Jurnal CyberTech
Vol.x. No.x, Mei 2019, pp. xx~xx
P-ISSN :
E-ISSN :

Implementasi Keamanan Data Anggaran Pada Dinas KesehatanKabupaten Deli Serdang Menggunakan Algoritma RC4

Ma'ruf Rohadi M*, **Nurcahyo Budi Nugroho, S.Kom, M.Kom** **, **Fifin Sonata, S.Kom, M.Kom** **
*Program Studi Sistem Informasi, STMIK Triguna Dharma
** Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:

Keyword:
Pelaksanaan Data Anggaran Dinas Kesehatan Kabupaten Deli Serdang, keamanan, Kriptografi Rivest Code 4 (RC4)

ABSTRACT

Daftar Isian Pelaksanaan Anggaran (DIPA) adalah dokumen pelaksanaan anggaran yang disusun oleh Kementerian Negara/Lembaga dan disahkan oleh Dirjen Perbendaharaan atau Kepala Kanwil Ditjen Perbendaharaan atas nama Menteri Keuangan selaku Bendahara Umum Negara (BUN). DIPA merupakan data penting yang menjadi sebuah rahasia dalam pemerintahan. Maka sudah harus memperhatikan aspek keamanan dari data-data tersebut.

Untuk mengatasi masalah diatas, maka dibuatlah sebuah program untuk Mengamankan Data Daftar Isian Pelaksanaan Anggaran Dinas Kesehatan Kabupaten Deli Serdang Menggunakan Metode RC4. Metode ini memiliki tingkat keamanan yang cukup sulit untuk di dekripsikan. Sehingga mampu meningkatkan kerahasiaan data Daftar Isian Pelaksanaan Anggaran pada Dinas Kesehatan Kabupaten Deli Serdang.

Hasil yang diharapkan yaitu sebuah program dengan metode Rivest Code 4 ini dapat membantu dalam pengamanan Daftar Isian Pelaksanaan Anggaran Dinas Kesehatan Kabupaten Deli Serdang sehingga dapat mengamankan data tersebut.

Corresponding Author:

Nama : Ma'ruf Rohadi Muriana
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-mail : **marufrohadi8@gmail.com**

1. PENDAHULUAN

Penggunaan sistem informasi untuk membantu kinerja organisasi semakin dibutuhkan. Dengan dukungan dari kecanggihan teknologi informasi, telah memungkinkan pengembangan sistem informasi yang semakin handal. Informasi merupakan salah satu sumber daya penting dalam manajemen modern. Banyak keputusan strategis yang bergantung kepada informasi.

Sistem manajemen basis data adalah suatu kumpulan dari data yang saling terhubung dan suatu program yang dapat mengakses data tersebut[1]. Basis data mengandung informasi yang sesuai dengan kebutuhan organisasi yang

menggunakannya. Tujuan utama dari sistem manajemen basis data yaitu untuk menyediakan jalan untuk menyimpan dan mendapatkan kembali informasi pada basis data dengan aman dan efisien.

Maka dalam penulisan skripsi ini dipilih cara kedua, salah satunya dengan cara mengimplementasikan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Algoritma kriptografi adalah aturan untuk melakukan proses enkripsi yaitu proses menyandikan dari plainteks menjadi chiperteks dan proses dekripsi yang merupakan kebalikan dari enkripsi.Kriptografi memiliki dua konsep yaitu enkripsi dan deskripsi, enkripsi sendiri merupakan proses penyandian plainteks menjadi chipertext, sedangkan deskripsi adalah proses menggembalikan chiperteks menjadi plainteks ke semula[2].

2. KAJIAN PUSTAKA

2.1 Keamanan Data

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. 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]
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. Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah terjadinya penyangkalan terhadap pengirim atau terciptanya suatu informasi oleh pengirim pesan[4].

2.2 Kriptografi

Kriptografi Juga Merupakan Salah Satu Teknik Yang Dapat Digunakan Dalam Mengamankan Data Yang Bersifat Rahasia Atau Pribadi, Proses Transformasi Informasi Yang Berlangsung Dua Arah Yang Terdiri Dari Proses Enkripsi Dan Deskripsi Yaitu Ruang Lingkup Dari Kriptografi[5].

2.2.1 Konsep dasar Kriptografi

Untuk menjamin kerahasian dan keaslian data, maka digunakan teknik kriptografi yang melakukan tranformasi terhadap data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga[6].

2.2.2 Jenis-Jenis Kriptografi

1. Kriptografi Simetris
   Algoritma kriptografi simetris merupakan proses enkripsi dan deskripsi dilakukan dengan memakai 1 key yang sama disebut kunci privat yang terdiri dari metode-metode diantaranya data encryption standart (DES), Rivest Cipher 4 (RC4), On time Pad (OTP), Blowfish, dan sebagainya[7].
2. Kriptografi ASimetris
   Kriptografi asimetri adalah kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi lagi deskripsi.

2.3 Algoritma RC4

Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1987 oleh Ronal Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte[8].

3. Metode Penelitian

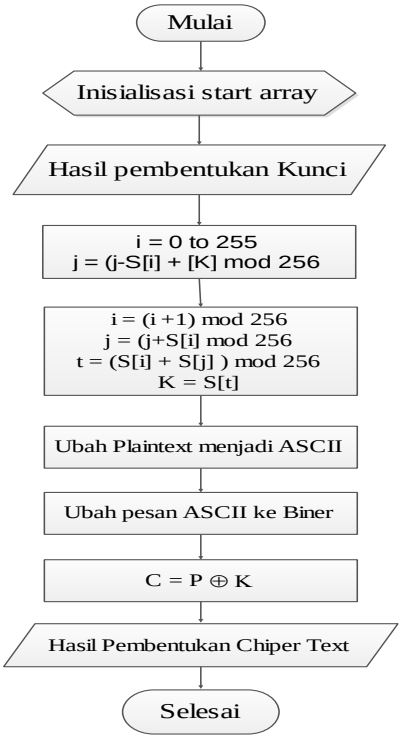
3.1 Analisa Permasalahan

Sistem keamanan data anggaran pada dinas kesehatan kabupaten deli serdang masih kurang efektif dimana istansi tersebut masih belum memiliki sistem keamanan data anggaran.

Dalam mengimplementasikan keamanan data anggaran pada Dinas Kesehatan Kabupaten Deli Serdang Menggunakan Algoritma RC4 diharapkan dapat membantu mengamankan keamanan data Anggaran 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 : Tunjangan Jabatan
Kunci : Maruf

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	35	155	5	87	190	55	180	35	122	230	100	230	90	182
39	170	49	170	11	129	9	149	19	121	244	159	48	179	30	158
48	198	78	190	67	218	117	2	119	1	157	61	207	73	216	121
30	181	52	200	110	24	180	56	209	124	43	204	85	243	163	87
253	139	46	227	156	71	218	130	60	250	170	66	239	174	113	38
195	117	57	1	187	93	20	221	170	105	16	204	154	108	48	220
157	112	71	16	193	135	95	59	9	191	138	103	72	27	214	166
136	110	70	6	219	194	173	138	79	41	21	5	231	177	144	159
148	123	74	46	36	30	10	222	199	194	193	178	189	121	121	125
115	81	68	73	82	77	48	40	50	64	64	40	37	52	71	76
57	59	79	103	113	99	106	131	160	175	166	178	208	242	6	2
19	54	93	118	119	141	181	225	255	5	32	77	126	161	172	204
254	52	84	100	137	192	251	40	61	103	163	227	21	47	94	159
228	27	58	110	180	254	58	94	151	226	49	114	155	217	41	125
195	241	52	137	226	45	96	168	2	96	176	232	53	148	247	76
137	219	63	167	1	67	154	3	112	207	22	114	224	82	182	2

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(T)
i = (i + 1) mod 256
= (0 + 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 + 2) mod 256
= 177 mod 256
= 177
Key[0] = S[177] = 54

Setelah dilakukan Perhitungan Dari Iterasi ke- 1 Menggunakan Plainteks (T), hingga Iterasi ke-17 Menggunakan Plainteks (n) maka Diperoleh Hasil Enkripsi dan Dekripsi sebagai berikut

Plaintext	Binary	Key (K)	XOR	Chipertext
T	01010100 (84)	00110110 (54)	01100010 (98)	b

Tabel 2 Hasil Enkripsi Plaintext

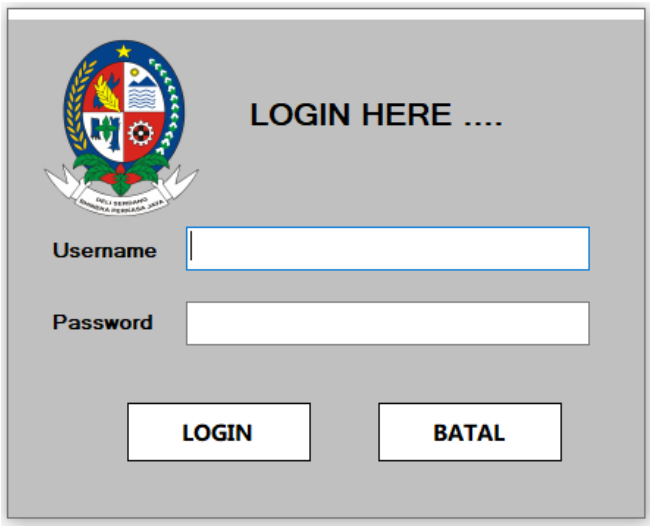
Chipertext	Binary	Key (K)	XOR	Plaintext
b	01100010 (98)	00110110 (54)	01010100 (84)	T

Tabel 3 Hasil Dekripsi Chipertext

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*

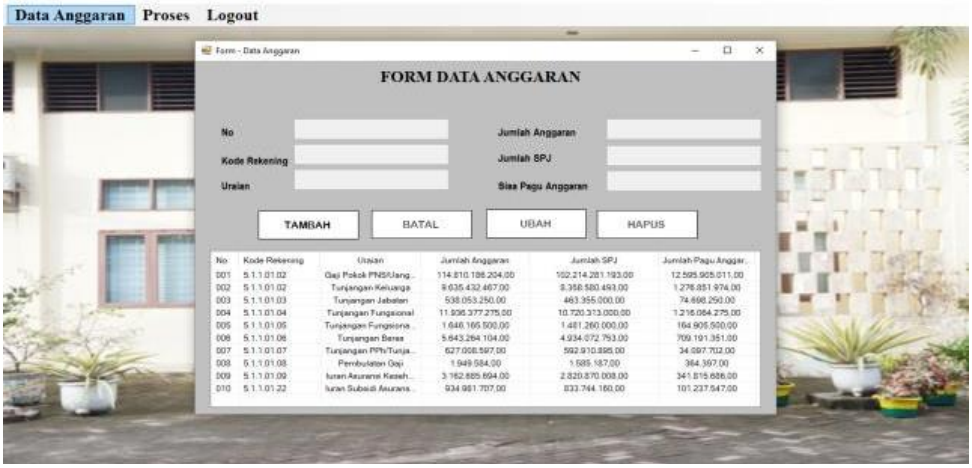
2. *Form* Menu Utama

Halaman ini akan tampil setelah *user* berhasil melakukan *login* ke dalam sistem. Pada halaman ini terdapat beberapa *link* seperti data Anggaran Proses Enkripsi Dan Dekripsi.

Gambar 3. Tampilan *Form* Menu Utama

3. *Form* Input Data Anggaran

Halaman ini berfungsi untuk menambahkan, mengubah , menambah dan menghapus data Anggaran



Gambar 4. Tampilan *Form* Input Data Gaji

4. *Form* Enkripsi
   Halaman ini berfungsi untuk menkripsi data menggunakan algoritma RC4:

Gambar 5. Tampilan *Form* Enkripsi

5. *Form* Dekripsi
   Halaman ini berfungsi untuk mendekripsi data yang telah di amankan:

Gambar 6. Tampilan *Form* Enkripsi

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 Anggaran Pada Dinas Kesahatan kabupaten Deli Serdang Menggunakan Algoritma RC4. Maka dapat diambil kesimpulan :

1. Berdasarkan pengujian dan implementasi, pengaruh penerapan sistem keamanan data terhadap keamanan data anggaran pada Dinas Kesehatan Kabupaten Deli Serdang terlihat sangat baik, hal ini dapat dilihat dengan kemudahan dalam proses pengamanan data anggaran tersebut.
2. Dalam menangani masalah keamanan data digunakan metode RC4, pengguna menginput beberapa data berupa susunan anggaran dan data anggaran.
3. Dengan menggunakan algoritma RC4 pemecahan masalah dalam mengamankan data anggaran berhasil diterapkan.

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. Fifin Sonata, 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] *Database System Concepts*, 4th Editio. New York: Silberschatz, A., H.F. Korth, Dan S. Sudarshan, 2002.

[2] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[3] M. Syahril and H. Jaya, "Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4," *Semin. Nas. Sains Teknol. Inf.*, pp. 505–509, 2019.

[4] R. N. Ibrahim, "PERANGKAT LUNAK KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI SIMETRI TINY ENCRIPTION ALGORITHM (TEA) Data security is one of the most important aspects in information technology . With a high level of security , it is expected that the information pr," vol. 13, no. 1, pp. 1–10, 2019.

[5] M. Diana and T. Zebua, "Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS," no. 1, pp. 12–22, 2018.

[6] B. Setiaji, "Analisis Dan Implementasi Algoritma Kriptografi Kunci Publik Rsa Dan Luc Untuk Penyandian Data," *Data Manaj. dan Teknol. Inf.*, vol. 16, no. 3, p. 27, 2015.

[7] B. Dan and A. Rsa, "ANALISIS PERFORMA KRIPTOGRAFI HYBRID ALGORITMA PENDAHULUAN Keamanan informasi merupa-kan salah satu masalah penting , seiring dengan perkembangan software dan pengguna internet . Keamanan komputer berhubungan dengan pencegahan dari pencurian data atau inf," vol. VI, no. 1, 2019.

[8] S. Subhan, S. Amini, and F. Ariyani, "Implementasi Pengamanan Data Enkripsi Sms Dengan Algoritma Rc4 Berbasis Android," *Semin. Nas. Inov. Dan Apl. Teknol. Di Ind. 2017*, pp. 1–6, 2017.

BIOGRAFI PENULIS

Nama	:	Ma'ruf Rohadi Murian
E-mail	:	marufrohadi8@gmail.com
T.T.L	:	Langsa, 07 Juni 1998
Program Studi	:	Sistem Informasi
Mobile	:	0852-7058-1661

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

Nama	:	Fifin Sonata, S.Kom, M.Kom
NIDN	:	0124128202
Dosen Tetap Stmik Triguna Dharma Medan		