

DAFTAR PUSTAKA

Suryokusumo A, (2001), *Microsoft Visual Basic 6.0*, PT. Elex Media Komputindo.

Schneier Bruce, (1996), *Applied Cryptography, Second Edition*, John Willey and Sons Inc.

Pramono Djoko,(2002), *Mudah menguasai Visual Basic 6*, PT. Elex Media Komputindo.

Seberpy Jennifer, Pieprzyk Jojef, *Cryptography : An Introduction to Computer Security*.

Jusuf Kurniawan,(2004), *Keamanan Internet dan Jaringan Komunikasi*, Informatika Bandung.

<http://www.encryption-security.com/directory/international-data-encryption-algorithm>.

<http://www.pasta.cs.uit.no/thesis/html/ronnya/node16.html>.

http://www.cs.nps.navy.mil/curricula/tracks/security/notes/chap04_43.htm

<http://www.unix.ecs.umass.edu/~ccowell/projects/VLSI%20Projects/IDEA%20overview.html>

LAMPIRAN

File Abstraksi.txt

Dalam sebuah masalah kerahasiaan 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).

File Abstraksi-cip.txt

[illegible]

File Abstraksi-pl.txt

Dalam sebuah masalah kerahasiaan 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).

File Bab 1.txt

BAB I

PENDAHULUAN

1.1 Latar Belakang Pemilihan Judul

Dalam sebuah masalah kerahasiaan 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 perubahan 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 216 (addition modulo 216). 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”.

1.2 Perumusan Masalah

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).

1.3 Tujuan dan Manfaat

Tujuan penyusunan tugas akhir (skripsi) ini adalah untuk merancang suatu perangkat lunak pembelajaran untuk membantu pemahaman metoda kriptografi IDEA dan mengembangkan inputan plaintext lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit)..

Manfaat dari penyusunan tugas akhir (skripsi) ini yaitu untuk membantu pembelajaran metoda kriptografi IDEA dan perangkat lunak dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar.

1.4 Pembatasan Masalah

Pembatasan permasalahan dalam merancang perangkat lunak ini adalah :

1. Perangkat lunak akan menampilkan tahap – tahap perhitungan dalam bentuk bilangan biner.
2. Input data berupa bilangan biner, desimal, heksadesimal dan karakter (string).
3. Input data / plainteks dengan jumlah bit 32, 64, dan 128 bit.
4. Perangkat lunak tidak menampilkan tahap – tahap konversi bilangan ke dalam bilangan biner.
5. Perangkat lunak menyediakan teori – teori dasar dari metoda IDEA.

1.5 Sistematika Penulisan

Sistematika penulisan dari skripsi ini terdiri dari beberapa bagian utama sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang pemilihan judul skripsi “Pengamanan Data dengan Metoda Kriptografi IDEA”, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini akan membahas mengenai tinjauan pustaka yang berkaitan dengan definisi kriptografi, sejarah kriptografi, jenis kriptografi, operasi matematika yang berhubungan dengan kriptografi, Enkripsi dan Dekripsi pada Algoritma IDEA.

BAB 3 METODOLOGI PENELITIAN

Bab ini membahas mengenai pendefinisian lingkup sistem dan pemodelan pada pengamanan data menggunakan metode IDEA.

BAB 4 ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan memuat kesimpulan isi dari keseluruhan uraian bab-bab sebelumnya dan saran-saran dari hasil yang diperoleh yang diharapkan dapat bermanfaat untuk pengembangan selanjutnya.

Tujuan penyusunan tugas akhir (skripsi) ini adalah untuk merancang suatu perangkat lunak pembelajaran untuk membantu pemahaman metoda kriptografi IDEA dan mengembangkan inputan plaintext lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit)..

Manfaat dari penyusunan tugas akhir (skripsi) ini yaitu untuk membantu pembelajaran metoda kriptografi IDEA dan perangkat lunak dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar.

1.4 Pembatasan Masalah

Pembatasan permasalahan dalam merancang perangkat lunak ini adalah :

1. Perangkat lunak akan menampilkan tahap – tahap perhitungan dalam bentuk bilangan biner.
2. Input data berupa bilangan biner, desimal, heksadesimal dan karakter (string).
3. Input data / plainteks dengan jumlah bit 32, 64, dan 128 bit.
4. Perangkat lunak tidak menampilkan tahap – tahap konversi bilangan ke dalam bilangan biner.
5. Perangkat lunak menyediakan teori – teori dasar dari metoda IDEA.

1.5 Sistematika Penulisan

Sistematika penulisan dari skripsi ini terdiri dari beberapa bagian utama sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang pemilihan judul skripsi “Pengamanan Data dengan Metoda Kriptografi IDEA”, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini akan membahas mengenai tinjauan pustaka yang berkaitan dengan definisi kriptografi, sejarah kriptografi, jenis kriptografi, operasi matematika yang berhubungan dengan kriptografi, Enkripsi dan Dekripsi pada Algoritma IDEA.

BAB 3 METODOLOGI PENELITIAN

Bab ini membahas mengenai pendefinisian lingkup sistem dan pemodelan pada pengamanan data menggunakan metode IDEA.

BAB 4 ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi implementasi dari Pengamanan Data dengan Metoda Kriptografi IDEA dan pengujian sistem secara manual.

BAB 5 KESIMPULAN dan SARAN

Bab ini akan memuat kesimpulan isi dari keseluruhan uraian bab-bab sebelumnya dan saran-saran dari hasil yang diperoleh yang diharapkan dapat bermanfaat untuk pengembangan selanjutnya.

File Bab 5.txt

BAB V

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Setelah melalui proses penyelesaian tugas akhir (skripsi) yang berjudul ‘Pengamanan Data Dengan Metoda Kriptografi IDEA’, penulis menarik kesimpulan sebagai berikut :

1. Dalam proses pengujian untuk kunci yang sama antara proses enkripsi dan dekripsi perangkat lunak berjalan sesuai harapan, akan tetapi jika kunci berbeda antara proses enkripsi dan dekripsi maka plaintext tidak sama antara proses dekripsi dengan masukan awal pada proses enkripsi.
2. Perangkat lunak pembelajaran ini menyediakan fasilitas pengaturan kecepatan visualisasi proses.
3. Perangkat lunak pembelajaran ini dapat menampilkan langkah-langkah penyelesaian algoritma untuk proses pembentukan kunci, enkripsi dan dekripsi secara tahap demi tahap sehingga mempermudah pemahaman.
4. Perangkat lunak pembelajaran ini menyediakan teori-teori dasar mengenai metode IDEA.

5.2 SARAN

Penulis ingin memberikan beberapa saran yang mungkin berguna untuk pengembangan lebih lanjut pada perancangan perangkat lunak pembelajaran kriptografi dengan metode IDEA yaitu :

1. Perangkat lunak dapat dikembangkan agar dapat digabungkan dengan pembelajaran untuk metode kriptografi yang lain.

Akhir Disusun Untuk Melengkapi dan Memenuhi Syarat Kelulusan Program Strata 1 Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember dan juga sebagai syarat untuk memperoleh Gelar Sarjana Komputer (S.Kom).

Ucapan terima kasih penulis sampaikan kepada pihak-pihak yang telah membantu penulis, baik selama pembuatan aplikasi maupun selama penyusunan

Laporan Tugas Akhir, di antaranya :

1. Bapak Daryanto dan Bapak Lutfi dosen pembimbing,
 2. Para Dosen Fakultas Teknik Informatika, terima kasih atas semua ilmu yang telah diberikan,
 3. Teman-teman yang telah mendukung dan memberi semangat kepada penulis, khususnya Pak Edy, Mas Faiz, dan Mas Afiadi,
 4. Keluarga penulis dan La'aliy Afida yang telah memberikan do'a dan juga bantuan secara moril dan materil,
 5. Serta pihak-pihak yang telah membantu dan tidak dapat penulis sebutkansatu persatu.
- Penulis menyadari bahwa masih banyak kekurangan dan kelemahan dalam penyusunan Laporan Skripsi ini. Oleh karena itu, kami mengharapkan kritik dan saran yang membangun dan menambah wawasan dan wacana ilmu kami. Besar harapan kami laporan ini dapat bermanfaat bagi semua pihak dan dapat dimanfaatkan sebaik-baiknya.

Jember,

Penulis

BIODATA PENULIS



Penulis, Aditya Pratama, lahir di Blitar pada tanggal 27 April 1987 dan merupakan putra pertama dari tiga bersaudara. Lulus Sekolah Dasar tahun 1999, Sekolah Menengah Pertama (SMP) tahun 2002, Sekolah Menengah Kejuruan (SMK) tahun 2005. Sarjana Ahli Madya (A.Md) Jurusan Teknik Listrik Program Studi Komputer tahun 2009. Pernah bekerja sebagai teknisi ahli di sebuah badan usaha yang bergerak dibidang komputerisasi di Kab. Malang pada tahun 2006 sampai tahun 2009. Saat ini pekerjaan penulis adalah mengajar mata pelajaran Teknik Informasi dan Komunikasi (TIK) di lingkungan SMP Negeri 1 Jember mulai tahun 2009.

Terima Kasih