Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA Dan MD5

Tri Ferga Prasetyo, Aris Hikmawan

Abstract—The development of computer systems and interconnections through Multimedia networkhas Increased . Currently computer system more accessible , Time sharing system and remoteaccess system causes a security problem Becomes one of the weaknesses of communication data.In an era of universal electronic connectivity Often there is interference in the form of hackers,viruses , fraud , electronic or hear secretly electronically. Data security issues for organizations or educational institutions is very important in theinformation age. In the world of education, especially among university one way to secure the data ofstudents who are in an existing information systems in college as I-LISTPRO, required cryptographicencryption methods. Encryption method used in this study using three methods of encryption, namely RC4SHA and MD5. Data security is one very important aspect in the use of computers. The data owner willwant to secure their data against interference from actions that are not in want, either from a personalcomputer (PC) or a network.

Keyword—data security, Encryption, RC4, SHA, MD5.

1. Pendahuluan

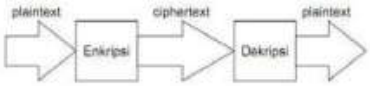
Dalam dunia pendidikan khususnya di kalangan perguruan tinggi salah satu cara untuk mengamankan data mahasiswa yang berada di dalam sebuah sistem informasi yang ada di perguruan tinggi seperti I-LISTPRO, diperlukan kriptografi dengan metode enkripsi. Proses pengamanan data mahasiswa yang berada di dalam sebuah jaringan yang berbasis localhost / website, memerlukan metode khusus. Diantaranya yaitu metode algoritma Rivest Code 4 (RC4), RC4 ini merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data pada satu saat. Unit atau data pada umumnya sebuah byte atau bahkan kadang kadang bit (byte dalam hal RC4). [SA10]. Metode yang digunakan selanjutnya adalah Secure Hash Algoritma (SHA), SHA adalah serangkaian fungsi cryptographic hash yang dirancang oleh National Security Agency (NSA) dan diterbitkan oleh NIST sebagai US Federal Information Processing Standard. Jenis-jenis SHA yaitu SHA-0, SHA-1, dan SHA-2. Untuk SHA-2 menggunakan algoritma yang identik dengan ringkasan ukuran variabel yang terkenal sebagai SHA-224, SHA-256, SHA-384, dan SHA-512. [F11]. Metode yang terakhir ialah Message-Digest algortihm 5 (MD5), MD5 adalah salah satu dari serangkaian algortima message digest yang didesain oleh Profesor Ronald Rivest dari MIT pada tahun 1994. Saat kerja analitik menunjukkan bahwa pendahulu MD5 yaitu MD4 mulai tidak aman, MD5 kemudian didesain pada tahun 1991 sebagai pengganti dari MD4 (kelemahan MD4 ditemukan oleh Hans Dobbertin). Dalam kriptografi, MD5 (Message- Digest algortihm 5) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada Standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file. [PA08]. Untuk memperkuat sistem keamanan data pada I-LISTPRO, maka dibutuhkanlah sebuah sistem keamanan data yang paling baik dari ketiga metode diatas dengan memberikan manfaat untuk menghindari ancaman keamanan data.

2. Pembahasan

2.1 Kriptografi

Kriptografi (cryptographi) berasal dari BahasaYunani: “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Sehingga kriptografi berarti “secret writing” (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara

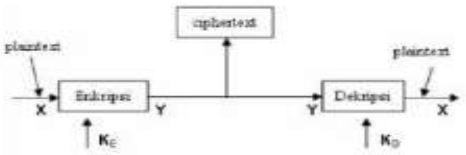
menyandikannya kebentuk yang tidak dapat dimengerti lagi maknanya. Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (chipertext) yang tidak dapat dibaca secara langsung. Chipertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi. Urutan proses kriptografi secara umum dapat dilihat pada gambar 2.1



Gambar 2.1 Mekanisme Enkripsi dan Deskripsi

2.2 Enkripsi dan Deskripsi

Proses penyandian pesan dari plaintext ke ciphertext dinamakan enkripsi / enchipering. Sedangkan proses mengembalikan pesan dari chipertext ke plaintext dinamakan deskripsi / dechipering. Proses enkripsi dan deskripsi ini dapat diterapkan pada pesan yang dikirim ataupun pesan yang disimpan. Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi. Secara sederhana proses kriptografi dapat digambarkan sebagai berikut :



Gambar 2.2 Kriptografi secara umum.

Operasi enkripsi dan dekripsi dijelaskan secara umum sebagai berikut :

Y Eĸe = (enkripsi)

X Dĸd = (dekripsi)

Ada dua cara yang paling dasar pada kriptografi klasik. yaitu adalah Transposisi dan Subsitusi :

1) Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
2) Substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu.

2.3. Tahapan Analisis

Pada tahapan Pertama proses Analisis Penelitian, Penulis melakukan identifikasi masalah yang ada seperti dibutuhkannya sebuah sistem keamanan data yang bisa menjamin keamanan data login mahasiswa secara cepat dan kuat, dengan menggunakan metode yang terbaik dari tiga metode yang di uji. Tahapan selanjutnya, Penulis melakukan Studi Literatur, Internet Research ataupun dari Penelitian Terdahulu untuk mengumpulkan referensi – referensi tentang sistem Keamanan data dengan menggunakan Algoritma kriptografi. Setelah melalui Proses Tinjauan Pustaka, Penulis melakukan pengumpulan data yang diperlukan untuk menganalisa sistem keamanan yang sedang digunakan, data tersebut berupa source code Halaman Login Mahasiswa dan Data base berupa username / password untuk di Uji pada Tahapan selanjutnya. Selanjutnya Tahapan paling sulit dan paling panjang prosesnya yang Penulis lakukan ialah pada saat melakukan Pengujian kepada 3 (tiga) Metode Enkripsi, dimana dari ke 3 (tiga) metode tersebut mempunyai proses yang berbeda satu sama lainya. Kemudian dari pengujian ke 3 (tiga) metode tersebut akan dipilih metode yang terbaik untuk di Implementasikan kedalam Sistem Informasi I- LISTPRO, Selanjutnya akan mendapatkan sebuah rekomendasian Sistem Keamanan dengan memperlihatkan sebuah data hasil perbandingan dari ke 3 (tiga) Metode Enkripsi di atas.

2.4 Sampel Penelitian

Sampel yang Penulis ambil untuk Penelitian ini berupa Database Mahasiswa yang ada di Sistem Informasi I-LISTPRO yaitu Username dan Password Mahasiswa, dimana rata-rata password dari kebanyakan mahasiswa masih menggunakan password default nya. Sehingga tidak jarang dari Mahasiswa tersebut sering kesulitan untuk masuk kedalam akunnya sendiri karena kesalahan password yang telah dirubah oleh orang-orang jahil. Username dan Password default yang telah di setting oleh pihak Fakultas ialah menggunakan NPM sebagai Username dan 123456789 sebagai Password nya.

Tabel 2.1 Sampel Data *Username* dan *Password* I-LISTPRO

Username	*Password*	Nama
11.14.1.0035	123456789	ARIS HIKMAWAN
11.15.1.0019	123456789	RIKI ISMAYA
14.16.1.0032	123456789	DETRA PANDJI WIWAHA
14.17.1.0006	123456789	DETTA WARDHANA

3. Hasil Pembahasan

Sesuai yang telah dikemukakan di Bab sebelumnya, bahwa pengujian dari ke 3 (Tiga) Algoritma Kriptografi untuk keamanan sistem informasi I-LISTPRO Fakultas Teknik Universitas Majalengka dilakukan pengujian secara otomatis menggunakan alat pengenkripsi HashKiller.

3.1 Langkah – Langkah Penyelesaian

Menurut (Munir, 2006) Dari permasalahan diatas, maka penulis mencoba untuk membuat sebuah rancangan yang berguna untuk mengamankan sebuah data dengan menggunakan algoritma terbaik dari kriptografi RC4, SHA dan MD5. Langkah – langkah simulasi dalam penyelesaian masalah diatas yaitu :

3.1.1 Pengujian Algoritma Kriptografi RC4

Sistem sandi RC4 menggunakan State, yaitu larik byte berukuran 256 yang terpermutasi, dan tercampur oleh kunci. Kunci juga merupakan larik byte berukuran 256. Sebelum melakukan proses enkripsi, Tahap Pertama kita harus menginisialisasi terhadap state dengan melakukan Penjadwalan kunci (key scheduling / setup key).

```
Input : key
Output : {S[1],...,S[N]}
for i = 0⟶ 255 do
S[i] = i
end for
j=0
for i = 0⟶ 255 do
j = (j + S[i] + key[i mod |key|]) mod 256
swap values of S[i] and S[j]
end for
```

Setelah *state* S terinisialisasi oleh penjadwal kunci setiap *byte* pada teks asli dikenakan operasi XOR dengan kunci *byte* untuk menghasilkan *byte* pada teks sandi. Kunci *byte* yang digunakan pada enkripsi dibangkitkan dengan memanfaatkan *state* S.

```
Input : P {Stream teks asli}
Output : C {Stream teks sandi}
i = 0, j = 0 {Bisa diisi nilai lain}
while P masih memiliki byte do
i = (i + 1) mod 256
j = (j + S[i]) mod 256
swap (S[i], S[j])
K = S[S[i] + S[j]] mod 256
C=P k⊕
End while
```

Hasil Pengujian RC4 Terhadap *Password User* pada I-LISTPRO :

Tabel 3.1 Tabel Hasil Enkripsi RC4

Plaintext (*Password*)	Key	Chipertext
123456	labft	É²âäÊ
123456789	M	'%xÛÈR#C
130979	labft2	]EÛ™e
ftgelo	perpusteknik	Ðôu'g

3.1.2 Pengujian Algoritma Kriptografi SHA

Algoritma SHA1 bekerja seperti berikut:

1. Penambahan bit-bit pengganjal. Ini dilakukan agar panjang pesan kongruen dengan 448 modulo 512. Ini berarti panjang pesan setelah ditambahi bit penganjal adalah 64 bit kurang dari kelipatan 512;
2. Pesan dengan panjang 448 bit juga ditambah dengan bit-bit pengganjal. Ditambah dengan 512 bit pengganjal sebanyak 512 bit agar panjangnnya menjadi 960 bit. Bit pengganjal adalah sebuah bit 1 diikuti selebihnya bit 0;
3. Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Panjang bit ini menggenapkan panjang pesan menjadi kelipatan 512bit;
4. SHA membutuhkan 5 buah penyangga uang masing-masing panjangnya 32 bit. Total panjang penyangga adalah 5 x 32 bit = 160 bit;
5. Kelima penyangga tesebut diberi nama A,B,C,D,E dan diberi nilai inisiasi 8 hexa;
6. Pesan dibagi menjadi L buah blok yang masing masing panjangnya 512 bit;
7. Setiap blok 512bit ini diproses bersama dengan penyangga MD dari langkah 6 menjadi keluaran 128 bit. Proses SHA-1 terdiri dari 80 putaran dan masing-masing putaran menggunakan bilangan penambah Kt yaitu :

Putaran 0 – 19 mengunakan K1
Putaran 20-39 menggunakan K2
Putaran 40-59 menggunakan K3
Putaran 60-79 menggunakan K4

K1- K4 adalah bilangan hexa yang ibangkitkan mirip dengan MD pada langkah 5. Operasi dasar SHA ditulis dengan notasi sebagai berikut : A,B,C,D,E _ (CLSs(A) + Ft(B,C,D) + E + Wt + Kt), A, CLS30(B), C,D. Dalam hal ini :

a. A,B,C,D,E adalah lima buah penyangga 32 bit;
b. t adalah Putaran (0 – 79), Ft adalah fungsi logika tiap putaran yang berbeda-beda tiap 20 putaran;
c. CLSs adalah operasi bit circular left sebanyak s bit;
d. Wt adalah word 32 bit yang diturunkan dari 512 blok bit yang sedang diproses;
e. Kt adalah konstanta penambah + operasi penjumlahan modulu 2pangakat 32. Untuk tiap putaran Ft adalah sebagai berikut :
   Putaran 0 -19 : (B and C) OR (~B and D)
   Putaran 20-39 : (B xor C xor D)
   Putaran 40-59 : (B and C) or (B and D) or (C and D) Putaran 60 – 79 : B xor C xor D

Langkah-langkah kerja pada SHA-1 adalah sebagai berikut:

a) Melakukan padding terhadap pesan sehingga panjangnya adalah 448 modulus 512;
b) 64 bit sisanya adalah representasi biner dari
   panjang pesan;
c) Melakukan inisialisasi 5 word buffer (160 bit)A, B, C, D, dan E dengan nilai A=67452301, B=efcdab89, C=98badcfe, D= 10325476, dan E=c3d2e1f0. Memproses pesan dalam blok-blok 16 word (512 bit) dengan ketentuan:
d) Ekspansi 16 words menjadi 80 words dengan teknik mixing dan shifting;
e) Menggunakan 4 round dari 20 operasi bit
   pada blok pesan dan buffer;
f) Menambahkan output dengan input untuk
   mempeoleh nilai buffer yang baru. fungsi kompresi yang digunakan oleh algoritma sha-1 adalah sebagai berikut :

a. A,b,c,d,e ← (e + f(t,b,c,d) + s5(a) + wt +
   kt),a,s30(b),c,d;
b. Output nilai hash adalah nilai terakhir dari
   buffer.

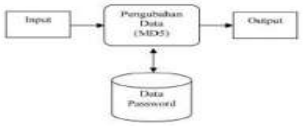
HA-1 adalah yang paling banyak digunakan dari fungsi hash SHA yang ada, dan digunakan dalam beberapa aplikasi keamanan secara luas digunakan dan protocol, Memiliki Panjang 20 bytes (40 karakter).

Hasil Pengujian SHA1 Terhadap *Password User* pada I-LISTPRO :

Tabel 3.2 Tabel Hasil Enkripsi SHA1

Usernam	Plaintext (Password	Chipertext (Password)
labft2	123456	7c4a8d09ca3762af61e59520943dc26494f8941
11.14.1.0035	123456789	f7c3bc1d808e04732adf679965ccc34ca7ae3441
Labft	130979	7852c5b542b32c360c83
Perpustek	ftgelo	28f1da59d5f74ae4bce724 10355ff6264c30e660

3.1.3 Pengujian Algoritma Kriptografi MD5



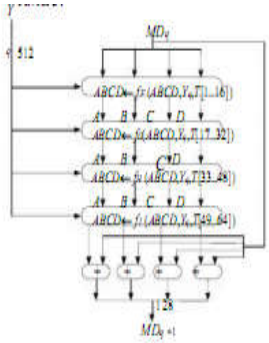
Gambar 3.1 Alur Proses Pembuatan *Password MD5*

Langkah-Langkah Pembuatan MD, sebagai berikut :

1. Penambahan Bit-bit Pengganjal
   a. Pesan ditambah dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512;
   b. Jika panjang pesan 448 bit, maka pesan tersebut ditambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah antara 1 sampai 512;
   c. Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0.
2. Penambahan Nilai Panjang Pesan
   a. Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula;
   b. Jika panjang pesan > 264 maka yang diambil adalah panjangnya dalam modulo 264. Dengan kata lain, jika panjang pesan semula adalah K bit, maka 64 bit yang ditambahkan menyatakan K modulo 264;
   c. Setelah ditambah dengan 64 bit, panjang

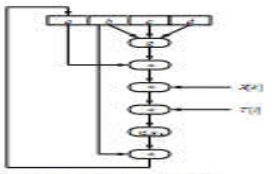
pesan sekarang menjadi kelipatan 512 bit.

3. Inisialisai Penyangga MD
   a. MD5 membutuhkan 4 buah penyangga (buffer) yang masing-masing panjangnya 32 bit. Total panjang penyangga adalah 4 x 32 = 128 bit. Keempat penyangga ini menampung hasil antara dan hasil akhir;
   b. Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut:
      A = 01234567
      B = 89ABCDEF
      C = FEDCBA98
      D = 76543210
4. Pengolahan Pesan dalam Blok Berukuran 512 bit
   a. Pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit (Y0 sampai YL – 1);
   b. Setiap blok 512-bit diproses bersama dengan penyangga MD menjadi keluaran 128-bit, dan ini disebut proses HMD5.

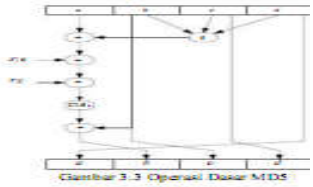


Gambar 3.2 Gambaran Proses HMD5

   c. Pada Gambar diatas, yang menyatakan blok 512-bit ke-q dari pesan yang telah ditambah bit-bit pengganjal dan tambahan 64 bit nilai panjang pesan semula;
   d. MDq adalah nilai message digest 128-bit dari proses HMD5 ke-q. Pada awal proses, MDq berisi nilai inisialisasi penyangga MD;
   e. Proses HMD5 terdiri dari 4 buah putaran, dan masing-masing putaran melakukan operasi dasar MD5 sebanyak 16 kali dan setiap operasi dasar memakai sebuah elemen T. Jadi setiap putaran memakai 16 elemen Tabel T;
   f. Fungsi-fungsi fF, fG, fH, dan fI masing-masing berisi 16 kali operasi dasar terhadap masukan, setiap operasi dasar menggunakan elemen Tabel T;



Gambar 3.4 Operasi Dasar MD5



Gambar 3.3 Operasi Dasar MD5

   g. Karena ada 16 kali operasi dasar, maka setiap kali selesai satu operasi dasar, penyangga-penyangga itu digeser ke kanan secara sirkuler dengan cara pertukaran sebagai berikut:
      Temp←d
      d←c
      c←b
      b←a
      a←temp

Hasil Pengujian MD5 Terhadap *Password User* pada I-LISTPRO :

Tabel 3.3 Tabel Hasil Enkripsi MD5

Username	*Plaintext (Password)*	*Chipertext (Password)*
labft2	123456	e10adc3949ba59abbe56e057f20f883e
11.14.1.0035	123456789	25f9e794323b453885f5181f1b624d0b
labft	130979	b7852fd328b06c8ef18617b4fd03b8ca
perpustaknik	Ftgelo	a293486fac430911a977e415b9a7a3a0

3.2 Laporan Hasil Perbandingan

Dari Hasil pengujian Data Base diatas, didapat perbandingan waktu sebagai berikut :

Tabel 3.4 Tabel Perbandingan Waktu deskripsi

Test	*Plaintext*	Metode RC4	Metode SHA1	Metode MD5
1	ftunma	144 m/s [Succes]	440 m/s [Succes]	209 m/s [Succes]
2	FTunma	148 m/s [Succes]	345 m/s [Failed]	318 m/s [Failed]
3	1234567	186 m/s [Succes]	111 m/s [Succes]	135 m/s [Succes]
4	ftunma12	150 m/s [Succes]	306 m/s [Succes]	310 m/s [Failed]
5	FTunma#	153 m/s [Succes]	439 m/s [Succes]	326 m/s [Failed]
Rata - Rata		156 m/s	328,2 m/s	259,6 m/s

Keterangan : Hasil pada Tabel diatas dipengaruhi oleh Koneksi dan Spesifikasi PC/Laptop yang digunakan.

4. Kesimpulan

Berdasarkan pembahasan pada sebelumnya, mengenai hasil dari Analisis Perbandingan dan

Implementasi Sistem Keamanan Data dengan menggunakan Metode Enkripsi RC4 SHA dan MD5, maka didapat Kesimpulan :

1. Dari hasil perbandingan 3 Metode Enkripsi diatas, dapat disimpulkan bahwa Metode Enkripsi SHA lebih kuat dibanding 2 Metode lainya, dan bisa di implementasikan kedalam Program PHP, Karena SHA mempunyai jumlah karakter yang paling banyak (40 Karakter) dan paling lama di Deskripsi dibanding Metode lainnya;
2. Dari pengujian ke 3 metode enkripsi di atas menggunakan HashKiller, Plainteks / Password yang menggunakan kombinasi Huruf, Angka dan Simbol hasilnya akan mengalami kegagalan (Failed) atau gagal di Deskripsi, dalam kata lain password akan jauh lebih aman;
3. Dari Hasil Implementasi didapat bahwa, RC4 kurang cocok untuk digunakan dalam sistem keamanan data berbasis web karena RC4 merupakan metode enkripsi chiper key, sedangkan metode enkripsi MD5 kurang bagus jika dibandingkan dengan SHA, Karena rentan terhadap serangan collision attack. Jadi SHA direkomendasikan untuk digunakan dalam sistem keamanan data.

5. Daftar Pustaka

Alfikri, Zakry,"Studi dan Analisis Dua Algoritma Block Chiper : RC4", ITB, Bandung, 2010.

Barthos, Basir,”Pengertian Perguruan Tinggi”, 1992:25.

Fantony,"Penerapan Enkripsi dengan metode SHA pada aplikasi berbasis web situs E-Commerce kuepalembang.com", STMIK GI MDP, Palembang, 2011.

Fatta, A.,”Analisis dan Perancangan Sistem Informasi”, Andi, Yogyakarta, 2007.

Kurniawan, Ashadi,"Analisa Dan Implementasi Sistem Keamanan Data Dengan Menggunakan Metode Enkripsi Algoritma RC-5", ITS, Surabaya, 2009. [MR02] Munir, Rinaldi,."Algoritma dan Pemograman", ITB, Bandung, 2002.

Munir, Rinaldi,."Hash Satu Arah dan Algoritma MD5", ITB, Bandung, 2004.

Munir, Rinaldi,."Pengantar Kriptografi", ITB, Bandung, 2004.

Perdana, Adya Rahmat,"Metode Penyandian Pesan Dan Menjaga Integritas Data Menggunakan Kriptografi Algoritma MD5", Universitas Sriwijaya, Palembang, 2008.

Sugiyono,”Populasi dan Sampel”, 2010:118.

Sutiono, Arie Pratama,"Algoritma RC4 sebagai Perkembangan Metode Kriptografi", ITB, Bandung, 2010.

Sukmawan, B.,”RC4 Stream Cipher”, 1998.

Sadikin, R.,”Kriptografi untuk Keamanan Jaringan”, Andi, Yogyakarta, 2012.