ENKRIPSI DATA KEUANGAN DENGAN MENGGUNAKAN METODE DIFFIE HELLMAN

M.Irwan Ukkas [1)], Asep Nurhuda [2)], Gerry Avianto Kurdi[3)]

[1]Teknik Informatika, STMIK Widya Cipta Dharma
[2]Teknik Informatika, STMIK Widya Cipta Dharma
[3]Teknik Informatika, STMIK Widya Cipta Dharma
[1,2,3]Jl. M. Yamin No.25, Samarinda, 75123
E-mail : Irwan212@yahoo.com [1)], [2)], gerryavianto@gmail.com[3)]

ABSTRAK

Penerapan Metode *Diffie Hellman* pada Enkripsi Data Keuangan dengan Menggunakan Metode *Diffie Hellman*, merupakan bentuk penelitian untuk membuktikan bahwa algoritma *Diffie Hellman* dapat digunakan untuk pencarian solusi, khususnya pada permasalahan kerahasian data .

Tujuan dari penelitian ini adalah merancang dan membangun sebuah aplikasi yang dapat menyelesaikan masalah eknripsi data untuk merahasiakan sebuah data dengan mengacak nilai dari *Byte* yang terdapat pada data dengan menggunakan bahasa pemrograman *Microsoft Visual Studio 2012*. Dalam penelitian ini, teknik pengumpulan data yang digunakan adalah studi pustaka. Metode pengujian yang digunakan adalah dengan pengujian *White-Box.*

Hasil dari penelitian ini adalah dibuatnya aplikasi enkripsi Data yang dapat mengacak *byte* yang terdapat pada data agar terjadi pengacakan *byte* pada data yang dienkripsi. Pengguna dapat menentukan kunci yang digunakan dalam melakukan proses enkripsi dan kemudian proses enkripsi menggunakan metode *Diffie Hellman*. Setelah Proses enkripsi maka data yang telah terenkripsi dapat disimpan.

.

Kata Kunci: *Data, Keuangan, Enkripsi, Diffie Hellman*

1. PENDAHULUAN

Teknologi komputer pada masa ini sangat membantu hampir seluruh kegiatan manusia. Tetapi dengan perkembangan teknologi komputer yang pesat, penyalahgunaan akan pemakaian komputer juga semakin meningkat. Salah satu faktor yang perlu diperhatikan seiring dengan kemajuan teknologi komputer adalah masalah keamanan komputer. Keamanan pada komputer lebih mengarah kepada keamanan data yang tersimpan di dalam komputer tersebut. Salah satu cara untuk mengamankan data komputer adalah melakukan enkripsi pada sebuah data atau file yang kita anggap penting. Teknik enkripsi ini adalah teknik untuk merubah bentuk data, sehingga orang lain tidak mengetahui bentuk asli dari data tersebut.

Untuk melakukan pengiriman data secara manual, sangat memungkinkan diketahui oleh orang lain. Untuk mengirimkan data yang bersifat rahasia, maka diperlukan teknik enkripsi untuk merubah bentuk data tersebut agar tidak mudah dibaca atau dilihat oleh orang lain. Setelah melalui teknik enkripsi, data yang telah dirubah tetap dapat terlihat. Tetapi data yang telah melalui proses enkripsi memiliki bentuk yang telah berubah dari bentuk aslinya.

Data adalah keterangan tertulis mengenai sesuatu fakta yang masih berdiri sendiri-sendiri, belum mempunyai pengertian sebagai kelompok, belum terkoordinasi satu sama lain, dan belum diolah sesuai keperluan tertentu

Dalam penelitian ini teknik enkripsi yang di gunakan untuk mengenkripsi sebuah data adalah dengan metode diffie hellman yang lebih menekankan proses matematika untuk menghasilkan kunci rahasia yang dapat disebarkan secara luas tanpa harus khawatir karena kunci rahasia tersebut hanya dapat di dekripsi hanya oleh pengirim dan penerima

Maka dalam penelitian ini penulis akan melakukan penelitian dalam mengenkripsi data keuangan menggunakan metode diffie hellman Algoritma ini pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1975. Mereka berdua adalah peneliti pada universitas Stanford. Mereka memperkenalkan algoritma ini untuk memberi solusi atas pertukaran informasi secara rahasia.

2. RUANG LINGKUP PENELITIAN

1. Cakupan Permasalahan

Berdasarkan uraian latar belakang masalah diatas, maka dapat diambil rumusan masalah dari penelitian ini adalah, “Bagaimana membuat Aplikasi Enkripsi Data Keuangan dengan menggunakan metode Diffie Hellman ?”

2. Batasan masalah pada penelitian ini Batasan masalah pada penelitian ini adalah :

Implementasi enkripsi tidak untuk gambar, Maksimal karakter kunci yang digunakan adalah 3 karakter, hal ini dilakukan agar proses enkripsi tidak memakan waktu yang terlalu lama, Inputan berupa file Microsoft exel, Menggunkan algoritma Rijndael untuk proses enkripsi File

3. Tujuan penyusunan penelitian ini adalah untuk Menghasilkan "Enkripsi Keuangan dengan Menggunakan metode Diffie Hellman ", sehingga diharapkan mampu menyembunyikan informasi penting dari sebuah data dan mampu menjaga privasi kerahasiaan dari data tersebut.

3. BAHAN DAN METODE

3.1 Algoritma Diffie Hellman

Menurut Ramdan (2010), Algoritma ini pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1975. Mereka berdua adalah peneliti pada universitas Stanford. Mereka memperkenalkan algoritma ini untuk memberi solusi atas pertukaran informasi secara rahasia.

Algoritma ini tidak berdasarkan pada proses *enkripsi* dan *dekripsi*, melainkan lebih kepada proses matematika yang dilakukan untuk menghasilkan kunci rahasia yang dapat disebarkan secara bebas tanpa harus khawatir karena kunci rahasia tersebut hanya dapat *didekripsi* hanya oleh pengirim dan penerima pesan. Dasar dari algoritma ini adalah matematika dasar dari aljabar eksponen dan aritmatika modulus.

Langkah-langkah dalam pertukaran kunci dengan menggunakan algoritma Diffie-Hellman adalah sebagai berikut:

1. Pilih bilangan prima yang besar, ***p*** dan bilangan integer yang tidak melebihi dari nilai ***p***, ***g***, biasa disebut bilangan basis atau generator. Kedua bilangan tersebut dapat diketahui secara publik.
2. Pilih sebuah bilangan acak oleh pengirim, ***x***, bilangan ini tidak boleh diketahui oleh orang lain.
3. Pilih sebuah bilangan acak oleh penerima, ***y***, bilangan ini tidak boleh diketahui oleh orang lain.
4. Pengirim menghitung **A = g^x mod p**. Bilangan A ini dapat diketahui secara publik.
5. Penerima menghitung **B = g^y mod p**. Bilangan B ini dapat diketahui secara publik.
6. Lakukan pertukaran bilangan A dan B terhadap pengirim dan penerima.
7. Lalu Pengirim menghitung **ka = B^x mod p**.
8. Penerima menghitung **kb = A^y mod p**.
9. Berdasarkan hukum aljabar nilai **ka** sama dengan **kb** atau bisa disebut **ka = kb = k.** Sehingga pengirim dan penerima tersebut mengetahui kunci rahasia tersebut “**k”**.

Bukti dari **ka = kb = k** :
ka = **kb**
Bx mod p = Ay mod p
(gy mod p)x mod p = (gx mod p)y mod p
(gy)x mod p = (gx)y mod p
gyx mod p = gxy mod p

Contoh penggunaan dari algoritma ini adalah:

1. Alice dan Bob menetapkan ***p* = 23** dan ***g* = 5**.
2. Eve (penyadap) tahu nilai ***p*** dan ***g***.
3. Alice memilih nilai ***x* = 6** dan Bob memilih nilai ***y* = 15**.
4. Alice menghitung nilai **A = 15625 mod 23 = 8**.
5. Bob menghitung nilai **B = 30517578125 mod 23 = 19**.
6. Alice dan Bob bertukar nilai **A** dan **B**.
7. Eve menyadap mereka dan tahu nilai A dan B.
8. Alice melakukan perhitungan **ka = 47045881 mod 23 = 2**.
9. Bob melakukan perhitungan **kb = 35184372088832 mod 23 = 2**.
10. Eve mengetahui nilai ***p*** , ***g***, **A**, dan **B** tetapi dia tidak dapat mengetahui kunci rahasia, **k** dari Bob dan Alice.

Alice dan Bob dapat mengetahui kunci rahasia tersebut dan dapat bertukar pesan dengan aman tanpa harus diketahui oleh Eve. Eve hanya dapat mengetahui nilai p, g, A, dan B tetapi tidak dapat menghitung kunci rahasia dari mereka berdua. Sehingga Eve tidak dapat mengetahui pesan rahasia apa antara Alice dan Bob.

Algoritma ini tidak hanya terbatas pada 2 pengguna saja. Jumlah pengguna yang ingin menggunakan pertukaran kunci menggunakan algoritma Diffie-Hellman ini tidak dibatasi. Hal ini hanya berlaku jika memenuhi 2 prinsip yang harus dilakukan:

1. Bilangan *p* dan *g* yang telah disetujui oleh semua anggota.
2. Setiap anggota harus melakukan pertukaran data yang diperlukan oleh anggota lainnya sehingga semua data dapat didapatkan secara merata

3.2 Rijndael

Menurut Munir (2006) dalam bukunya “Kriptografi“, Rijndael menggunakan substitusi dan permutasi, dan sejumlah putaran (cipher berulang) setiap putaran menggunakan kunci internal yang berbeda (kunci setiap putaran disebut round key). Joan Daemen & Vincent Rijmen, dalam artikel yang berjudul A Specification for Rijndael, the AES Algorithm,

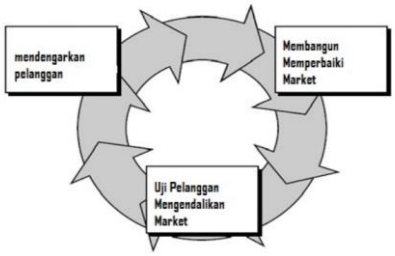
menjelaskan input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext. Chiper keydari AES terdiri dari keydengan panjang 128 bit, 192 bit, atau 256 bit. *pattern* ditemukan.

3.3 Kriptografi

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. (Dony ,2008)

4. Metode Pengembangan Sistem

Dalam pengembangan sistem paradigma yang digunakan adalah prototipe dengan alasan prototipe perlu digunakan untuk pembuatan suatu proyek, karena sering terjadinya seorang pengguna hanya mendefinisikan secara umum apa yang dikehendakinya tanpa menyebutkan secara detail *output* apa saja yang di butuhkan, pemrosesan dan data-data apa saja yang dibutuhkan. Sebaliknya disisi pengembang kurang memperhatikan efesiensi algoritma, kemampuan sistem operasi dan interface yang menghubungkan manusia dengan komputer. Untuk dapat mengatasi ketidakserasian antara pengguna dan pengembang itu, maka harus dibutuhkan suatu prototipe untuk menimbulkan kerjasama yang baik diantara keduanya, sehingga pengembang akan mengetahui dengan benar apa yang diinginkan pengguna dengan tidak mengesampingkan segi-segi teknis dan pengguna akan mengetahui proses-proses dalam menyelesaikan sistem yang diinginkan.



Gambar 1. *Prototype*

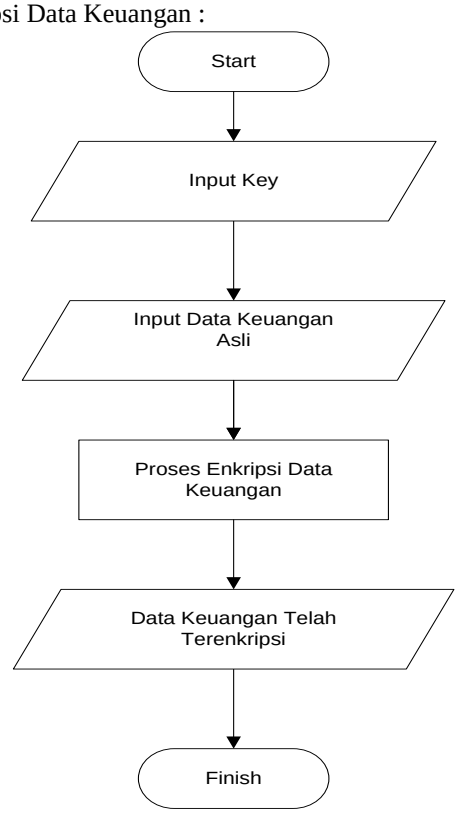
5. IMPLEMENTASI

5.1 Implementasi Rancangan Sistem

Desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemrograman Visual Basic.Net 2012 dan menggunakan Aplikasi Visual Basic.Net 2012. Program yang dibangun langsung diuji secara unit, apakah sudah bekerja dengan baik. Adapun bagian-bagian yang dibangun dalam aplikasi ini adalah Tampilan *Form.*

5.1.1 Tahapan Penerapan Enkripsi Data Keuangan Metode *Diffie-Hellman*

Di bawah ini adalah tahapan flowchart penerapan enkripsi Data Keuangan :

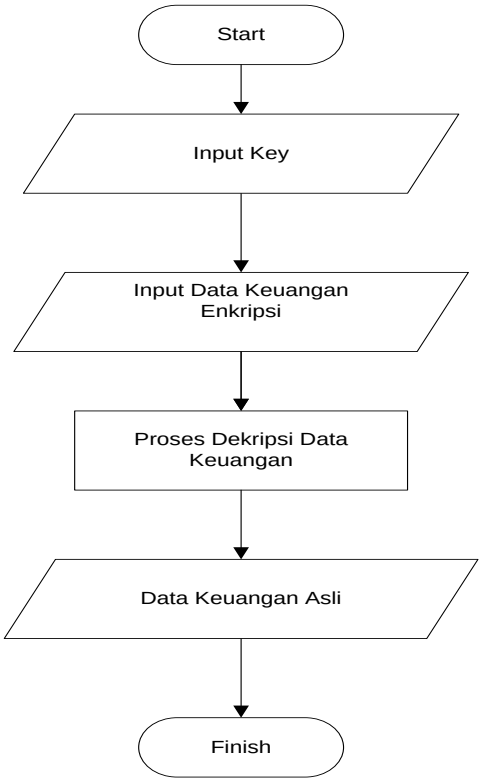


Gambar 2 Tahapan Penerapan Enkripsi Data Keuangan

Flowchart proses enkripsi merupakan suatu rancangan sistem yang digunakan untuk memperlihatkan alur dari kinerja sistem untuk melakukan proses enkripsi pada aplikasi enkripsi.

5.1.2 Tahapan Penerapan Dekripsi Data Keuangan Metode *Diffie-Hellman*

Di bawah ini adalah tahapan flowchart penerapan dekripsi Data Keuangan :

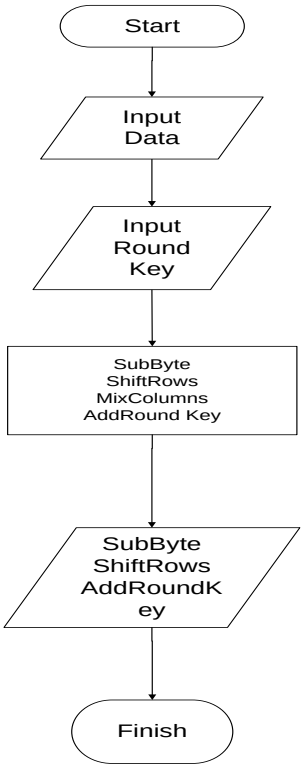


Gambar 3 Tahapan Penerapan Dekripsi Data Keuangan Asli

Flowchart proses dekripsi merupakan suatu rancangan sistem yang digunakan untuk memperlihatkan alur dari kinerja sistem untuk melakukan proses dekripsi pada aplikasi enkripsi.

5.1.3 Tahapan Penerapan Algoritma Enkripsi Data Keuangan Rijndael

Pada gambar di bawah ini adalah *flowchart* desain algoritma enkripsi data keuangan :

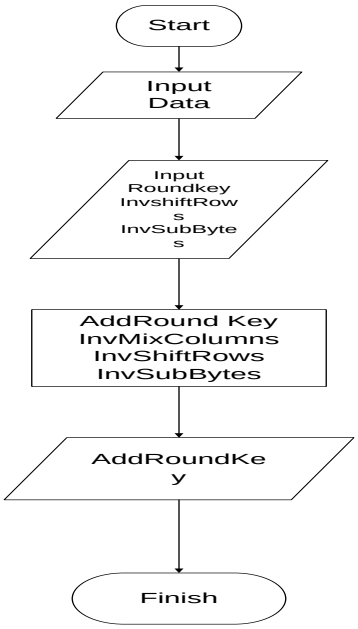


Gambar 4 Desain Algoritma Enkripsi Data Keuangan Rijndael

Flowchart proses enkripsi rijndael merupakan suatu rancangan sistem yang digunakan untuk memperlihatkan alur dari kinerja sistem untuk melakukan proses enkripsi pada aplikasi enkripsi alogritma rijndael.

5.1.4 Tahapan Penerapan Algoritma Enkripsi Data Keuangan Rijndael

Pada gambar di bawah ini adalah *flowchart* desain algoritma enkripsi data keuangan :



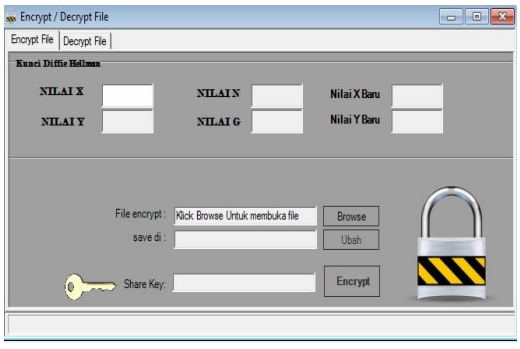
Gambar 5 Desain Algoritma Enkripsi Data Keuangan Rijndael

Flowchart proses dekripsi rijndael merupakan suatu rancangan sistem yang digunakan untuk memperlihatkan alur dari kinerja sistem untuk melakukan proses dekripsi pada aplikasi enkripsi alogritma rijndael.

5.2 Implementasi Program

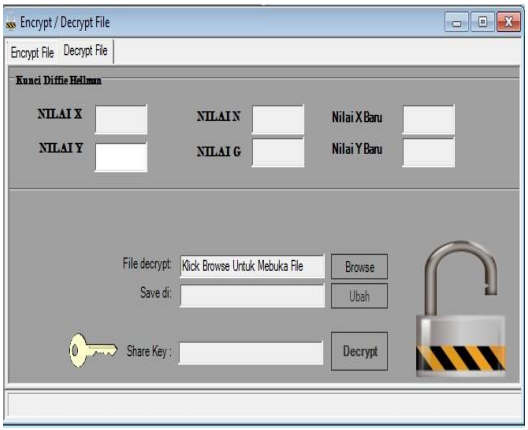
Kamus istilah kesehatan yang telah dirancang merupakan aplikasi berbasis *dekstop* yang dapat digunakan secara *offline* dengan menerapkan algoritma *brute force* dalam proses pencariannya. Berikut tampilan dari aplikasi kamus istilah kesehatan.

5.2.1 *Form* Enkripsi



Gambar 6 *Form* Enkripsi

5.2.2 *Form* Dekripsi



Gambar 7 *Form* Dekripsi

6. KESIMPULAN

Dengan adanya hasil penelitian yang dilakukan dan berdasarkan uraian uraian yang dibahas dalam bab-bab sebelumnya, maka dapat ditarik kesimpulan bahwa :

1. Metode Dieffie Hellman yang diaplikasikan pada aplikasi ini dapat berfungsi dengan baik untuk enkripsi dan dekripsi.
2. Waktu yang digunakan untuk melakukan proses enkripsi tergantung dari besar file yang di gunakan.

7. SARAN

Adapun saran-saran yang dapat dikemukakan yaitu sebagai berikut :

1. Dalam Pemrosesan Enkripsi dan Dekripsi kunci yang digunakan harus lebih variatif lagi maka lebih baik lagi untuk kunci di enkripsikan menggunakan metode yang berbeda.
2. Aplikasi dapat di kembangkan ke system operasi *mobile* seperti android , windows phone dan ios.
3. Kunci yang digunakan dalam implementasi masih tergolong lemah karena pendeknya jumlah karakter, maka diharapkan untuk penelitian yang lebih lanjut ada metode pembangkitan karakter.

8. DAFTAR PUSTAKA

Ariyus Dony. 2008. *Pengantar Ilmu Kriptografi*. Penerbit : ANDI. Yogyakarta.

Adriansyah Yudha 2011, *Perancangan Aplikasi Kriptografi Enkripsi dan Dekripsi Data Menggunkan Algoritma Skipjack*, Universitas Mercu Buana

Arif 2008. *Kriptografi visual pada biner dan citra berwarna serta pengembangannya dengan setenografi*

Harahap , Sofyan Syafri. 2006. *Analisis Kritis Atas Laporan Keuangan, Edisi Satu*, PT Raja Grafindo Persada, Jakarta

Jogiyanto. 2007. *Analisis dan Desain Sistem Informasi*. Yogyakarta: Penerbit Andi.

Kristanto, Andri 2007, *Perancangan sistem informasi dan aplikasinya* ,Yogyakarta:Gava Media, 2007

Megawati Sri 2010, *Algoritma Hill Cipher untuk Enkripsi Data Text yang di Gunakan untuk Steganografi Gambar dengan Metode Lsb, Universitas Sumatera Utara*

Mulyanto , Agus. 2009. *Sistem Informasi Konsep dan Aplikasi*. Pustaka Pelajar.

Munir, Rinaldi 2006, *Kriptografi*, Informatika, Bandung

Nugroho Adi. *Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP*. Yogyakarta: Andi, 2010

Prayudi, Yudi, Idham Halik. 2005. *Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data*. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.

Pressman, R.S. (2005). *Software Engineering: A Practiotioner's Approach, Forth Edition, McGraw-Hill Book*, Co.

Romdhoni M. Arif. 2008, *Kriptografi visual pada biner dan citra berwarna serta pengembangannya dengan steganografi dan fungsi XOR. Sekolah Teknik Elektro dan informatika, ITS. Surabaya.*

Simarmata. Janner (2010), *Rekayasa Perangkat Lunak*, Andi Offset, Yogyakarta.

Tjiharjadi Samuji. 2009, *Pengaman data menggunakan metode enkripsi Einstein. Sistem Komputer, Fakultas Teknik, Universitas Kristen Maranatha. Bandung.*

Wahana kompuer 2013, shourtcourse : *visual basic 2012 programing*

Widya. Kadir, Abdul. 2009. *Dasar Perancangan dan Implementasi Database Relasional. Yogyakarta : Andi Offset.*

.