Jurnal CyberTech
Vol.x. No.x, Agustus 2020, pp. xx~xx
P-ISSN :
E-ISSN :

Implementasi Keamanan Data Gaji Pada Dinas Komunikasi Dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4

Muhammad Haris Hrp*, **Nurcahyo Budi Nugroho, S.Kom, M.Kom** **, **Rico Imanta Ginting, S.Kom, M.Kom** **

*Program Studi Sistem Informasi, STMIK Triguna Dharma
** Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:

Keyword:
Kriptografi ,Algoritma RC4, Keamanan Data Gaji.

ABSTRACT

Dinas Komunikasi informatika dan Persandian Kabupaten Aceh Tamiang merupakan unusur pelaksana urusan pemerintahan bidang komunikasi dan informatika, urusan pemerintahan bidang persandian, dan urusan pemerintahan di bidang statistik yang di pimpin oleh Kepala Dinas yang berkedudukan di bawah dan bertanggung jawab kepada bupati melalui Sekretaris Daerah. Kehilangan data bisa sangat merugikan suatu perusahaan atau instansi tidak terkecuali dinas Komunikasi Informatika dan Persandian Kabupaten Aceh Tamiang.

Untuk mengatasi mengatasi masalah kehilangan data gaji, maka di buatlah sebuah program untuk mengamankan data gaji pada Dinas Komunikasi Informatika dan Persandian Kabupaten Aceh Tamiang Menggunakan Metode RC4.

Program keamanan data gaji yang menggunakan metode RC4 ini diharapkan dapat membantu menganmankan data gaji pada Dinas Komunikasi Informatika dan Persandian Kabupaten Aceh Tamiang.

Corresponding Author:

Nama : Muhammad Haris Hrp
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-mail : **Mhdharis479@gmail.com**

1. PENDAHULUAN

Perkembangan teknologi saat ini terutama pada sistem pengamanan data, dalam menjaga kemanan data dan informasi telah berkembang pesat. Ada beberapa cara dalam melakukan pengamanan data, diantaranya dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi dan teknik penyembunyian data atau disebut dengan steganografi. Kriptografi merupakan seni dan ilmu untuk mengamankan data yang akan dikirim dengan menjadikanya kode tertentu dan hanya ditujukan untuk orang yang memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan[1].

Salah satu metode enkripsi yang terkenal adalah metode RC4. RC4 pertama kali dibuat Ron Rivest di Laboratorium RSA pada tahun 1987. RC4 adalah sebuah *synchrone streamchiper*, yaitu chiper yang memiliki kunci simetris dan mengenkripsi plainteks secara byte per byte atau digit per digit dengancara mengkombinasikan dengan operasi biner(biasanya XOR) dengan sebuah angka semiacak[2].

RC4 merupakan algoritma enkripsi *Stream Chipher*. RC4 dirancang agar dapat di implementasikan di software secara efisien. Hal ini membuat RC4 sangat populer untuk aplikasi internet, antara lain RC4 digunakan dalam standard TLS(*Transport Layer Security*) dan WEP (*Wireless Equivalent Privacy)*[3].
Kemajuan teknologi informasi yang sangat pesat membuat permasalahan keamanan sering bermunculan. Seiring dengan permasalahan keamanan yang semakin meningkat, dibutuhkan pula peningkatan keamanan dalam dunia teknologi khususnya komputer dan jaringan yaitu dengan kriptografi[4].

2. KAJIAN PUSTAKA

2.1 Keamanan Data

Keamanan data adalah sebuah prosedur dengan dukungan dari regulasi dan teknologi untuk melindungi data dari perusakan data modifikasi data, serta penyebaran data baik disengaj maupun tidak disengaja. Di ungkapkan oleh Tedy Heryanto (1999) bahwa banyak kegiatan yang akan menimbulkan resiko bilamana informasi yang sensitive dan berharga terseut di akses atau dicuri oleh orang- orang yang tidak berhak(*Unauthorized Person*)[5]. Secara umum keamanan data ada beberapa aspek, yaitu sebagai berikut :

1. *Privacy/confidentiality*
   Privacy lebih kearah data-data yang bersifat rahasia, sedangkan *Confidentiality* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu.
2. *Integrity*
   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dengan saat informasi dikirimkan. Jika terdapat perbedaan antara informasi atau data yang dikirim dengan yang diterima maka aspek *integrity* tidak tercapai.
3. *Authenticity*
   Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah orang yang dimaksud.
4. *Availability*
   Aspek ini berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berbeda dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.
5. *Acces Control*
   Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. *Acces control* seringkali dilakukan dengan menggunakan kombinasi *user id/password* atau dengan menggunakan mekanisme lain[6].

2.2 Kriptografi

Secara umum kriptografi dapat di artikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data. Konsep kriptografi yang bertujuan untuk menjaga kerahasiaan pesan/data dalah dengan cara menyamarkan pesan/data menjadi bentuk tersandi yang tidak dapat dibaca oleh siapapun. Pesan/data yang akan disandikan disebut *plaintext*, sedangkan yang telah disamarkan disebut *chiphertext*. Proses penyamaran dari *plaintext* ke *chiphertext* disebut dengan enkripsi, sedangkan proses pengembalian dari *chiphertext* menjadi *plaintext* disebut dengan dekripsi[7].

2.2.1 Perkembangan Kriptografi

Secara umum kriptografi terbagi menjadi beberapa jenis diantaranya :

1. Kriptografi Klasik
   Kriptografi klasik merupakan kriptografi yang sudah digunakan pada zaman dahulu sebelum computer ditemukan atau sudah ditemukan namun belum secanggih sekarang.
2. Kriptografi modern
   Kriptografi modern merupakan teknik kriptografi yang beroperasi dalam mode karakter. Pengoprasian kriptografi ini dalam mode bit berarti semua data dan informasi (kunci, plainteks, maupun chipher teks) semua dinyatakan dalam rangkaian string ataupun bit biner 0 dan 1. Contoh dari kriptografi modern yaitu algoritma simetris dan algoritma asimetris[8].

2.2.2 Kriptografi Klasik

Kriptografi klasik terbagi menjadi 2 yaitu :

1. *Chipher* Substitusi (*Substitution Cipher*)

Merupakan algoritm kriptografi yang mula-mula digunakan oleh kaisar romawi, Julius Caesar (sehingga dinamakan juga *caesar chiper*), untuk menyandikan pesan yang ia kirim kepada para gubernurny. Caranya adalah mengganti/mensubstitusi setiap karakter dengan karakter lain sesuai susunan abjad.

2. *Chiper* Transposisi
   Pada *chiper* transposisi , plainteks tetap sama, tetapi urutannya diubah.
   Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian karakter dalam sebuah teks. Nama lain dari metode ini adalah permutasi[9].

.

2.2.3 Kriptografi modern

Kriptografi modern terbagi 2 yaitu :

1. Algoritma Simetris
   Merupakan pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi dekripsi. Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma seperti :
   a. *Data Encryption Standard* (DES)
   b. *Advance Encryption System* (AES)
   c.*International Data Encryption Algorithm* (IDEA)
   d. A5
   e.RC4
2. Algoritma Asimetris
   Merupakan pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi untuk proses dekripsi. Contoh algoritma terkenal
   yang menggunakan kunci asimetris adalah RSA(Rivest, Shamir, Adleman)[10].

2.3 Algoritma RC4

RC4 merupakan metode enkripsi tercepat dibandingkan DES, Triple DES, Blowfish 256, AES-128, dan AES-256. Secara luas pada sistem keamanan sepertiprotocol SSL (*Secure Socket Layer*). Algoritma kriptografi ini sederhana sehingga mudah di implementasikan. RC4 dibuat oleh Ron Rivest dari laboratorium RSA. Sistem sandi RC4 menggunakan State yaitu larik byte berukuran 256 yang terpermutasi, dan tercmpur oleh kunci. Sebelum melakukan enkripsi, dan dekripsi sistem sandi RC4 melakukan inialisasi terhadap state dengan Algoritma, algoritma ini disebut dengan penjadwalan kunci (*Key Scheduling*)[11].

Algoritma RC4 merupakan salah satu jenis *stream cipher* sehingga RC4 memproses unit atau input data, pesan atau informasi pada saat bersamaan. Unit atau data pada umumnya sebuah byte sehingga dengan cara ini enkripsi atau dekripsi dapat dilakukan pada panjang yang variabel. Algoritma RC4 menggunakan dua uah S-box yaittu *array* sepanjang 256 yang berisi permutasi dari bilangan 0 sampai 255, dan S-box kedua, yang berisis permutasi merupakan fungsi dari kunci dengan panjang yang variabel[12].

3. Metode Penelitian

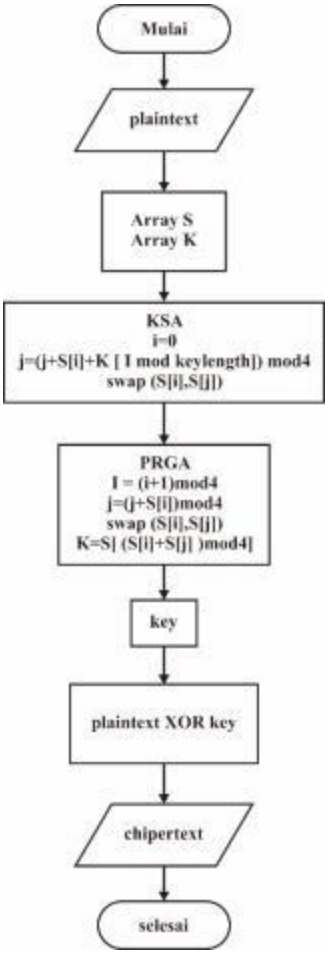
.3.1 Analisa Permasalahan

Sistem keamanan data gaji pada Dinas Komunikasi Informatika dan Persandian Kabupaten Aceh Tamiang masih kurang efektif dimana perusahaan tersebut masih belum memiliki sistem keamanan data Gaji.

Dalam mengimplementasikan keamanan data gaji pada Dinas Komunikasi Informatika Dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4 diharapkan dapat membantu mengamankan keamanan data gaji pada instansi tersebut;

3.1.1 *Flowchart* Algoritma RC4

Flowchart algoritma RC4 merupakan keterangan yang lebih rinci tentang bagaimana prosedur sesungguhnya yang dilakukan oleh suatu metode. *Flowchart* ini menggambarkan urutan logika dari suatu prosedur pemecahan masalah Berikut ini adalah *Flowchart* dari *Algoritma Rivest Chiper 4* adalah sebagai berikut:



Gambar 1 *Flowchart* Algoritma RC4

3.3.2 Algoritma RC4

Langkah-langkah dari proses algoritma RC4 stream chipper untuk melakukan enkrips – dekripsi yaitu :

1. Proses inisialisasi *S-Box* (*Array* S)
   For i = 0 to 255
   S[i] = i
2. Proses inisialisasi *S-Box* (*Array* K)
   For i = 0 to 255
   S[i] = i
3. Kemudian lakukan langkah pengacakan *S-Box*
   i=0; j=0
   for i= 0 to 255{
   j=(j+S[i]+[K] mod 256
   swap S[i] san S[j]
   }
4. Membuat *pseudorandom byte*
   i= (i+1) mod 256
   j= (j+S[i]) mod 256
   swap S[i] dan S[j]
   t=(S[i] +S[j]) mod 256
   K=S[t]

Byte K di-XOR-kan dengan *plainteks* untuk menghasilkan *cipherteks* atau di-XOR-kan dengan *cipherteks* untuk menghasilkan *plainteks*. Berikut adalah implementasi algoritma RC4 dengan mode 256 byte
Untuk mencoba kasus yang akan dibahas dan disimulasikan pembeljaraanya dalam penulisan skripsi ini adalah dengan menyajikan data sebagai berikut:

Plainteks : Amiruddin
Kunci : Manda

3.3.2 Perhitungan Iterasi Pertukaran *s-box* (*Swap*)

Hasil yang didapat setelah melakukan seluruh iterasi dari 0 s/d 255 kali iterasi dan melakukan pertukaran *s-box (swap)* adalah sebagai berikut :

77	175	31	134	235	61	164	25	133	239	70	185	51	8	119	211
68	195	57	173	14	139	15	138	3	105	228	109	237	107	214	86
228	105	236	92	225	116	254	134	251	137	37	180	65	187	74	231
123	13	140	32	194	91	242	118	15	182	84	240	121	23	195	42
203	89	252	173	89	255	146	58	240	157	72	224	141	72	250	170
71	249	185	112	37	199	126	67	255	185	96	28	230	167	102	18
211	162	107	47	224	166	122	69	14	196	143	104	56	6	193	145
111	68	23	215	172	143	105	65	6	224	200	167	132	78	45	26
254	224	175	160	136	110	66	42	32	13	248	208	189	184	170	154
119	105	105	96	85	55	46	51	47	41	16	12	22	23	258	2
16	21	24	8	17	36	46	54	43	66	80	92	85	99	127	146
163	161	180	213	237	3	6	30	68	74	101	109	138	181	215	247
4	38	86	95	132	150	189	242	30	72	95	139	194	243	34	62
112	175	229	25	58	112	180	239	40	78	137	210	18	80	123	187
9	78	145	193	6	89	163	235	32	110	198	21	98	156	235	72
156	238	45	129	227	60	147	215	48	151	245	81	154	248	100	199

Tabel 1 Hasil Pertukaran *s-box (swap)*

3.3.2 *Proses Enkripsi dan Dekripsi*

Berikutnya adalah proses membuat *pseudorandom byte* :

i= (i+1) mod 256
j=(j+S[i]) mod 256
swap S[i] dan S[j]
t=(S[i] + S[j]) mod 256
K=S[t]

Iterasi ke-1 : Plainteks(A)
i = (i + 1) mod 256
= 1
j = (j + S[i]) mod 256
= (0 + S[1]) mod 256
= (0 + 175) mod 256 = 175
Swap(S[1],S[175])

t = (S[i] + S[j]) mod 256
= (S[1] + S[175]) mod 256
= (175 + 146) mod 256

= 321 mod 256
= 65

Setelah dilakukan Perhitungan Dari Iterasi ke- 1 Menggunakan Plainteks (A), hingga Iterasi ke-9 Menggunakan Plainteks (n) maka Diperoleh Hasil Enkripsi dan Dekripsi sebagai berikut

Tabel 2 Hasil Enkripsi Plaintext "Amiruddin"

Plaintext	**Chipertext**	
A	Can	24
m	ñ	241
i	Ÿ	159
r	W	87
u	S	83
d	4	52
d	í	237
i	d	100
n	BEL	7

Tabel 3 Hasil Dekripsi Chipertext

Chipertext	**Plaintext**	
Can	A	65
ñ	m	109
Ÿ	i	105
W	r	114
S	u	117
4	d	100
í	d	100
d	i	105
Bell	n	110

4. HASIL

1. *Form Login*

Operator harus *login* untuk bisa masuk kedalam sistem, operator harus menginput *username* dan *password* dengan benar, jika *username* dan *password* salah maka akan kembali untuk melakukan *login* kembali.

Gambar 2. Tampilan *Form Login*

2. *Form* Menu Utama

Halaman ini akan tampil setelah *user* berhasil melakukan *login* ke dalam sistem. Pada halaman ini terdapat beberapa *link* seperti data gejala, data kerusakan, basis aturan dan deteksi kerusakan.

Gambar 3. Tampilan *Form* Menu Utama

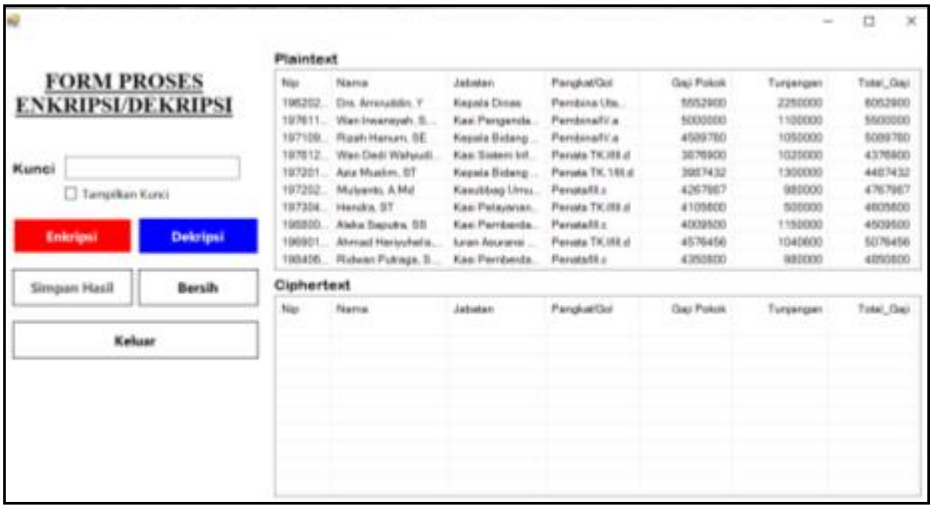
3. *Form* Input Data Gaji

Halaman ini berfungsi untuk menambahkan, mengubah , dan menghapus data gaji

Gambar 4. Tampilan *Form* Input Data Gaji

4. *Form* Proses

Halaman ini berfungsi untuk memproses data yang akan di enkripsi dan dekripsi menggunakan algoritma RC4:



Gambar 5. Tampilan *Form* Proses

Sebagai penutup pembahasan dalam penulisan penelitian ini, dapat diambil kesimpulan atas penulisan dan kemajuan sistem yang dibuat, adapun kesimpulan tersebut adalah

5. KESIMPULAN

Berdasarkan analisa permasalahan yang terjadi pada bab sebelumnya mengenai kasus yang diangkat tentang Implementasi Keamanan Data Gaji Pada Dinas Komunikasi Informatika Dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4. Maka dapat diambil kesimpulan :

1. Berdasarkan Pengujian dan Implementasi, pengaruh penerapan sistem keamanan data terhadap keamanan data gaji pada dinas komunikasi Informatika Dan Persandian Kabupaten Aceh Tamiang terlihat sangat baik, hal ini dapat dilihat dengan kemudahan dalam proses pengamanan data gaji tersebut.
2. Dengan menggunakan algoritma RC4 pengimplementasian keamanan data gaji berhasil di terapkan.

UCAPAN TERIMA KASIH

Alhamdulillah, segala puji dan syukur atas kehadirat Allah SWT, yang telah melimpahkan rahmat, taufik serta hidayah – Nya sehingga penulis masih diberikan kesehatan dan kesempatan sehingga mampu menyelesaikan jurnal ilmiah ini dengan baik. Ucapan terima kasih teristimewa ditujukan kepada orang tua, yang telah mengasuh, membesarkan dan selalu memberikan doa, motivasi serta pengorbanan baik bersifat moril maupun materil yang tidak terhingga selama menjalani pendidikan. Ucapan terima kasih yang sebesar-besarnya juga ditujukan terutama kepada Bapak Rudi Gunawan, SE., M.Si., selaku Ketua Sekolah Tinggi Manajemen Informatika Dan Komputer (STMIK) Triguna Dharma Medan. Bapak Dr.Zulfian Azmi, ST., M.Kom., selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan. Bapak Marsono, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan. Bapak Nurcahyo Budi Nugroho, S.Kom., M.Kom, selaku Dosen Pembimbing I yang telah memberikan saran, arahan dan dukungannya serta motivasi, sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Bapak Rico Imanta Ginting, S.Kom, M.Kom selaku Dosen Pembimbing II yang telah memberikan bimbingan tata cara penulisan, saran dan motivasi sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu.

DAFTAR PUSTAKA

[1] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016.

[2] K. Kirman, "Implementasi Algoritma Rc4 Untuk Proteksi File Mp3," *Pseudocode*, vol. 5, no. 1, pp. 80–86, 2018.

[3] P. S. Ke-, "PENDAHULUAN PHP telah mengalami perkembangan pesat baik dari segi fungsi maupun penggunanya. Berkembangnya PHP tidak lain karena bahasa pemrograman ini mempunyai beberapa keunggulan. Terutama karena sifatnya yang gratis dan," pp. 113–120, 2014.

[4] D. Putra *et al.*, "Implementasi Algoritma RC4 dan Playfair Cipher untuk Menggunakan Data Teks," *J. Pelita Inform.*, vol. 16, pp. 328–334, 2017.

[5] D. Atmodjo, "Peningkatan Keamanan Data dengan Metode Cropping Selection Pseudorandom," vol. 4, no. 3, pp. 132–138, 2016.

[6] N. B. Nugroho, "Aplikasi Keamanan Email Menggunakan Algoritma Rc4," *J. SAINTIKOM*, vol. 15, no. ISSN : 1978-6603, pp. 81–88, 2016.

[7] E. S. Aes, R. Cipher, R. C. Dan, and C. Cipher, "a. Aplikasi ini dibuat menggunakan bahasa pemrograman PHP. b. Username dan password untuk masuk ke aplikasi ini menggunakan akun Gmail. c. Algoritma AES dan RC4 digunakan untuk mengenkripsi isi pesan dan lampiran. d. Algoritma Caesar Cipher digunakan untu," vol. 4, pp. 273–278, 2018.

[8] S. Suhardi, "Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-or (Xor)," *Teknovasi*, vol. 3, no. 2, pp. 23–31, 2016.

[9] R. Munir, "Algoritma Kriptografi Klasik," *Algoritm. Kriptografi Klas.*, pp. 0–18, 2004.

[10] Sumandri, "Studi Model Algoritma Kriptografi Klasik dan Modern," *Semin. Mat. dan Pendidik. Mat. UNY*, pp. 265–272, 2017.

[11] K. Kirman, "Implementasi Algoritma Rc4 Untuk Proteksi File Mp3," *Pseudocode*, vol. 5, no. 1, pp. 80–86, 2018, doi: 10.33369/pseudocode.5.1.80-86.

[12] "SKRIPSI oleh : DEWI CHUMAIROH IMPLEMENTASI ALGORITMA RC4 PADA APLIKASI SMART," 2014.

BIOGRAFI PENULIS

Nama	:	Muhammad Haris Hrp
E-mail	:	Mhdharis479@gmail.com
T.T.L	:	Sungai Liput, 19 Maret 1998
Program Studi	:	Sistem Informasi
Mobile	:	0812-6042-4348

Nama	:	Nurcahyo Budi Nugroho, S.Kom, M.Kom
NIDN	:	0130038201
Dosen Tetap Stmik Triguna Dharma Medan		

Nama	:	Rico Imanta Ginting, S.Kom, M.Kom
NIDN	:	0102029002
Dosen Tetap Stmik Triguna Dharma Medan		