ISBN: 978-623-7297-02-4

RANCANG BANGUN APLIKASI PENYANDIAN DATA TEXT MENGGUNAKAN ALGORITMA DIFFIE-HELLMAN DAN ALGORITMA RC4

Hermansyah ALam[1)], Helma widya[2)], Syafrawali[3)], Kharisma Maulana Pasaribu[4)]
[1)] Dosen Teknik Informatika, [2)] Dosen Teknik Informatika
[3)] Dosen Teknik Pertambangan, [4)] Alumni Teknik Informatika

Abstrak

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak berhak. Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyandikan isi informasi (plaintext) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli, dilakukan proses , disertai dengan menggunakan kunci yang benar. Algoritma Diffie-Hellman adalah suatu algoritma pembangkit kunci untuk menghasilkan sebuah kunci privasi yang digunakan dalam proses enkripsi dan de data text. Algoritma RC4 adalah salah satu jenis stream cipher yang sinkron yaitu cipher yang memiliki kunci simetris dan mengenkripsi atau men plainteks secara digit per digit atau bit perbit dengan cara mengkombinasikan secara operasi biner (biasanya operasi XOR) dengan sebuah angka semiacak. Maka dari ini dapat diambil kesimpulan penggabungan algoritma Diffle-Hellman sebagai protocol antar user 1 dan lainnya dan algoritma RC4 untuk melakukan proses enkripsi dan de data text agar terjamin keamanan dalam proses mentransfer data.

Kata-Kata Kunci *: Algoritma Diffie-Hellman, Algoritma RC4, Data Text*

I. PENDAHULUAN

Berkat perkembangan teknologi yang begitu pesat berdampak positif bagi kehidupan manusia, salah satunya dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota, antar wilayah, antar negara, bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu instansi perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Sejak jaman dahulu, kriptografi sudah digunakan untuk kepentingan pengiriman pesan saat perang (kriptografi kalsik). Sistem peyandian kriptografi masih berdasarkan jumlah karakter pesan yang akan disandikan. Kriptografi klasik menggunakan teknik operasi sandi menggunakan metode subtitusi (perpindahan/pergantian huruf) dan metode transposisi (pertukaran posisi). Kemajuan teknologi yang sangat pesat telah menciptakan berbagai bentuk alat komunikasi seperti laptop serta perkembangan PC (*Personal Computer*) yang makin canggih serta memiliki memory yang cukup besar sehingga memungkinkan untuk untuk melakukan implementasi kriptografi pada informasi/data yang ada didalamnya. dalam melakukan implementasi kriptografi pada informasi/data menggunakan algoritma simetris yakni suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci sehingga algoritma ini disebut juga sebagai *single-ke algorithm* Sebelum melakukan pengiriman, Kriptografi simetrik (*symetric chipers*) adalah kriptografi dimana dalam proses enkripsi dan nya menggunakan satu key yang sama disebut juga *private key* atau *chiper secret key*.

Algoritma RC4 yakni algoritma yang memiliki suatu kunci simetri untuk melakukan enkripsi dan de. dalam pendistribusian kunci RC4 supaya lebih aman digunakan untuk kunci public maka dibutuhkan suatu algoritma pertukaran kunci simetris yaitu menggunakan algoritma pertukaran kunci diffle-helman. Algoritma ini sering juga disebut dengan protocol Diffie-Hellman atau Diffie-Hellman *key exchange* yang berguna untuk mempertukarkan kunci sesi (simetri). Tetapi protocol Diffie-Hellman dan algoritma RC4 rentan terhadap serangan, untuk itu perlu dilakukan modifikasi untuk mengatasi ini maka pada implementasinya nanti kita menggunakan hasil hash 160 bit SHA1 dari password kita untuk mencegah hal ini terjadi.

II. TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi penting dalam dunia teknologi informasi saat ini terutama dalam bidang komputer yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. Kriptografi juga menjadi salah satu syarat penting dalam keamanan teknologi informasi dalam melakukan pengiriman informasi ataupun data yang dianggap sangat penting dan rahasia.

2.2 Tujuan Kriptografi

Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, keaslian, dan ketiadaan penyangkalan. Keempat aspek terserbut yang menjadi tujuan fundamental dari suatu sistem kriptografi (Munir,2011).

1. Kerahasiaan
   Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja.
2. Integritas Data (*Data Integrity*)
   Integritas data merupakan layanan yang bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berwenang. Untuk meyakinkan integritas data ini harus dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi data. Manipulasi data yang dimaksud meliputi penyisipan, penghapusan, maupun penggantian data.
3. Keaslian (*authentication*)
   Keaslian merupakan layanan yang terkait dengan pembuktian identifikasi terhadap pihak-pihak yang ingin mengakses sistem informasi (*entity authentication*) maupun pembuktian data dari sistem informasi itu sendiri (*data origin authentication*).
4. Ketiadaan Penyangkalan (*non-repudiation*)
   Ketiadaan penyangkalan merupakan layanan yang berfungsi untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.3 Algoritma Diffie-Hellman

Algoritma Pertukaran kunci Diffie Hellman (DH), diusulkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976, adalah skema algoritma asimetris yang pertama kali diterbitkan dalam literatur terbuka. penemuan ini juga dipengaruhi oleh karya Ralph Merkle. pertukaran kunci ini memberikan solusi praktis untuk masalah distribusi kunci, yaitu, memungkinkan dua pihak untuk mendapatkan kunci rahasia dengan berkomunikasi melalui saluran tidak aman. Kita dapat memberikan public *key* ke manapun tujuan yang kita inginkan, melalui telepon, internet, *key*server, dan sebagainya. Kunci rahasia yang telah didistribusikan kemudian digunakan untuk enkripsi dan .Fungsi algoritma ini sendiri terbatas pada pertukaran nilai rahasia.

2.4 Algoritma RC4

Algoritma RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang kadang bit (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkripsi.

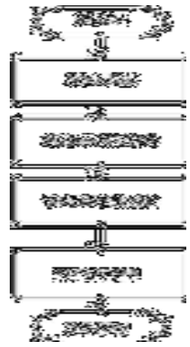
2.5 Delphi 7.0

Delphi 7 merupakan bahasa pemrograman yang dikeluarkan pada bulan agustus tahun 2002 oleh borland software corporation sebuah perusahaan perangkat lunak komputer yang berkantor pusat di austin, texas. Walaupun perkembangan delphi sudah sangat pesat masih banyak pengembang aplikasi yang menggunakan delphi 7, alasannya yaitu delphi 7 masih sangat memadai dan mempunyai kestabilan yang prima serta kebutuhan akan perangkat keras yang tidak terlalu tinggi.

III METODE PENELITIAN

3.1 Analisis Sistem

Analisis sistem merupakan kegiatan penguraian suatu sistem dalam aplikasi yang utuh dan nyata dalam bagian bagian atau komponen komponen pada sistem yang bertujuan untuk mengidentifikasi-kan serta mengevaluasi masalah-masalah yang muncul, hambatan-hambatan yang mungkin terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga mengarah kepada suatu solusi untuk perbaikan maupun pengembangan ke arah yang lebih baik dan sesuai dengan kebutuhan serta perkembangan teknologi diantaranya membahas mengenai sistem dalam bidang kriptografi yang selama ini ada, baik dari segi kelebihan dan kekurangannya. Dalam kegiatan untuk melakukan penguraian penelitian serta mempelajari interaksi sistem diantaranya, analisis masalah, analisis algoritma, analisis aplikasi sistem berjalan, analisis kebutuhan sistem, analisis aplikasi yang diusulkan dan lain-lain, yang dilakukan untuk mengetahui kegiatan-kegiatan yang sedang berjalan maupun yang sedang diusulkan suatu sistem.



Gambar 1. Diagram Alir Penelitian

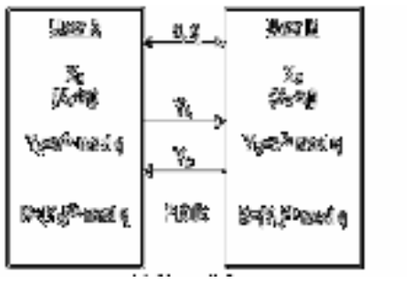
3.2 Implementasi

Implementasi merupakan tahapan penulis dalam melakukan analisis terhadap cara kerja dari algoritma diffie hellman dan algoritma RC4 serta mengimplementasikannya ke dalam sebuah program

dengan menggunakan Borland Delphi 7. Lebih spesifiknya, Diffie hellman dan RC4 dengan Fungsi Hash SHA-1.

3.3 Pembangkit Kunci Dengan Algoritma Diffie-Hellman

Untuk membangkitkan kunci, Kharisma sebagai pengirim akan mengirimkan bilangan acak integer x besar. Maulana sebegai penerima data juga akan melakukan hal yang sama, kemudian mereka akan melakukan pertukaran angka. Dalam scenario ini Kharisma memilih bilangan 257, dan Maulana memilih 281. Karena Kharisma sebegai pengirim maka Kharisma akan menentukan nilai p = 331 dan g = 2. Kemudian keduanya melakukan perhitungan untuk mendapatkan kunci publik masing-masing.



$$Y_{Kharisma} = g^x \bmod p \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$Y_{Kharisma} = 2^{257} \bmod 331$$

$$Y_{Kharisma} = 327$$

$$Y_{Maulana} = g^x \bmod p \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$Y_{Maulana} = 2^{281} \bmod 331$$

$$Y_{Maulana} = 62$$

Dari perhitungan diatas diperoleh kunci publik

$$Public_{Kharisma} = y, g, p$$

$$Public_{Kharisma} = (327,2,331)$$

$$Public_{Maulana} = y, g, p$$

$$Public_{Maulana} = (62,2,331)$$

Setelah mendapatkan kunci publik, mereka akan saling bertukar kunci dan secara terpisah akan melakukan perhitungan untuk mendapatkan kunci rahasia.

$$X_{Kharisma} = Y_{Maulana}^{x} \bmod p \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$X_{Kharisma} = 62^{257} \bmod 331$$

$$X_{Kharisma} = 128$$

$$X_{Maulana} = Y_{Kharisma}^{x} \bmod p \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$X_{Maulana} = 327^{281} \bmod 331$$

$$X_{Maulana} = 128$$

Dari hasil perhitungan diatas maka telah diperoleh kunci rahasia dari pertukaran kunci tersebut yaitu nilai $X_{Kharisma}$ dan nilai $X_{Maulana}$ yakni = 128.

3.4 Algoritma RC4 dan Fungsi Hash SHA1

Sebelum dilakukan proses enkripsi dan de menggunakan algoritma RC4 dilakukannya fungsi HASH SHA1 untuk men*digest* kunci yang dihasilkan yang digabungkan dalam melakukan proses enkripsi dan de pada proses ini kunci user di-*expand* hingga 260 byte (tetapi kemudian hanya 256 byte saja yang digunakan) dengan menggunakan SHA- 1, caranya pertama kunci user dijadikan kunci, kemudian 1-20 byte pertama pada buffer diproses dengan SHA kemudian digestnya diletakan pada 20 byte pertama, kemudian diambil byte 1-40 diproses dengan SHA dan hasilnya diletakan mulai pada byte 20, berikutnya byte 1-60 hasilnya diletakkan pada mulai byte 40, dan seterusnya. Kemudian buffer ini dienkrip dengan RC4, lalu buffer dijadikan kunci kembali, proses terakhir ini diulang sebanyak 16 kali untuk mencoba mencampur dengan baik sehingga dihasilkan kunci yang se-random mungkin.

Langkah-langkah dalam menghitung nilai hash adalah sebagai berikut:

Step 1	Divide M(i) into 16 words W(0), W(1), … , W(15), where W(0) is the left-most word.
Step 2	For t = 16 to 79 do W(t) = S^1(W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16))
Step 3	Let A = H0, B = H1, C = H2, D = H3, E = H4
Step 4	For t = 0 to 79 do TEMP = S^5(A) + f(t;B,C,D) + E + W(t) + K(t); E = D; D = C; C = S^30(B); B = A; A = TEMP;
Step 5	H0 = H0 + A; H1 = H1 + B; H2 = H2 + C; H3 = H3 + D; H4 = H4 + E;

Kemudian dilakukan fungsi Enkripsi dan De menggunakan algoritma RC4, Untuk menghasilkan keystream, cipher menggunakan state internal yang meliputi dua bagian :

1. Tahap key scheduling State yang diberi nilai awal berupa array yang merepresentasikan suatu permutasi dengan 256 elemen, jadi hasil dari algoritma RC4 adalah permutasi awal. Array yang mempunyai 256 elemen ini (dengan indeks 0 sampai dengan 255) dinamakan S. Berikut adalah algoritma RC4 dalam 29 bentuk pseudo-code dimana key adalah kunci enkripsi dan keylength adalah besar kunci enkripsi dalam bytes (untuk kunci 128 bit, keylength = 16).

   for i = 0 to 255…….(6)

   S [i] := i… ……..(7)

   j := 0 for i = 0 to 25.....(8)

j := (j + S[i] + key [I mod keylenght]) mod 256……...(9)

swap (S[i], S[j])… ……(10)

2. Tahap pseudo-random generation dimana state automaton beroperasi dan outputnya menghasilkan keystream. Setiap putaran, bagian keystream sebesar 1 byte (dengan nilai antara 0 sampai dengan 255) dioutput oleh PRGA berdasarkan state S. Berikut adalah algoritma PRGA dalam bentuk pseudocode:

i := 0

j := 0

loop i := (i + 1) mod 256…….(11)

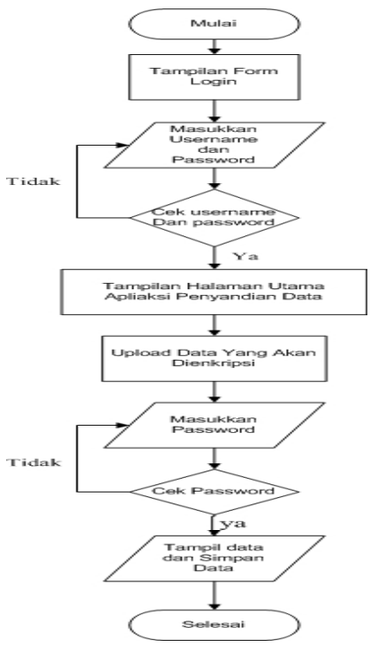
j := (j + S[i]) mod 256…….(12)

swap (S[i], S[j])……..(13)

output S[(S[i] + S[j]) mod 256].(14)

Setelah terbentuk keystream, kemudian keystream tersebut dimasukkan dalam operasi XOR dengan plaintext yang ada, dengan sebelumnya pesan dipotong-potong terlebih dahulu menjadi byte-byte. Sedangkan untuk de, XOR kan nilai keystream dengan byte chipertext.

3.5 Analisis Sistem Yang Sedang Berjalan

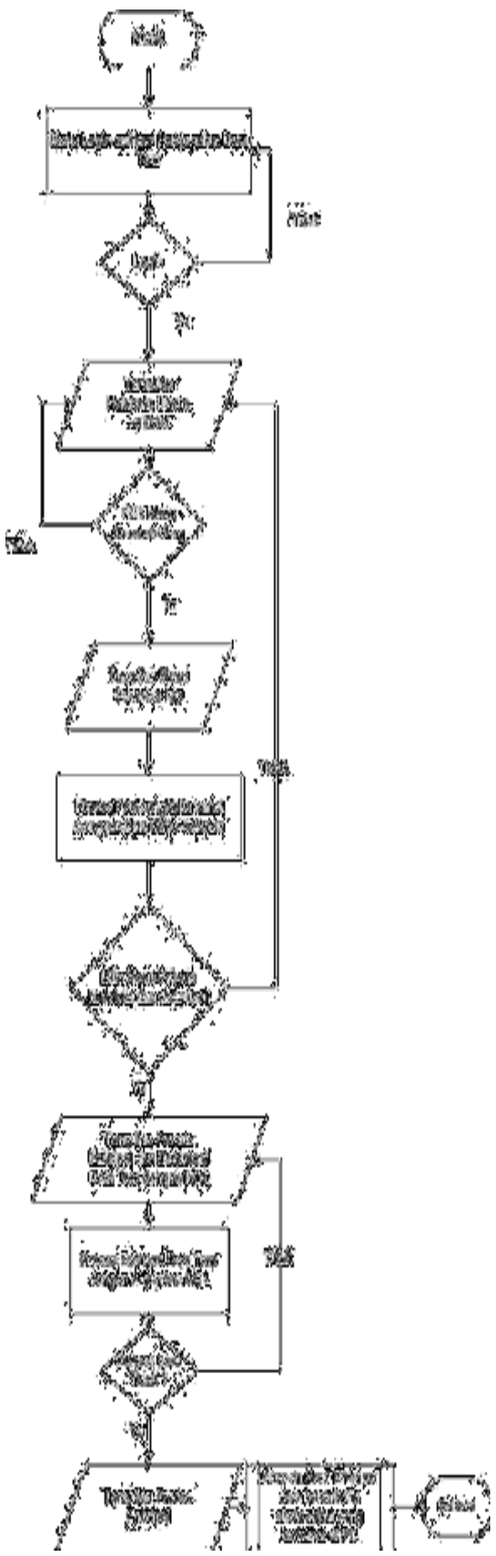


Gambar 2. Flowchart Sistem Yang Sedang Berjalan

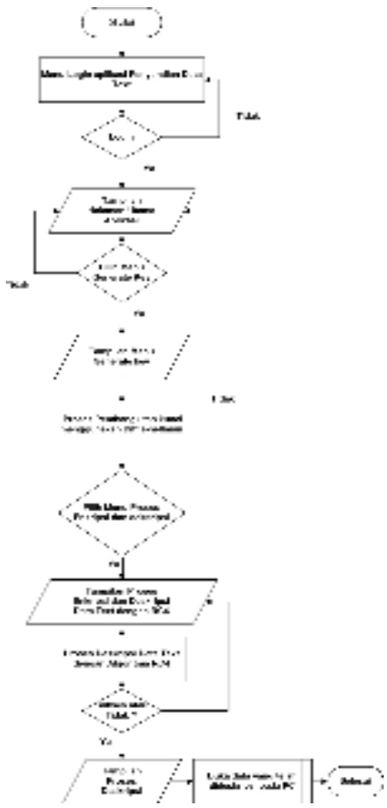
3.6 Perancangan Yang Diusulkan

Setelah tahap analisa telah dilakukan tahap selanjutnya yakni adalah perancangan aplikasi yang akan dibuat berdasarkan hasil dari analisis kebutuhan yang telah diperoleh. Dimulai dari *input,* proses hingga hasil yang diperoleh.

Dalam hal ini berdasarkan uraian analisis aplikasi sistem yang diusulkan dapat diperlihatkan lebih jelas dalam flowchart di bawah ini :



Gambar 3. *Flowchart* Sistem Enkripsi Data Text yang Diusulkan

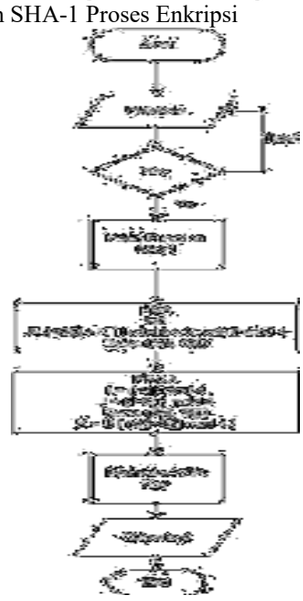


Gambar 4. *Flowchart* Sistem De Data Text yang Diusulkan

3.7 Perancangan Flowchart

Dalam hal ini berdasarkan penggunaan aplikasi dalam melakukan proses enkripsi dan de ,uraian alur penyandian data text dapat dilihat pada flowchart dibawah ini :

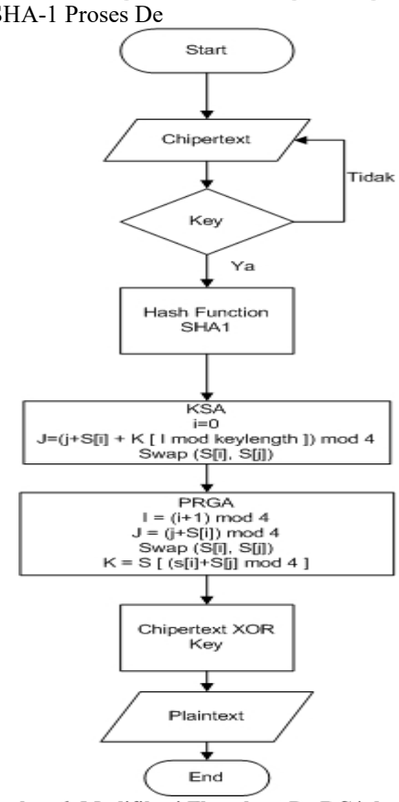
1. Flowchart Algoritma RC4 dengan Fungsi Hash SHA-1 Proses Enkripsi



Gambar 5. Modifikasi Flowchart Enkripsi RC4 dengan Fungsi Hash SHA-1

Flowchart pada Gambar 5 dimulai dengan memasukan kunci private lalu bisa dilakukan fungsi hash SHA-1 jika tidak ingin mengggunakan nya langsung dilakukan proses KSA (*Key Schedulling Algorithm*) atau sebelum masuk proses KSA fungsi dan dilanjutkan dengan proses PRGA (*Pseudo Random Generation Algorithm*). Dari proses tersebut akan dihasilkan sebuah kunci baru (*cipher*). Proses selanjutnya adalah dilakukan proses XOR antara *plaintext* dengan kunci yang didapatkan (*cipher*) sehingga hasil akhirnya berupa *chipertext.*

1. Flowchart Algoritma RC4 dengan Fungsi Hash SHA-1 Proses De



Gambar 6. Modifikasi Flowchart De RC4 dengan Fungsi Hash SHA-1

IV. ANALISA PEMBAHASAN

4.1 Pembahasan

Aplikasi dengan judul " Rancang Bangun Aplikasi Penyandian Data Text Menggunakan Algoritma Diffie-Hellman dan Algoritma RC4 " dibangun dengan menggunakan bahasa pemograman pascal dengan menggunakan aplikasi Borland Delphi 7. Berdasarkan analisis dan perancangan sistem yang telah dibuat pada Bab sebelumnya, maka untuk Bab ini, akan diimplementasikan ke dalam sebuah sistem yang dapat dioperasikan dalam keadaan yang sebenarnya.

4.2 Kebutuhan Sistem

Kebutuhan sistem yang dibutuhkan dalam rancang bangun aplikasi penyandian data text menggunakan algoritma diffie-hellman dan algoritma RC4 dibedakan menjadi kebutuhan

perangkat keras, kebutuhan perangkat lunak dan kebutuhan pengguna.

4.2.1 Perangkat Keras

Spesifikasi kebutuhan sistem perangkat keras yang dibutuhkan adalah, *Processor Intel Core* i3, RAM 3 Gb, *Hardisk* 500 Gb, *Keyboard*, Mouse dan juga monitor 14".

4.2.2 Perangkat Lunak

Spesifikasi kebutuhan sistem perangkat lunak yang dibutuhkan adalah, sistem operasi menggunakan *Microsoft Windows* 10, *Microsft Office Word* 2007, *Microsoft Office Visio* 2007, dan bahasa pemograman menggunakan Borland Delphi 7.

4.3 Implementasi Sistem

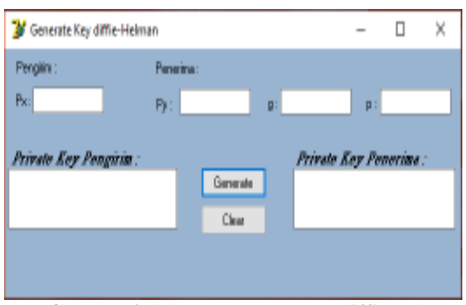
Pada implementasi sistem aplikasi penyandian data text menggunakan algoritma diffie-hellman dan algoritma RC4 merupakan hasil pengerjaan program dengan menggunakan Borland Delphi 7.

Gambar 7. Tampilan Login Aplikasi

Setelah login aplikasi masuk pada menu utama aplikasi

Gambar 8. Menu Utama Aplikasi

Tahapan selanjutnya yakni membangkitkan kunci dengan algoritma diffie hellman yang terdapat pada menu generate key diffie-hellman



Gambar 9. Menu generate key diffie-hellman

Form untuk melalukan enkripsi de yakni pada menu enkripsi dan deksripsi yang berguna untuk menyandikan data text.

Gambar 10. Menu Enkripsi dan De

V. KESIMPULAN DAN SARAN

Kesimpulan dari hasil penelitian ini adalah, bahwa aplikasi penyandian data text menggunakan menggunakan algoritma diffie-hellman dan algoritma RC4 adalah :

1. Dapat menyandikan data text tanpa menimbulkan keruskan terhadap data aslinya.
2. Aplikasi penyandian data text menggunakan algoritma diffie-hellman dan Algoritma RC4 ntuk mengamankan keaslian data agar tidak mudah dirubah oleh orang yang tidak bertanggung jawab.
3. Aplikasi penyandian data text menggunakan algoritma diffie-hellman dan algoritma RC4 untuk meningkatkan keamanan data.
4. Menghasilkan aplikasi penyandin data text menggunakan algoritma diffie-hellman dan algoritma RC4 dalam mengamankan beberapa jenis file tidak hanya data text saja , adapun jenis data lain yakni, text, audio, video, dan gambar.

DAFTAR PUSTAKA

[1] Ana Wahyuni, 2011, *Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid : Diffie-Hellman dan RSA,* Fakultas Ilmu Komputer Universitas AKI, Majalah Ilmiah INFORMATiKA Vol. 2 No. 2, Mei 2011

[2] Arifyanto, A.E, 2013. '*Implementasi Enkripsi Basis Data Berbasis Web Dengan Algoritma Stream Cipher RC4*', Dokumen Karya Ilmiah Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dian Nuswantoro Semarang

[3] ARIYUS, D. 2008. *Pengantar Ilmu Kriptografi*, Yogyakarta: Andi

[4] HAJI, W. H. & MULYONO, S. 2012. *Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data*. Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

[5] Hendarsyah.Decky, Wardoyo.Rentatyo, 2011. *Implementasi Protokol Diffie-Hellman Dan Algoritma RC4 Untuk Keamanan Pesan SMS*, IJCCS, Vol. 5 No. 1, Jan, 2011

[6] Hendrawati, Hamdani, Awang Harsa K, 2014, *Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 (Rc4) Dan Steganografi Pada Citra Digital,* Informatika Mulawarman | Februari 2014 Vol. 9 | No. 1 ISSN 1858-4853

[7] Kristanto, Andri. 2003. *Keamanan Data pada Jaringan Komputer.* Yogyakarta: Penerbit Gava Media

[8] Kusnassriyanto , 2011, *Belajar Pemograman Delphi*, Modul-Bandung

[9] Mollin, R. A. 2007. *An Introduction to Cryptography*. 2nd ed. Florida: Chapman & Hall/CRC.

[10] Mousa, A. dan Hamad, A., 2006, *Evaluation of the RC4 Algorithm for Data Encryption*, *International Journal of Computer Science & Applications*, No.2, Vol.3, June 2006,pp. 44-56, An-Najah University, Nablus, Palestine

[11] Munir, Rinaldi. 2011. *Kriptografi Keamanan*. Bandung: Informatika Bandung

[12] Munir, Rinaldi. 2008. *Belajar Ilmu Kriptografi*. Yogyakarta: Penerbit Andi

[13] Purwadi,Jaya Hendra ,Calam.Ahmad , 2014. *Aplikasi Kriptografi Asimetris Dengan Metode Diffie-Hellman Dan Algoritma Elgamal Untuk Keamanan Teks,* Jurnal SAINTIKOM Vol. 13, No.3, Januari 2014

[14] Sadikin, Rifki. 2012. *Kriptografi Untuk Keamanan Jaringan.* Yogyakarta: Penerbit Andi Offset.

[15] Stalling, W. 2004. *Cryptography and Network Security*, Pearson Education, India

[16] Stallins, W., 2005, *Cryptography and Network Security Principles and Practices Fourth Edition*, Prentice Hall,New Jersey

[17] Taronisokhi Zebua, Eferoni Ndruru, 2017*, Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4*, Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.201744474 Vol. 4, No. 4, Desember 2017999