KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Vol. 2, No. 3, Juli (2021), pp. 174-181

Implementasi Revest Code 4 (RC4) Untuk Data Resep Obat Di RSUP H.Adam Malik

Jaka Prayudha[1], Oris Krianto Sulaiman[2], Ita Mariami[3], Jufri Halim[4]
[1,3,4] STMIK Triguna Dharma, [2]Universitas Islam Sumatera Utara
[1]jakaprayudha3@gmail.com

Abstract

Advances in technology will run in accordance with advances in science which will get information easily and quickly. This is supported by information and communication technology which is growing rapidly from year to year. An example is in the management of drug data which is considered very important at H. Adam Malik Hospital. Where the possibility of falsification of drug data and not according to the availability of the number and type according to the needs due to the weakness of the system used. Seeing the existing problems is a consideration for choosing a cryptographic algorithm. Cryptography is based on an information coding algorithm that supports the needs of two aspects of information security, namely the protection of the confidentiality of information data and the protection against falsification of information. Rivest Code 4 (RC4) is one of the methods used to encode text messages in securing drug redemption data for research at H.Adam Malik Hospital. Implementation of Cryptography Implementation in Encoding Drug Redemption Data at H. Adam Malik Hospital Using the Rivest Code 4 (RC4) Method, carried out in two processes, namely the encryption process and the decryption process on the drug redemption data, where the original data (plaintext) entered can be encrypted into encoded data (ciphertext) and can be returned to the original data back as before with the decryption process.

Keywords: *Computer Security, Revest Code 4, Drug Prescription*

Abstrak

Kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan yang akan mendapatkan informasi dengan mudah dan cepat. Hal ini didukung oleh teknologi informasi dan komunikasi yang berkembang pesat dari tahun ke tahun. Contohnya dalam pengelolaan data obat yang dianggap sangat penting di RS H. Adam Malik. Dimana kemungkinan terjadi pemalsuan data obat dan tidak sesuai dengan ketersediaan jumlah dan jenis sesuai kebutuhan karena kelemahan sistem yang digunakan. Melihat permasalahan yang ada menjadi pertimbangan untuk memilih algoritma kriptografi. Kriptografi didasarkan pada algoritma pengkodean informasi yang mendukung kebutuhan dua aspek keamanan informasi, yaitu perlindungan kerahasiaan data informasi dan perlindungan terhadap pemalsuan informasi. Rivest Code 4 (RC4) merupakan salah satu metode yang digunakan untuk mengkodekan pesan teks dalam mengamankan data penebusan obat untuk penelitian di Rumah Sakit H.Adam Malik. Implementasi Implementasi Kriptografi Dalam Pengkodean Data Tebusan Obat Di RS H. Adam Malik Menggunakan Metode Rivest Code 4 (RC4), dilakukan dalam dua proses yaitu proses enkripsi dan proses dekripsi pada data penebusan obat, dimana data asli (plaintext) yang dimasukkan dapat dienkripsi menjadi data yang disandikan (ciphertext) dan dapat dikembalikan ke data aslinya kembali seperti semula dengan proses dekripsi.

Kata kunci: *Keamanan Komputer, Revest Code 4, Resep Obat*

1. Introduction

Kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan yang dimana akan mendapatkan sebuah informasi dengan mudah dan cepat. Hal ini didukung

ISSN: 2720-992X

dengan teknologi informasi dan komunikasi yang berkembang pesat dari tahun ke tahun. Serta sumber daya manusia merupakan faktor yang mendukung kemajuan sebuah teknologi [1]. Dalam hal ini informasi sering disalah gunakan oleh orang-orang yang tidak bertanggung jawab. Sebagai contohnya adalah dalam pengelolaan data obat yang dianggap sangat penting pada RSUP H. Adam Malik. Dimana kemungkinan adanya pemalsuan data obat dan tidak sesuai ketersediaan jumlah dan jenis sesuai dengan kebutuhan karena adanya kelemahan sistem yang digunakan. Kemajuan teknologi yang sangat cepat mendorong setiap instansi untuk mengikuti perkembangan teknologi dan meningkatkan kemampuan dalam mengelola data-data dan informasi yang lebih aman, akurat dan efesien dalam mendukung kebutuhan informasi yang akan membantu manajemen RSUP H.Adam Malik dalam meningkatkan pelayanan obat-obatan. Dengan suatu sistem informasi maka pengelolaan data akan lebih mudah dan efesien [2].

Melihat permasalahan yang ada menjadi pertimbangan untuk memilih sebuah algoritma kripgorafi yang akan digunakan dalam penyusunan skripsi ini, kriptografi berbasis pada algoritma pengkodean informasi yang mendukung kebutuhan dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data infromasi dan perlindungan terhadap pemalsuan informasi. Rivest Code 4 (RC4) merupakan salah satu metode yang digunakan untuk menyandikan pesan teks dalam pengamanan data penebusan obat yang akan dilakukan penelitian pada RSUP H.Adam Malik. Dari pembahasan ini maka dibuatlah sebuah teknik pengamanan data dengan cara melakukan enkripsi dan deskripsi sehingga hanya dapat diakses pihak tertentu.

2. Metodologi Penelitian

2.1. Kriptografi

Kata kriptografi berasal dari Bahasa yunani. Dalam Bahasa yunani kriptografi terdiri dari buah kata yaitu cryptos dan graphia. Kata crypto berarti rahasia sedangkan graphia berarti tulisan.[3] Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Kata seni tersebut berasal dari fakta sejarah pada masa-masa awal sejarah kriptografi, setiap orang mempunyai cara yang unik untuk merahasiakan pesan. Untuk menjaga pesan, maka pesan tersebut diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain. Enkripsi merupakan proses penyandian yang dilakukan pengkodean data yang dapat dipahami (plainteks) menjadi sebuah kode yang tidak dapat dimengerti (cipherteks). Sedangkan proses kebalikannya mengubah cipherteks menjadi plainteks disebut deskripsi [4].

2.2. Revest Code 4

Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu : Rivest shamir Adleman). Kunci enkripsi didapat dari sebuat 256 bit state-array (KSA) yang diinisialisasi dengan sebuah key tersendiri dengan panjang 1-256 bit. Dimana state-array tersebut akan diacak kembali dan diproses untuk menghasilkan sebuah kunci enkripsi yang akan di-XOR-kan dengan plainteks ataupun cipherteks. Masing-masing elemen yang terdapat dalam tabel saling ditukarkan minimal sekali [3][4].

2.3. Resep Obat

Obat resep (juga obat resep atau obat resep) adalah obat farmasi yang secara hukum memerlukan resep medis untuk dibagikan. Sebaliknya, obat bebas dapat diperoleh tanpa resep dokter. Alasan untuk perbedaan ini dalam pengendalian zat adalah potensi ruang lingkup penyalahgunaan, dari penyalahgunaan obat-obatan ke praktek kedokteran tanpa lisensi dan tanpa pendidikan yang memadai. Yurisdiksi yang berbeda memiliki definisi yang berbeda tentang apa yang merupakan obat resep [2].

3. Hasil dan Pembahasan

3.1. Analisa Data

Pada permasalahan ini, data yang akan di enkripsi dan deskripsi yaitu berupa nama pasien, nama obat, jenis dan data lainnya yang ada di RSUP H. Adam Malik dalam bentuk file. Pada proses enkripsi dan deskripsi untuk membuat data atau informasi agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali pihak yang berhak untuk melihat dan mengetahuinya. Dalam hal ini maka perlu dibutuhkan aplikasi yang dapat menjaga keamanan data yaitu dengan menerapkan metode Rivest Code 4 sebagai salah satu bentuk keamanan data:

a) Proses inisialisasi S-Box (*Array* S)
for i = 0 to 255
S[i] = i

b) Proses inisialisasi S-Box (*Array* K)
For = 0 to 255
S[i] = i

c) Kemuian lakukan langkah pengacakan S-Box
I= 0; j=0
For i=0 to 255
{
j=(j+S[i]+[k]) mod 256
swap S[i] dan S[j]
}

d) 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]

e) 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 256 byte.

1) Inisialisasi S-Box dengan panjang 256 byte. Dengan S[0]=0, S[1]=1, S[2]=2, S[3]=3, …, S[255]=255 sehingga array S menjadi :

Tabel 1. Inisialisasi S-Box dengan panjang 256 *byte*

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191

192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

2) Inisialisasi 7 *byte* kunci *array* Ki, Misalkan kunci terdiri dari 7 *byte* yaitu "BINECAP" maka kalimat akan diubah kedalam bentuk Desimal "68 73 78 69 67 65 80". Ulangi kunci sampai memenuhi seluruh *array* K sehingga *array* K menjadi:

Tabel 2. Inisialisasi 4 *byte* Kunci *Array* Ki

Iterasi-1	Key-char	Key[i]	S-Box[i]
0	B	68	0
1	I	73	1
2	N	78	2
3	E	69	3
4	C	67	4
5	A	65	5
6	P	80	6
….	….	….	….
….	….	….	….
….	….	….	….
255	B	68	254
256	I	73	255

3) Berikutnya mencapur operasi dimana akan menggunakan variabel i dan j ke *index array* S[i] dan K[i]. pertama kita beri inisial untuk i dan j dengan 0. Operasi pencampuran adalah pengulangan rumusan (j + S[i] + K[i]) mod 256 yang akan diikuti dengan penukaran S[i] dengan S[j]. untuk contoh ini, karena kita mneggunakan *array* dengan pajang 256 *byte* maka algoritma menjadi

For I = 0 to 256
J= (j + S[i] + K[i]) mod 256
Swap S[i] dan S[j]

Dengan algoritma seperti di atas maka dengan nilai awal i=0 sampai i= 255 akan menghasilkan *array* S seperti berikut ini :

Iterasi ke-1 :
I= 0, maka
J= (j + S[i] + K[i]) mod 256
=(j + S[0] + S[0]) mod 256
=(0 + 0 + 66) mod 256
= 66
Swap S[0] dan S[66]
Iterasi ke-2 :
I= 1, maka
J= (j + S[i] + K[i]) mod 256
=(j + S[1] + S[1]) mod 256
=(66 + 1 + 73) mod 256
= 140
Swap S[1] dan S[140]
Iterasi ke-3 :
I= 1, maka
J= (j + S[i] + K[i]) mod 256

=(j + S[2] + S[2]) mod 256
=(140 + 2 + 78) mod 256
= 220
Swap S[2] dan S[220]
Iterasi ke-4 :
I= 1, maka
J= (j + S[i] + K[i]) mod 256
=(j + S[3] + S[3]) mod 256
=(220 + 3 + 69) mod 256
= 36
Swap S[3] dan S[36]
Iterasi ke-5 :
I= 1, maka
J= (j + S[i] + K[i]) mod 256
=(j + S[4] + S[4]) mod 256
=(36 + 4 +67) mod 256
= 107
Swap S[4] dan S[107]
Iterasi ke-6 :
I= 1, maka
J= (j + S[i] + K[i]) mod 256
=(j + S[5] + S[5]) mod 256
=(107 + 5 +65) mod 256
= 177
Swap S[5] dan S[177]
…
…
…
Iterasi ke-255 :
I= 1, maka
J= (j + S[i] + K[i]) mod 256
=(j + S[254] + S[254]) mod 256
=(17 + 95 + 78) mod 256
= 190
Swap S[254] dan S[190]
Iterasi ke-256 :
I= 1, maka
J= (j + S[i] + K[i]) mod 256
=(j + S[255] + S[255]) mod 256
=(190 + 255 + 69) mod 256
= 2
Swap S[255] dan S[2]

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

Tabel 3. Hasil pertukaran *S-box* (*swap*)

66	212	255	36	107	34	233	51	24	83	69	148	225	62	166	230
248	253	239	90	167	254	93	85	31	231	214	65	209	35	113	206
49	25	29	237	132	130	117	189	43	2	72	6	54	168	50	55
247	4	178	127	38	88	197	76	198	84	208	191	207	245	99	164
192	12	98	10	193	71	234	122	140	136	159	45	249	174	158	153
131	173	180	238	121	92	163	14	60	105	37	176	94	185	112	39
28	139	146	169	241	162	108	183	111	70	118	126	149	78	144	172

194	235	133	77	110	13	211	26	151	42	221	96	246	171	202	40
53	199	157	97	182	216	138	250	143	86	145	155	41	251	87	229
204	20	218	115	104	184	177	156	119	242	210	3	23	81	89	125
252	30	17	187	188	21	142	32	44	64	129	205	224	47	18	195
215	80	15	103	170	200	46	79	73	82	33	56	179	91	95	201
22	175	8	101	227	109	134	0	196	5	217	120	19	243	160	57
141	74	48	9	128	124	213	232	114	228	11	100	67	161	61	27
236	150	75	16	1	244	52	59	165	116	102	226	219	106	152	181
190	240	63	203	7	186	135	223	68	137	222	154	147	58	123	220

4) Berikutnya adalah proses *enkripsi* yaitu meng-XOR-kan *pseudo random byte* dengan *plainteks*, misalnya *plainteks* dari "NURASIAH". *Plainteks* terdiri dari 8 karakter maka terjadi 8 iterasi. Sebelum di-iterasi, ubah karakter menkadi bentuk bilangan *binner*.

Tabel 4. Tabel Binner *Plainteks*

Character	Desimal	Binner
N	78	01001110
U	85	01010101
R	82	01010010
A	65	01000001
S	83	01010011
I	73	01001001
A	65	01000001
H	72	01001000

Pada permasalahan ini, data yang akan di enkripsi dan deskripsi yaitu berupa nama pasien, nama obat, jenis dan data lainnya yang ada di RSUP H. Adam Malik dalam bentuk file. Pada proses

Tabel 5. Enkripsi

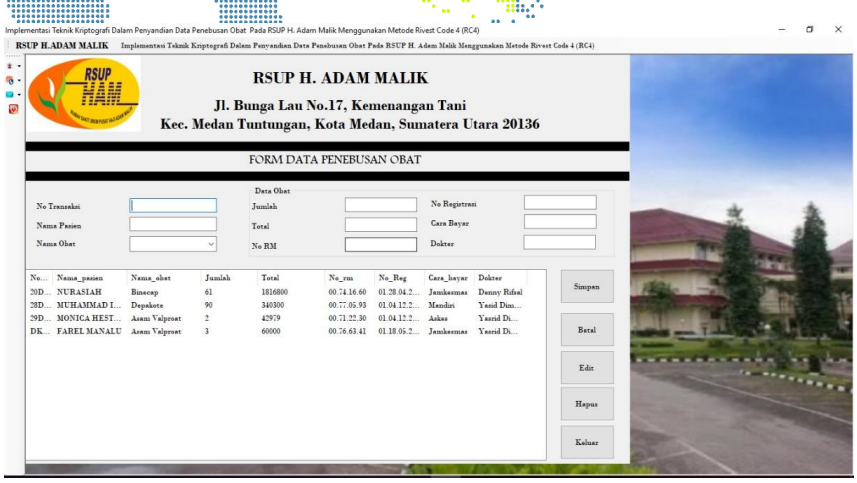
Iterasi	Plainteks			Key (K)	XOR	Cipherteks	
1	N	78	01001110	01111001	00110111	55	7
2	U	85	01010101	00011000	01001101	77	M
3	R	82	01010010	11011111	10001101	141	
4	A	65	01000001	00111010	01111011	123	{
5	S	83	01010011	10000101	11010110	214	Ö
6	I	73	01001001	01001100	00000101	5	.
7	A	65	01000001	00110111	01110110	118	v
8	H	72	01001000	10001011	11000011	195	Ã

Tabel 6. Dekripsi

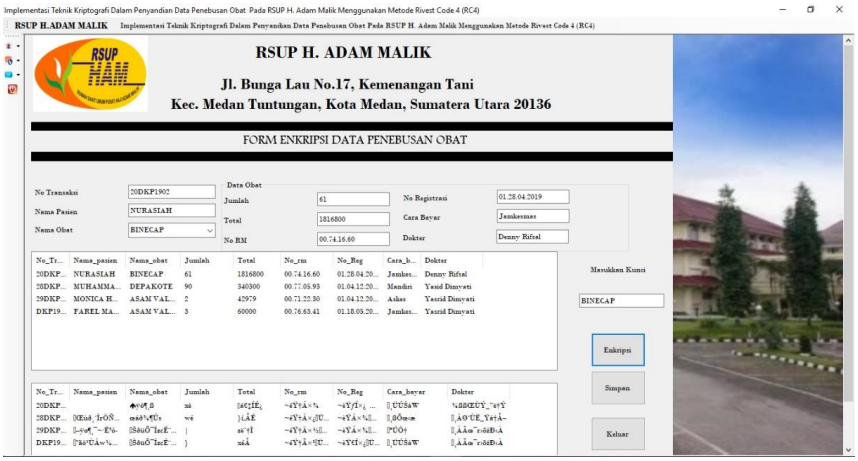
Iterasi	Cipherteks			Key (K)	XOR	Plainteks	
1	7	55	00110111	01111001	01001110	78	N
2	M	77	01001101	00011000	01010101	85	U
3		141	10001101	11011111	01010010	82	R
4	{	123	01111011	00111010	01000001	65	A
5	Ö	214	11010110	10000101	01010011	83	S
6	.	5	00000101	01001100	01001001	73	I
7	V	118	01110110	00110111	01000001	65	A
8	Ã	195	11000011	10001011	01001000	72	H

3.2. Hasil

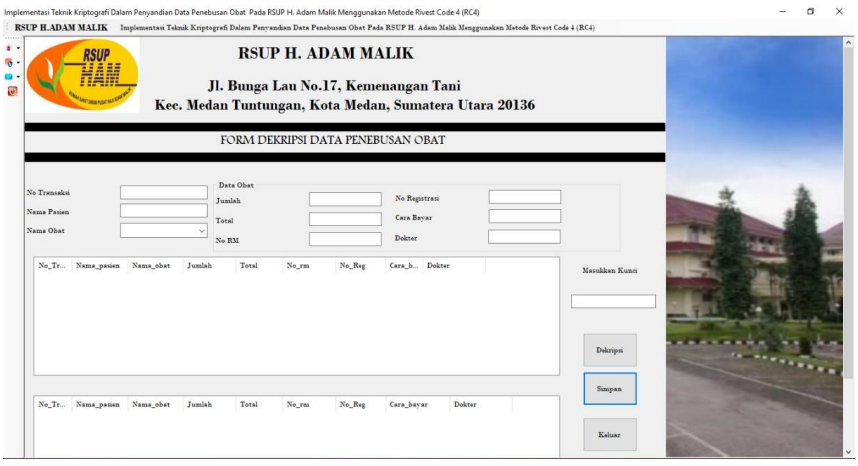
Implementasi RC 4 untuk pengamanan informasi data resep pasien di RSUP H Adam Malik dilakukan dengan menggunakan platform desktop application dengan hasil sebagai berikut :



Gambar 1. *Form* Data Resep Obat



Gambar 2. *Form* Enkripsi



Gambar 3. *Form* Dekripsi

4. Kesimpulan

Penerapan Implementasi Kriptografi Dalam Penyandian Data Penebusan Obat Pada RSUP H. Adam Malik Menggunakan Metode Rivest Code 4 (RC4), dilakukan dengan dua proses, yaitu proses pengenkripsian dan proses pendekripsian pada data penebusan obat, yang mana data asli (plainteks) yang diinputkan dapat dienkripsi menjadi data yang disandikan (cipherteks) dan dapat dikembalikan menjadi data asli kembali seperti semula dengan proses dekripsi.

Daftar Pustaka

[1] I. S. Sabana and L. Tanti, "Pengembangan Model Keamanan Data Inventory Dengan," *J. FTIK*, vol. 1, no. 1, pp. 607–618, 2020.

[2] N. Tanjung, "Perancangan Sistem Informasi Data Rekam Medis Pasien Rawat Jalan Pada Klinik Utama Al-Basyariah Citayam," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 4, no. 1, pp. 119–124, 2018, [Online]. Available: http://ejournal.nusamandiri.ac.id/index.php/jitk/article/view/454/400.

[3] G. Ammary and S. Mulyati, "Aplikasi Kriptografi Untuk Keamanan Databse Dengan Metode Rc4 Dan Elgamal Berbasis Web Pada Jxl Design Co," *Skanika*, vol. 1, no. 2, pp. 815–820, 2018.

[4] W. H. Haji and S. Mulyono, "Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data," *Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data*, vol. 2012, no. Snati, pp. 15–16, 2012, [Online]. Available: e-mail:wahyuhari@gmail.com,slamet_mulyono@yahoo.com.