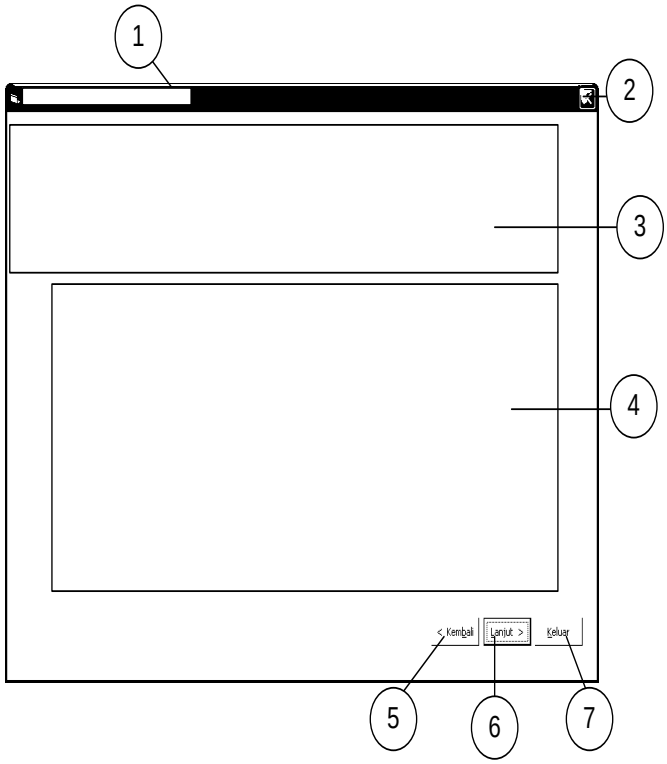


Gambar 3.8 Rancangan Form Proses Enkripsi /Dekripsi

Keterangan :

1. *Title bar*, berisi tulisan ‘IDEA - Proses xxx’.
2. Tombol ‘Close’, berfungsi untuk menutup *form*.
3. Daerah tampilan diagram dari algoritma.
4. Daerah tampilan hasil eksekusi.
5. *Combo box* ‘Kecepatan’, berfungsi untuk mengatur kecepatan algoritma.
6. Tombol ‘Simpan’, berfungsi untuk menyimpan hasil proses eksekusi.
7. Tombol ‘Cetak’, berfungsi untuk mencetak hasil proses eksekusi.
8. Tombol ‘Mulai’, berfungsi untuk memulai proses enkripsi / dekripsi.
9. Tombol ‘Ulang’, berfungsi untuk mengulangi proses enkripsi / dekripsi.
10. Tombol ‘Keluar’, berfungsi untuk keluar dari *form*.
11. *Vertical scrollbar*.

Form Teori



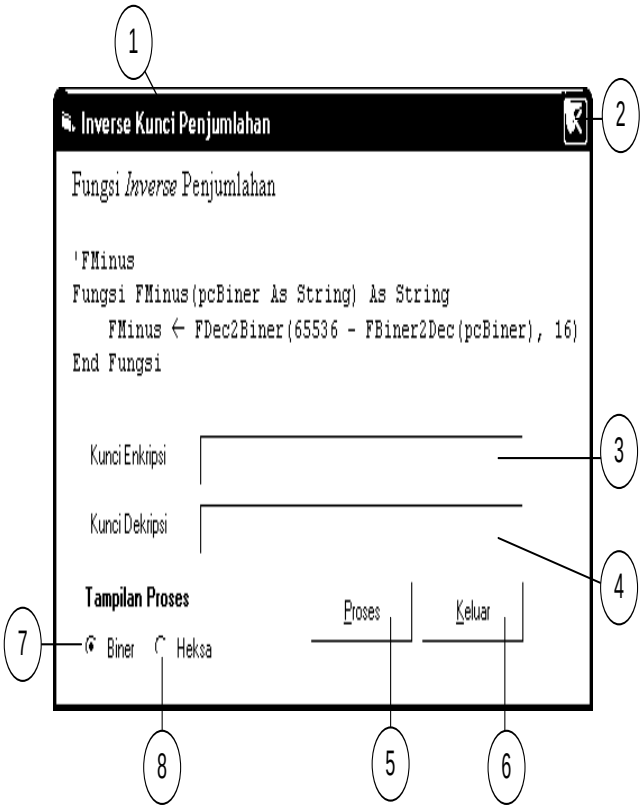
Gambar 3.9 Rancangan Form Teori

Keterangan :

1. *Title bar*, berisi tulisan ‘Teori xxx’.
2. Tombol ‘Close’, berfungsi untuk menutup *form*.
3. Daerah tampilan judul teori.
4. Daerah tampilan teori.

5. Tombol '< Kembali', berfungsi untuk menampilkan halaman sebelumnya.
6. Tombol 'Lanjut >', berfungsi untuk menampilkan halaman selanjutnya.
7. Tombol 'Keluar', berfungsi untuk keluar dari *form*.

Form Proses Inverse Penjumlahan

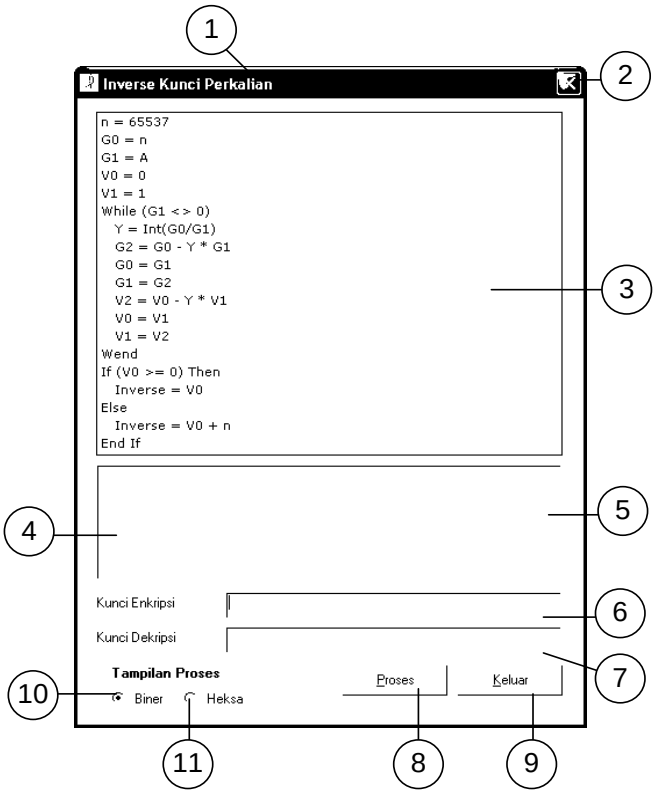


Gambar 3.10 Rancangan Form Proses Inverse Penjumlahan

Keterangan :

1. *title bar*, berisi tulisan 'Inverse Kunci Penjumlahan'.
2. tombol 'Close', berfungsi untuk menutup *form*.
3. daerah penginputan kunci enkripsi.
4. daerah tampilan kunci dekripsi yang dihasilkan.
5. tombol 'Proses', berfungsi untuk memulai proses.
6. tombol 'Keluar', berfungsi untuk keluar dari *form*.
7. *option button* 'Biner', berfungsi untuk menampilkan hasil proses dalam biner.
8. *option button* 'Heksa', berfungsi untuk menampilkan hasil proses dalamheksadesimal.

3.3.2. Form Proses Inverse Perkalian



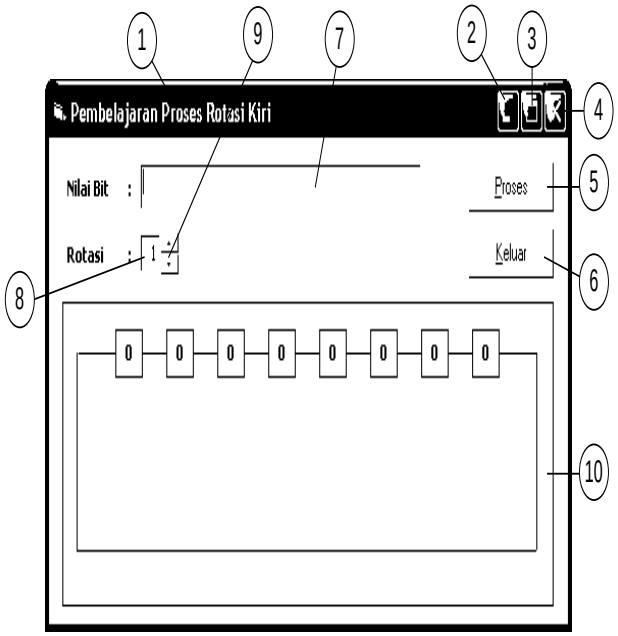
Gambar 3.11 Rancangan Form Proses Inverse Perkalian

Keterangan :

1. *Title bar*, berisi tulisan 'Inverse Kunci Perkalian'.
2. Tombol 'Close', berfungsi untuk menutup *form*.
3. Daerah tampilan animasi algoritma.
4. Daerah tampilan hasil eksekusi.
5. *vertical scroll bar*.
6. Daerah penginputan kunci enkripsi.

7. Daerah tampilan kunci dekripsi yang dihasilkan.
8. Tombol 'Proses', berfungsi untuk memulai proses.
9. Tombol 'Keluar', berfungsi untuk keluar dari *form*.
10. *Option button* 'Biner', berfungsi untuk menampilkan hasil proses dalam biner.
11. *Option button* 'Heksa', berfungsi untuk menampilkan hasil proses dalam heksadesimal.

Form Rotasi Kiri



Gambar 3.12 Rancangan Form Proses Inverse Perkalian

Keterangan :

1. *Title bar*, berisi tulisan 'Pembelajaran Proses Rotasi Kiri'.
2. Tombol 'Minimize', berfungsi untuk me-*minimize form*.
3. Tombol 'Maximize', berfungsi untuk memperbesar *form*.
4. Tombol 'Close', berfungsi untuk menutup *form*.
5. Tombol 'Proses', berfungsi untuk memulai proses.
6. Tombol 'Keluar', berfungsi untuk menutup *form*.
7. *Textbox*'Nilai Bit' berisi nilai dari bit yang akan dan telah dilakukan proses.
8. *Textbox*'Rotasi' berisi jumlah bit yang akan dirotasikan.
9. *Updow* untuk mengontrol isi dari *textbox* (8).
10. Daerah tampilan proses animasi.

ALGORITMA DAN IMPLEMENTASI

Algoritma

Algoritma perancangan perangkat lunak pembelajaran kriptografi metode IDEA dibagi menjadi 3 bagian yaitu :

1. Algoritma Pembentukan Kunci Enkripsi dan Dekripsi.
2. Algoritma Proses Enkripsi.
3. Algoritma Proses Dekripsi.
4. Algoritma Fungsi Pendukung dalam Proses Pembentukan Kunci, Enkripsi dan Dekripsi.

Implementasi Sistem

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

Spesifikasi Perangkat Keras dan Perangkat Lunak

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

1. Prosesor Intel Pentium IV 1,6 Ghz.
2. Memory 128 MB.
3. Harddisk 10 GB.
4. VGA *card* 64 MB.
5. Monitor dengan resolusi 800 × 600 *pixel*.

6. *Keyboard* dan *Mouse*.

Adapun perangkat lunak (*software*) yang digunakan untuk menjalankan aplikasi ini adalah lingkungan sistem operasi MS-Windows 98 atau MS-Windows NT/2000/XP.

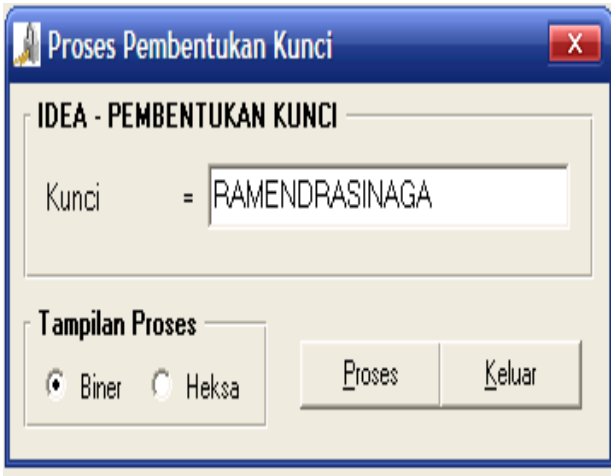
Cara Menggunakan Perangkat Lunak

Perangkat lunak pembelajaran metode kriptografi IDEA dapat dijalankan dengan cara sebagai berikut :

1. Untuk melakukan proses pembentukan kunci, lakukan langkah-langkah berikut ini :
   a. Klik menu 'Proses', pilih sub menu 'Pembentukan Kunci' seperti terlihat pada gambar berikut ini :

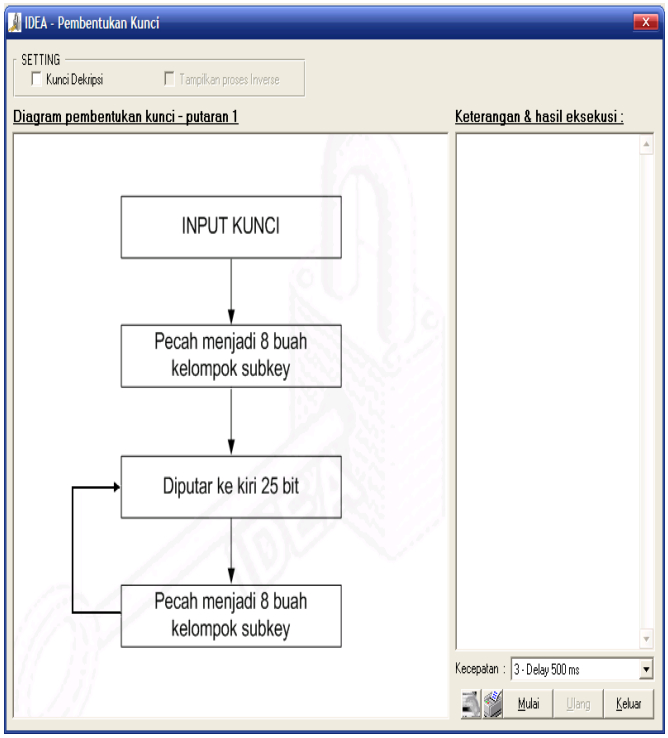
Gambar 4.1 Langkah-1 untuk proses pembentukan kunci

   b. Setelah itu, akan muncul *form* 'Input Data untuk Proses Pembentukan Kunci'. Ketikkan kunci yang diinginkan pada *textbox* 'Kunci'.



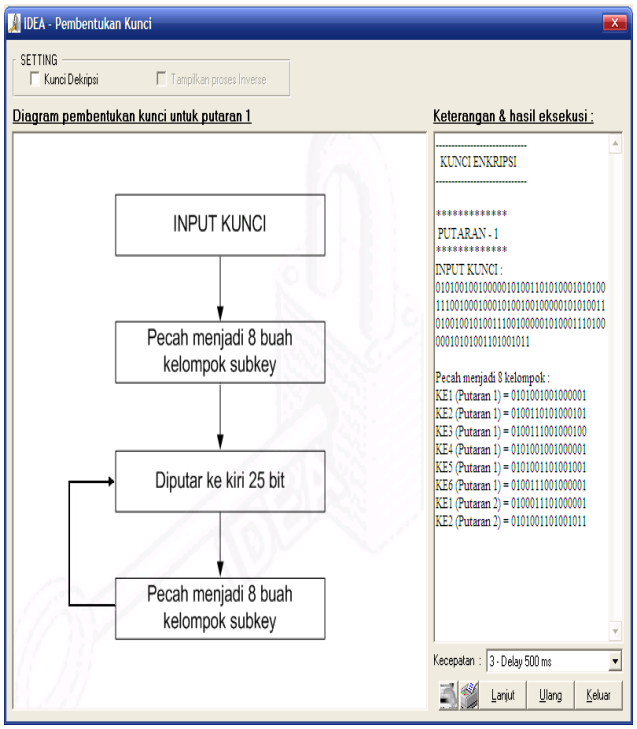
Gambar 4.2 Langkah-2 untuk proses pembentukan kunci

   c. Pilihlah bentuk tampilan hasil yang diinginkan. Setelah itu, klik tombol 'Proses', maka akan ditampilkan *form* 'Proses Pembentukan Kunci' berikut ini:



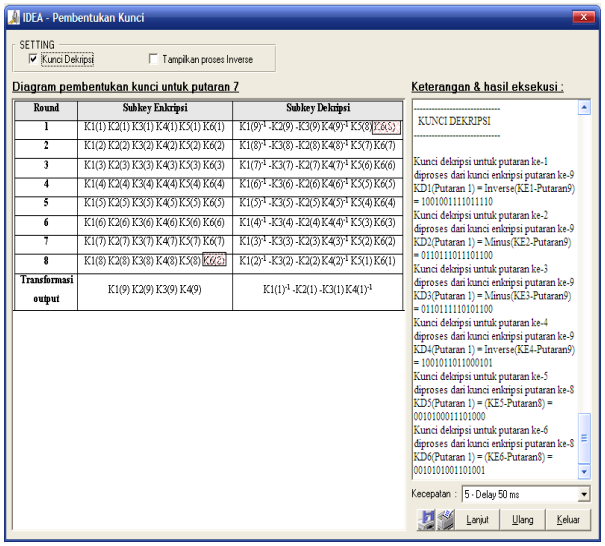
Gambar 4.3 Langkah-3 untuk proses pembentukan kunci

d. Jika ingin menampilkan kunci dekripsi, maka pilihlah *checkbox* 'Kunci Dekripsi'. Jika ingin menampilkan proses *inverse*-nya maka pilihlah *checkbox* 'Tampilkan proses Inverse'. Kliklah tombol 'Mulai' untuk memulai proses pembentukan kunci. Hasil proses ditunjukkan oleh gambar berikut :



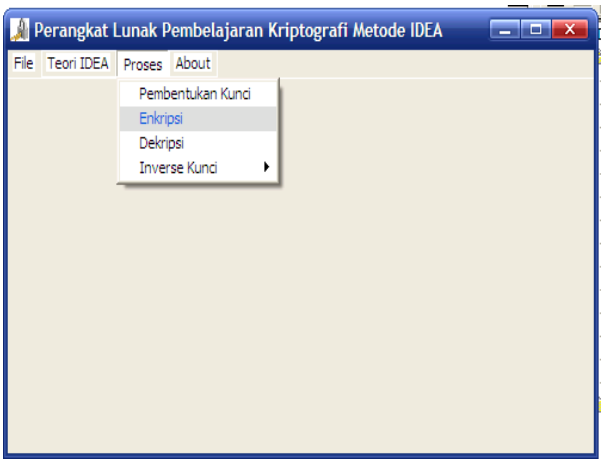
Gambar 4.4 Langkah-4 untuk proses pembentukan kunci

e. Jika ingin melanjutkan ke proses untuk putaran selanjutnya kliklah tombol 'Lanjut', maka proses akan dilanjutkan. Jika proses telah selesai, maka tombol 'Lanjut' tidak dapat diakses.



Gambar 4.5 Langkah-5 untuk proses pembentukan kunci

2. Untuk melakukan proses enkripsi, lakukan langkah-langkah berikut ini :
   a. Klik menu 'Proses', pilih sub menu 'Enkripsi' seperti terlihat pada gambar berikut ini :

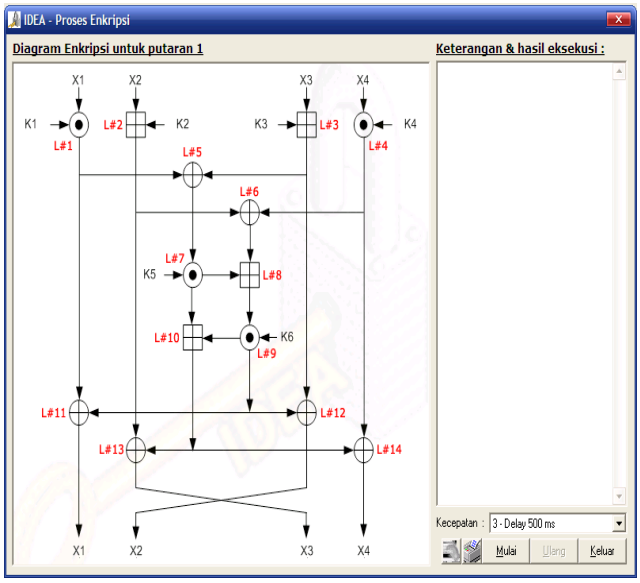


Gambar 4.6 Langkah-1 untuk proses enkripsi

b. Setelah itu, akan muncul *form* 'Input Data untuk Proses Enkripsi'. Ketikkan *plaintext* yang diinginkan pada *textbox* '*Plaintext*' dan kunci pada *textbox* 'Kunci Enkripsi'.

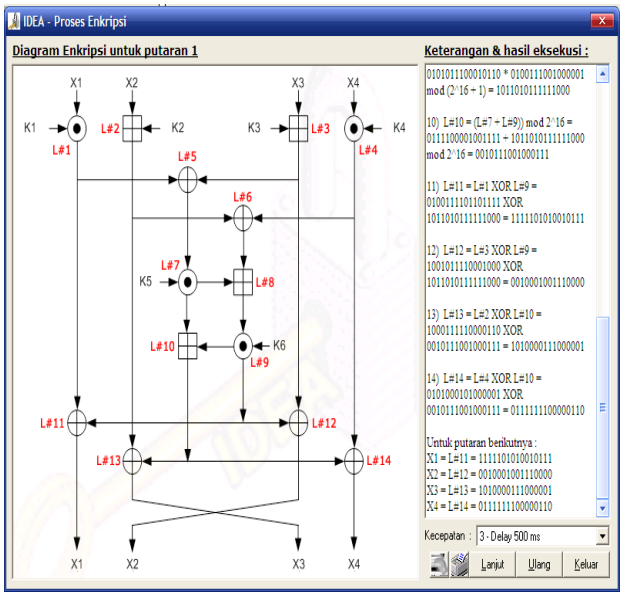
Gambar 4.7 Langkah-2 untuk proses enkripsi

c. Pilihlah bentuk tampilan hasil yang diinginkan. Setelah itu, klik tombol 'Proses', maka akan ditampilkan *form* 'Proses Enkripsi' berikut ini :



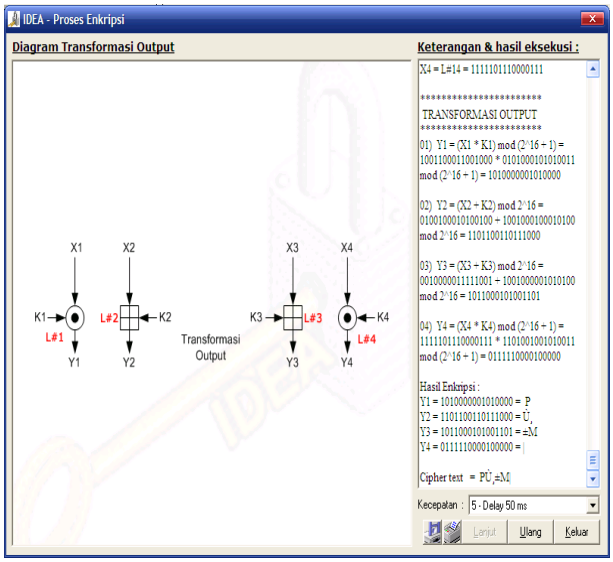
Gambar 4.8 Langkah-3 untuk proses enkripsi

d. Kliklah tombol 'Mulai' untuk memulai proses enkripsi. Hasil proses ditunjukkan oleh gambar berikut :



Gambar 4.9 Langkah-4 untuk proses Enkripsi

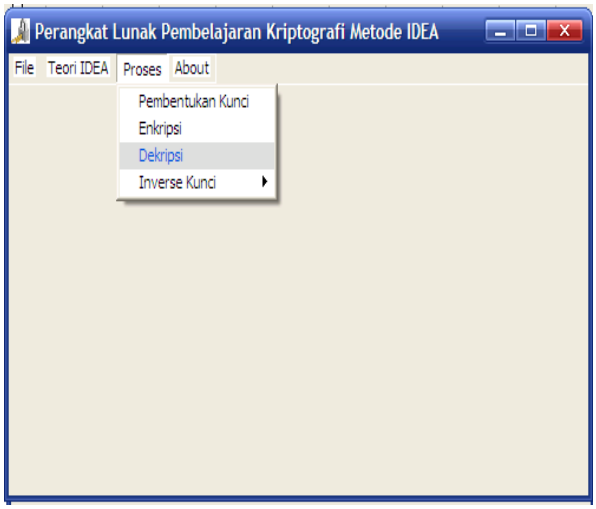
e. Jika ingin melanjutkan ke proses untuk putaran selanjutnya kliklah tombol 'Lanjut', maka proses akan dilanjutkan. Jika proses telah selesai, maka tombol 'Lanjut' tidak dapat diakses.



Gambar 4.10 Langkah-5 untuk proses enkripsi

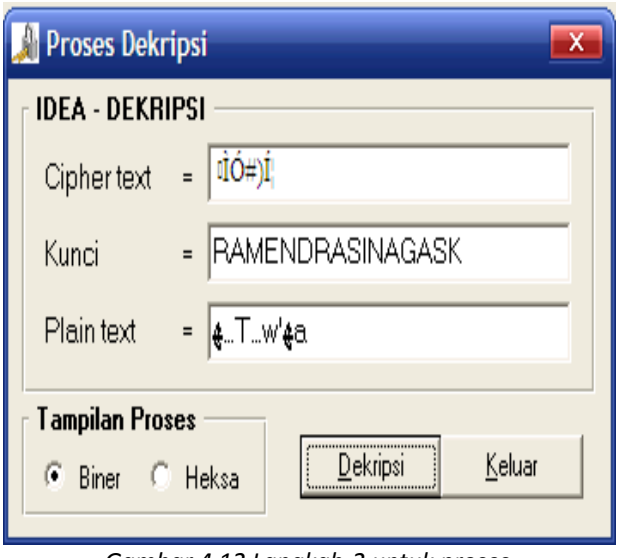
3. Untuk melakukan proses dekripsi, lakukan langkah-langkah berikut ini :

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



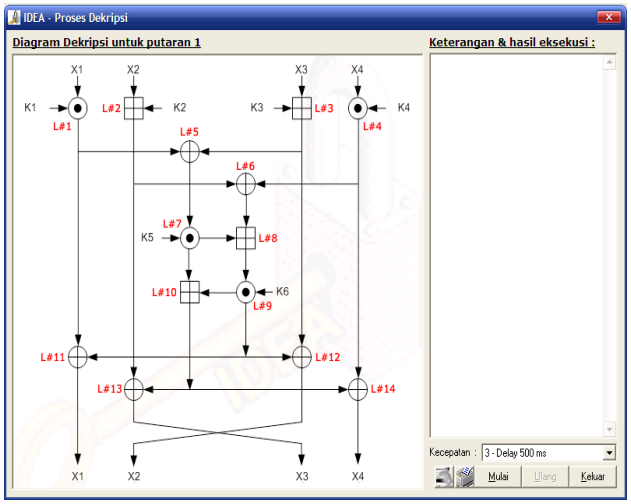
Gambar 4.11 Langkah-1 untuk proses Dekripsi

b. Setelah itu, akan muncul *form* ‘Input Data untuk Proses Dekripsi’. Ketikkan *plaintext* yang diinginkan pada *textbox* ‘*Ciphertext*’ dan kunci pada *textbox* ‘Kunci Dekripsi’.



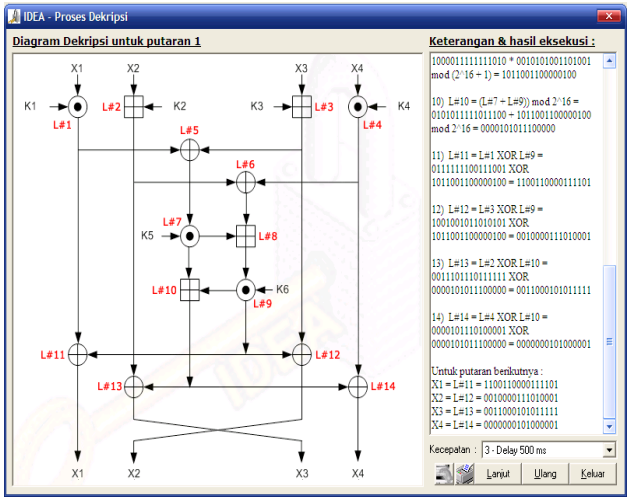
Gambar 4.12 Langkah-2 untuk proses dekripsi

c. Pilihlah bentuk tampilan hasil yang diinginkan. Setelah itu, klik tombol ‘Proses’, maka akan ditampilkan *form* ‘Proses Dekripsi’ berikut ini :



Gambar 4.13 Langkah-3 untuk proses dekripsi

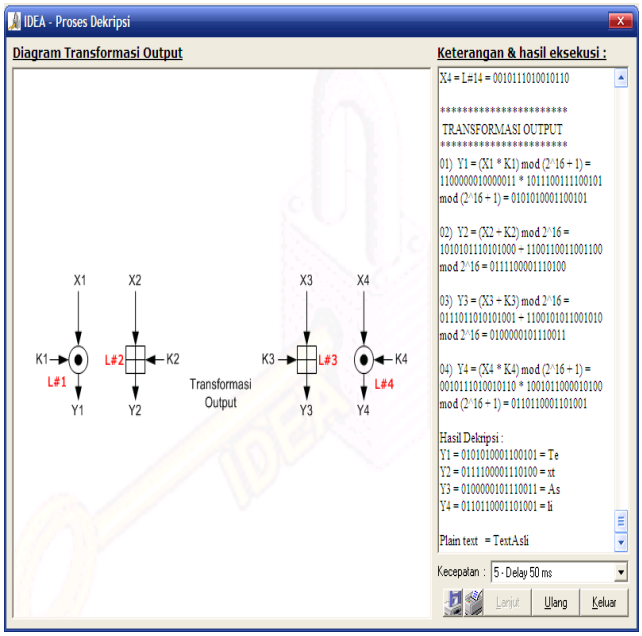
d. Kliklah tombol ‘Mulai’ untuk memulai proses dekripsi. Hasil proses ditunjukkan oleh gambar berikut :



Gambar 4.14 Langkah-4 untuk proses dekripsi

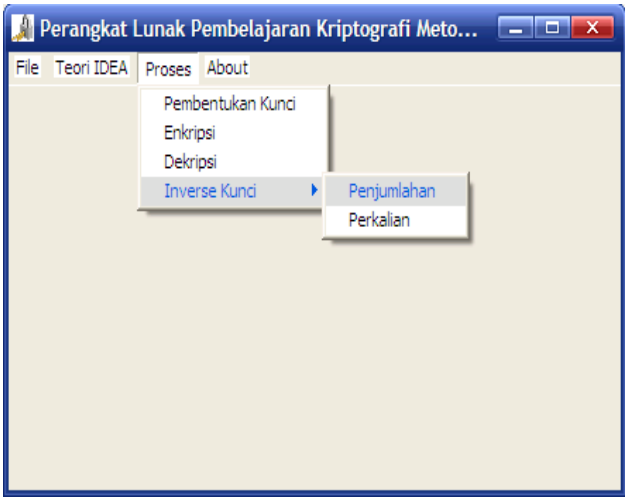
e. Jika ingin melanjutkan ke proses untuk putaran selanjutnya kliklah tombol

'Lanjut', maka proses akan dilanjutkan. Jika proses telah selesai, maka tombol 'Lanjut' tidak dapat diakses.



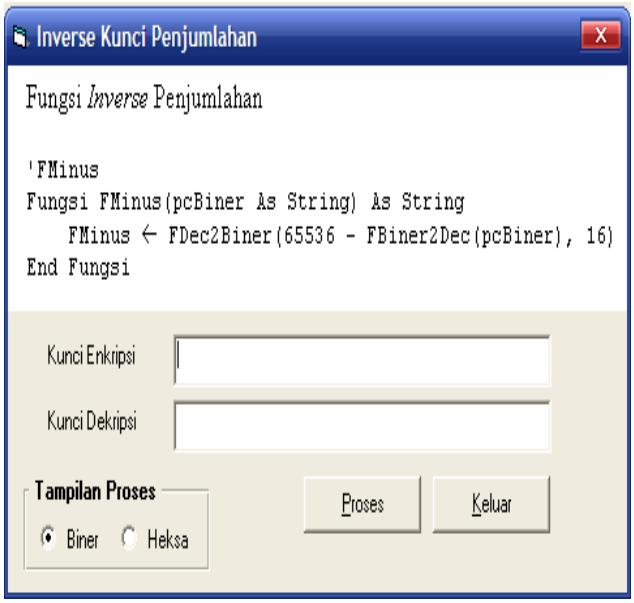
Gambar 4.15 Langkah-5 untuk proses dekripsi

4. Untuk melakukan proses *inverse* kunci penjumlahan, lakukan langkah-langkah berikut ini :
   a. Klik menu 'Proses', pilih sub menu 'Inverse Kunci' >> 'Penjumlahan' seperti terlihat pada gambar berikut ini :



Gambar 4.16 Langkah-1 untuk proses inverse kunci penjumlahan

   b. Setelah itu, akan muncul *form* 'Inverse Kunci Penjumlahan' seperti terlihat pada gambar berikut ini :

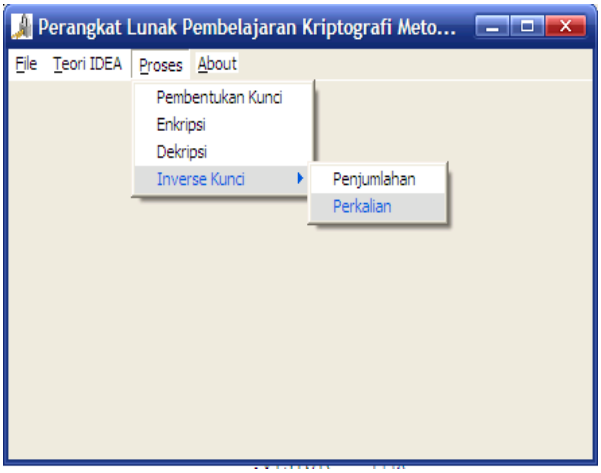


Gambar 4.17 Langkah-2 untuk proses inverse kunci penjumlahan

   c. Pilihlah bentuk tampilan output yang diinginkan. Klik tombol 'Proses' untuk memulai proses *inverse* kunci penjumlahan dan *bit output* akan ditampilkan pada *textbox*.

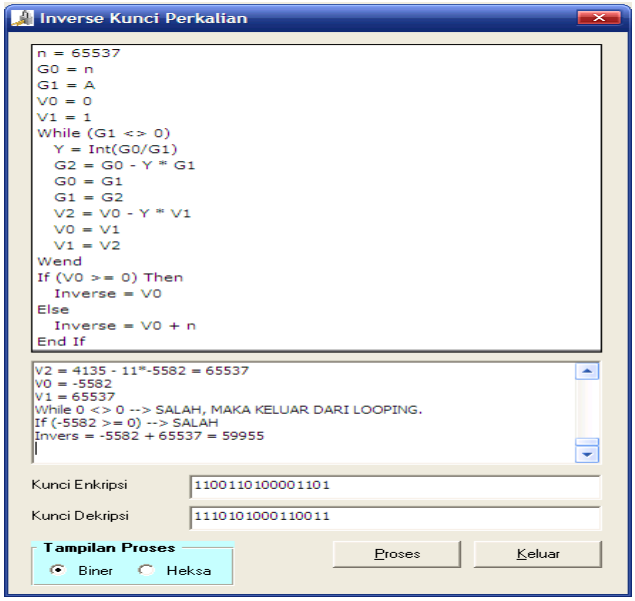
Gambar 4.18 Langkah-3 untuk proses inverse kunci penjumlahan

5. Untuk melakukan proses *inverse* kunci perkalian, lakukan langkah-langkah berikut ini :
   a. Klik menu 'Proses', pilih sub menu 'Inverse Kunci' >> 'Perkalian' seperti terlihat pada gambar berikut ini :



Gambar 4.19 untuk proses inverse kunci Perkalian

   b. Setelah itu, akan muncul *form* 'Inverse Kunci Perkalian', terlihat pada gambar



Gambar 4.20 Langkah-2 untuk proses inverse kunci perkalian

SIMPULAN

Untuk menjaga Keamanan dan kerahasiaan data dalam suatu jaringan komputer, maka diperlukan beberapa jenis enkripsi guna membuat data agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak. Enkrpsi merupakan salah satu metode untuk menjamin agar komonikasi menggunakan jaringan komputer menjadi lebih aman.

Dalam melakukan langkah-langkah enkripsi banyak cara atau algoritma yang tersedia, algoritma IDEA yang dibahas pada penelitian ini hanyalah salah satu dari sekian banyak algoritma yang berkembang saat ini. Dan algoritma IDEA ini sampai sekarang masih cukup handal untk diterapkan sebagai metode pengamanan data. Pengamanan data tersebut selain bertujuan meningkatkan keamanan data, juga berfungsi untuk :

1. Melindungi data agar tidak dapat dibaca oleh orang-orang yang tidak berhak
2. Mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus data

Dari uraian diatas tentang algoritma IDEA dapat diambil kesimpulan bahwa algoritma tersebut mempunyai keuntungan diantaranya sebagai berikut :

1. Algoritma ini menyediakan keamanan yang cukup tinggi yang tidak didasarka atas kerahasiaan algoritmanya akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan
2. Dapat dengan mudah untuk dipahami secara penuh
3. Algoritma ini dapat digunakan dan dimengerti oleh semua orang
4. Algoritma ini sangat layak untuk digunakan sebagai keamanan dalam bidang aplikasi

5. Algoritma ini memungkinkan untuk disebarluaskan keseluruh dunia.

DAFTAR PUSTAKA

Al Bahr, Brian. 2007. *International Data Encryption Algorithm.pdf*. http://www.answers.com/topic/cryptography1?cat=bizfin. Diakses: 7 Februari 2008.

A. Menezes, P. Van Oorschot, and S. Vanstone. 1996. *Handbook of Applied Cryptography*. USA : CRC Press, Inc.

Aryus, Doni. 2005. *Computer Security*. Yogyakarta : Andi Offset.

Jethefer, Stevens. 2006. *Studi dan Perbandingan Algoritma IDEA (International Data Encryption Algorithm) Dengan DES (Data Encryption Standard.pdf)*. Diakses: 8 Februari 2008.

Joan Daemen, Rene Govaerts, dan Joos Vandewalle. 1993. Weaks Keys for IDEA.*http://www.cosic.esat.kuleuven.ac.be/publications/article-140.pdf.* Diakses: 10 Februari 2008.

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

Kurniawan, Yusuf. 2004. *Kriptografi, Keamanan Internet dan Jaringan Telekomunikasi*. Bandung : Informatika.

MediaCrypt. Benefits of IDEA. *http://www.mediacrypt.com*.

Munir, Rinaldi. 2006. BahanKuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

Oppliger, Rolf. 2005. *Contemporary Cryptography.* Norwood : Artech House, Inc.

Pressman, Roger S. 2002. *Rekayasa PerangkatLunak: Pendekatan Praktisi*. Yogyakarta : Andi Offset.

Rahayu, Flourensia Sapty. 2005. *Suplemen Bahan Ajar Mata Kuliah Proteksi dan Teknik Keamanan Sistem Informasi – IKI 83408T*. Magister Teknologi Informasi. Universitas Indonesia.

Scheiner, Bruce. 1996. Applied Cryptography 2nd. John Wiley & Sons.

Sommerville, Ian. 2001. *Software Enginerring Rekayasa Perangkat Lunak Jilid 1*. Jakarta : Erlangga.

Viqarunnisa, Pocut. 2005. *Studi dan Analisis Perbandingan Keamanan PGP Algoritma IDEA-RSA dengan PGP Algoritma Cast-DH*. Tugas Makalah Program Studi Teknik Informatika. Institut Teknologi Bandung.