CESS
(Journal of Computing Engineering, System and Science) 8(1) January 2023 60-70
e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess

Pengamanan Data Transaksi Menggunakan AES dan RC4

Transaction Data Security Using AES and RC4

Puji Sari Ramadhan*[1], Muhammad Syahril[2], Rini Kustini[3], Hendryan Winata[4], Robin Darwis Gea[5]

[1,2,3,4] STMIK Triguna Dharma
Jl. AH Nasution No.73, 20142, Medan, Indonesia

email: [1]pujisariramadhan@gmail.com, [2]nakmuda@gmail.com, [3]rinikustini73@gmail.com, [4]hendryan.tgd@gmail.com , [5]robin_darwin@gmail.com

A B S T R A K

Penelitian ini membahas tentang efektifitas penggunaan AES (Anvanced Encryption Standard) dan RC4 (Rivest Chiper 4) sebagai algoritma dari pengamanan data digital untuk mencegah dan melindungi data transaksi dari pihak-pihak yang tidak bertanggung jawab. Hal ini perlu dilakukan karena perkembangan transaksi penjualan atau layanan lainnya telah banyak menggunakan teknologi digital. Keadaan tersebut menyebabkan perlunya melakukan pengamanan data digital dari transaksi yang ada, agar data transaksi dapat tersimpan dengan aman. Pengamanan data transaksi dilakukan dengan cara melakukan perubahan data kedalam bentuk sandi atau kode-kode yang sulit dibaca dengan menggunakan algoritma AES (Anvanced Encryption Standard) dan RC4 (Rivest Chiper 4). Penelitian ini dimulai dengan mengumpulkan data-data transaksi yang ada kemudian ditransformasikan kedalam kode ASCII. Hasil dari transformasi tersebut akan digunakan untuk melakukan perhitungan dengan menggunakan algoritma AES. Setelah selesai melakukan proses perhitungan dengan menggunakan algoritma AES, maka selanjutnya melakukan perhitungan dengan menggunakan RC4. Hasil inilah yang akan disimpan kedalam basis data sehingga data transaksi yang sudah berubah menjadi kode-kode tersebut tidak dapat diketahui oleh pihak lainnya. Kombinasi algoritma AES dan RC4 ini dilakukan untuk memperkuat enkripsi data yang dilakukan dikarenakan sistem perputarannya yang semakin banyak dan pengamanan ganda yang dilakukan agar data digital tersebut tidak mudah terbaca dan disalahgunakan. Dengan hadirnya penelitian ini dapat diperlihatkan bahwa algoritma AES dan RC4 mampu melakukan enskripsi data transaksi yang ada dengan tingkat pengamanan yang berlapis.

Kata Kunci: *Data Digital, Pengamanan Data, Kriptografi, AES, RC4*

A B S T R A C T
This study discusses the effectiveness of using AES (Advanced Encryption Standard) and RC4 (Rivest Chipper 4) as digital data security algorithms to prevent and protect transaction data from irresponsible parties. This needs to be done because the development of sales transactions or other services has used digital technology a lot. This situation causes the need to secure digital data from existing transactions, so that transaction data can be stored safely. Transaction data security is carried out by changing data into ciphers or codes that are difficult to read using the AES (Advanced Encryption Standard) and RC4 (Rivest Cipher 4) algorithms. This research begins by collecting existing transaction data and then transforming it into ASCII code. The results of the transformation will be used to perform calculations using the AES algorithm. After completing the calculation process using the AES algorithm, then do the calculations using RC4. These results will be stored in the database so that the transaction data that has turned into these codes cannot be known by other parties. The combination of the AES and RC4 algorithms is carried out to strengthen data encryption because there are more and more rotation systems and double security is carried out so that digital data is not easily read and misused. With the presence of this research, it can be shown that the AES and RC4 algorithms are capable of encrypting existing transaction data with multiple levels of security.

Keywords: *Digital Data, Data Security, Cryptography, AES, RC4*

---

1. PENDAHULUAN

Pentingnya pengamanan data transaksi dalam penyimpanan digital, hal tersebut dilakukan untuk mencegah terjadinya pecurian data dan informasi yang disimpan oleh pihak yang tidak bertanggung jawab. Saat ini penggunaan data digital telah banyak tersebar di lingkungan masyarakat dengan berbagai macam sektor, seperti : data penjualan, data pribadi, data kesehatan dan lainnya. Hal tersebut yang mendorong penelitian ini untuk mencoba menyelesaikan permasalahan dalam pengamanan data.

Pengamanan data yang dilakukan dalam penelitian ini akan menggunakan konsep kriptografi. Untuk konsep kriptografi itu sendiri merupakan bidang keilmuan yang telah banyak digunakan dalam penelitian sebelumnya untuk pengamanan data seperti : pengamanan data deposito nasabah[1], kemudian pengamanan data nilai yang dimiliki oleh siswa[2], dan pengamanan data pelanggan[2].

Penggunaan kriptografi dalam melakukan pengamanan data dinilai efektif untuk mencegah data yang dimasukkan atau disimpan dapat dimodifikasi oleh pihak yang tidak bertanggung jawab. Dalam penelitian ini kasus utama yang menjadi masalah adalah melakukan pengamanan data transaksi agar data dan informasi tersebut tidak dapat dibaca dan diakses oleh pihak lainnya. Berdasarkan hal tersebut maka dibutuhkanlah sebuah algoritma yang mampu melakukan enkripsi data agar data yang dimiliki dapat tersimpan dengan aman. Diantara algoritma dari konsep kriptografi yang memiliki kemampuan dalam melakukan enkripsi dan telah banyak digunakan dalam pengamanan data digital adalah AES (Anvanced Encryption Standard) dan RC4 (Rivest Chiper 4).

Kedua metode tersebut berhasil melakukan enkripsi data, hal ini terlihat dari penelitian sebelumnya yang menggunakan algoritma AES dalam penelitiannya, seperti : pengamanan data login E-Commerce[3], kemudian pengamanan data layanan cloud computing[4] dan

pengamanan pesan singkat[5]. Selain itu terdapat penelitian lainnya yang memaparkan tentang efektifitasnya penggunaan algoritma RC4 (Rivest Chiper 4) dalam pengamanan data, diantaranya : pengamanan data mahasiswa[6], dan pengamanan data arsitektur[7].

Dengan hadirnya algoritma AES dan RC4, maka dalam penelitian ini akan dilakukan penggabungan atau kombinasi algoritma untuk melakukan pengamanan data transaksi. Kemudian dapat dijadikan sebuah konsep untuk pengamanan data-data lainnya seperi hasil diagnosa kesehatan, data perbankan, perusahaan dan lainnya[8]. Hal ini dilakukan untuk memperkuat enkripsi data yang dilakukan dikarenakan sistem perputarannya yang semakin banyak dan pengamanan ganda yang dilakukan agar data digital tersebut tidak mudah terbaca dan disalahgunakan. Dengan hadirnya penelitian ini dapat diperlihatkan bahwa algoritma AES dan RC4 mampu melakukan enskripsi data transaksi yang ada dengan tingkat pengamanan yang berlapis.

2. TINJAUAN PUSTAKA

Dalam menyelesaikan permasalahan yang terjadi dalam penelitian ini maka dibutuhkan referensi yang nantinya akan menjadi rujukan dalam melakukan penelitian, rujukan tersebut meliputi tentang kriptografi, algoritma AES (Anvanced Encryption Standard) dan RC4 (Rivest Chiper 4). Berikut merupakan tinjauan pustaka dari penelitian pengamanan data transaksi dengan menggunakan algoritma AES dan RC4.

2.1. Kriptografi

Konsep kriptografi dikenal sebagai ilmu yang digunakan untuk menjaga kemananan data atau pesan dengan melakukan penyandian kedalam bentuk kode-kode yang sulit dimengerti[9]. Pendapat lainnya mengemukakan bahwa kriptografi merupakan sebuah seni dari ilmu pengamanan data atau informasi dengan menggunakan teknik tranformasi data ke dalam bentuk deretan karakter yang tidak memiliki arti[10].

2.2. Algoritma AES

AES (Anvanced Encryption Standard) adalah salah satu algoritma dalam bidang kelimuan kriptografi dengan memiliki luaran deretan data sebanyak 128 *bit*[11]. Algoritma ini dikenal sebagai algoritma kriptografi yang hadir untuk mengoptimalkan kinerja dari algoritma sebelumnya yaitu DES (Data Encryption Standard)[12]. Untuk algoritma AES (Anvanced Encryption Standard) ini termasuk kedalam jenis algoritma simetris, hal ini dikarenakan menggunakan kunci yang sama dalam proses enkripsi dan deskripsi[13].

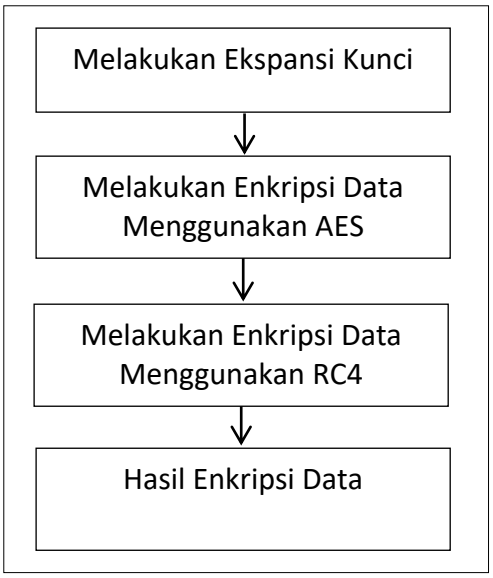
2.3. Algoritma RC4

RC4 (Rivest Chiper 4) merupakan bagian dari algoritma yang terdapat dalam bidang keilmuan kriptografi[14]. RC4 (Rivest Chiper 4) ini dikenal sebagai algoritma simetris yang modern dan memiliki kecepatan tinggi dalam dalam melakukan pengamanan data[15]. Dalam algoritma RC4 (Rivest Chiper 4) menggunakan kunci yang panjangnya dari 1 sampai dengan 256 *byte*[16].

3. METODE

Dalam menyelesaikan permasalahan yang terjadi dalam penelitian ini maka perlu menggunakan kerangka kerja penelitian yang berisi tentang alur atau tahapan kerja yang digunakan sebagai pedoman dalam menghasilkan kesimpulan dari penelitian yang

berlangsung untuk mencapai tujuan yang telah ditetapkan. Berikut merupakan kerangka kerja dari penerapan algoritma AES dan RC4 dalam pengamanan data transaksi.



Gambar 1. Kerangka Kerja Penelitian

Setelah kerangka kerja telah dibentuk maka proses selanjutnya adalah mengikuti tahapan-tahapan yang telah ditetapkan dalam kerangka kerja penelitian tersebut. Berdasarkan kerangka kerja yang telah disusun dapat diperoleh rincian tahapan sebagai berikut:

1) Melakukan Ekspansi Kunci, proses ini dilakukan untuk menghasilkan kunci yang dapat digunakan untuk melakukan proses enkripsi dan deskripsi dari suatu data serta mengawali proses dari pengamanan data.
2) Melakukan Enkripsi Data Menggunakan AES, proses ini dilakukan untuk menghasilkan sebuah kode rahasia dari sebuah informasi yang disimpan dalam basis data. Informasi atau pesan yang akan diamankan disebut dengan *plaintext*. Algoritma AES menggunakan 128-bit dengan 10 kunci ronde pada ekspansi kunci.
3) Melakukan Enkripsi Data Menggunakan RC4, proses ini dilakukan berkelanjutan setelah data tersebut telah dienkripsi oleh AES, sehingga pengamanan data dilakukan sebanyak 2 kali. Algoritma RC4 menggunakan panjang kunci yang berukuran 1 hingga 256-byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 *byte*.
4) Hasil Enkripsi Data, setelah melakukan proses enkripsi data dengan menggunakan AES dan RC4 maka dapat diperoleh hasil enkripsi data berupa tampilan kode-kode yang tersusun sehingga tidak mudah terbaca oleh pihak lainnya tanpa mengetahui kunci yang digunakan.

4. HASIL DAN PEMBAHASAN

Pada bagian ini akan ditampilkan hasil dari penerapan algoritma AES dan RC4 dalam melakukan pengamanan data transaksi berdasarkan tahapan-tahapan yang telah tersusun dalam kerangka kerja penelitian ini. Berikut merupakan hasil dari tahapan yang telah

dilakukan dalam penelitian tentang pengamanan data transaksi menggunakan algoritma AES dan RC4.

4.1. Hasil Ekspansi Kunci

Untuk kunci yang digunakan untuk menyelesaikan permasalahan ini adalah "DITOKOBUKITABADI". Berikut proses ekspansi kunci yang dilakukan:

1) Melakukan transformasi kunci ke dalam blok yang berukuran 128-bit dan diubah dalam bentuk bilangan Hexadecimal.

D	I	T	O	K	O	B	U	K	I	T	A	B	A	D	I
44	49	54	4F	4B	4F	42	55	4B	49	54	41	42	41	44	49

2) Melakukan perubahan kunci ke dalam blok 4x4 untuk membentuk *Roundkey* ke-0:

44	49	54	4F
4B	4F	42	55
4B	49	54	41
42	41	44	49

3) Setelah selesai, maka selanjutnya melakukan fungsi *RotWord*, dengan menggeser setiap bit pada kolom 4 ke atas 1 kali menggunakan *RoundKey* ke-0. Hasil tersebut akan dilakukan substitusi melalui nilai yang ada pada tabel S-Box (*SubBytes*).

4F	55	FC
55	41	83
41	49	3B
49	4F	84

4) Selanjutnya melakukan proses XOR antar kolom yang ada disetiap *RoundKey.* Sehingga diperoleh hasil dari *RoundKey* ke-1 sampai ke-10.

RoundKey ke-1

B9	F0	A4	EB
C8	87	C5	90
70	39	6D	2C
C6	87	C3	8A

RoundKey ke-2

DB	2B	8F	64
B9	3E	FB	6B
0E	37	5A	76
2F	A8	6B	E1

RoundKey ke-3

A0	8B	04	60
81	BF	44	2F
F6	C1	9B	ED
6C	C4	AF	4E

RoundKey ke-4

BD	36	32	52
D4	6B	2F	00
D9	18	83	6E
BC	78	D7	99

RoundKey ke-5

CE	F8	CA	98
4B	20	0F	0F
37	2F	AC	C2
BC	C4	13	8A

RoundKey ke-6

98	60	AA	32
6E	4E	41	4E
49	66	CA	08
FA	3E	2D	A7

RoundKey ke-7

F7	97	3D	0F
5E	10	51	1F
15	73	B9	B1
D9	E7	CA	6D

RoundKey ke-8

B7	20	1D	12
96	86	D7	C8
29	5A	E3	52
AF	48	82	EF

RoundKey ke-9

44	64	79	6B
96	10	C7	0F
F6	AC	4F	1D
66	2E	AC	43

RoundKey ke-10

04	60	19	72
32	22	E5	EA
EC	40	0F	12
19	37	9B	D8

4.2. Hasil Enkripsi AES

Plaintext yang digunakan dalam proses enkripsi ini adalah “Rp99000000000000” dimana tahapan proses enkripsinya seperti berikut ini:

1) *Plaintext* diurutkan kedalam blok kemudian diubah kedalam bentuk bilangan *hexadecimal*

R	p	9	9	0	0	0	0	0	0	0	0	0	0	0	0
52	70	39	39	30	30	30	30	30	30	30	30	30	30	30	30

2) *Plaintext* disusun kedalam *state* 4x4

52	70	39	39
30	30	30	30
30	30	30	30
30	30	30	30

3) Selanjutnya melakukan proses *AddRoundKey*, dimana *plaintext* akan di XOR-kan dengan *RoundKey* ke-0

52	70	39	39
30	30	30	30
30	30	30	30
30	30	30	30

⊕

44	49	54	4F
4B	4F	42	55
4B	49	54	41
42	41	44	49

=

16	39	6D	76
7B	7F	72	65
7B	79	64	71
72	71	74	79

4) Hasil dari *AddRoundKey* di atas akan menjadi *round* ke-1 sampai dengan round ke-10 untuk diproses dengan 4 transformasi yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey.* Berikut hasil akhir transformasi dari *round* ke-10

SubBytes

BD	BE	08	22
D1	86	38	C8
FB	35	A9	D2
5B	29	2A	85

ShiftRows

BD	BE	08	22
86	38	C8	D1
A9	D2	FB	35
85	5B	29	2A

RoundKey ke-10

04	60	19	72
32	22	E5	EA
EC	40	0F	12
19	37	9B	D8

AddRoundKey

B9	DE	11	50
B4	1A	2D	3B
45	92	F4	27
9C	6C	B2	F2

5) Dari tahapan yang telah dilakukan maka dapat diketahui hasil enkripsi dari algoritma AES adalah sebagai berikut:

B9	DE	11	50	B4	1A	2D	3B	45	92	F4	27	9C	6C	B2	F2
¹	p	◄	P	’	→	-	;	E	’	Ô	'	œ	l	²	ò

4.3. Hasil Enkripsi RC4

Setelah selesai melakukan proses enkripsi dengan menggunakan algoritma AES, maka selanjutnya melakukan proses enkripsi dengan menggunakan RC4 berdasarkan hasil dari enkripsi AES. Berikut hasil dari tahapan algoritma RC4:

Plaintext : **¹p ◄ P ’→ - ; E ’ Ô ' œ l ² Ò**
Kunci : DARWIS

1) Inisialisasi jumlah S-Box dengan panjang 256 *byte*, dimana S[0]=0, S[1]=1, S[2]=2, S[3]=3,……..S[255]=255 didapatkan array S.

Tabel 1. Array S

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 kunci array K, dimana kunci terdiri dari 6 *byte* yaitu “DARWIS” yang kemudian diubah kedalam bentuk desimal dan diulangi sampai memenuhi seluruh array K sebanyak 256 *byte*

Tabel 2. Array K

68	65	82	87	73	83	68	65	82	87	73	83	68	65	82	87
73	83	68	65	82	87	73	83	68	65	82	87	73	83	68	65
82	87	73	83	68	65	82	87	73	83	68	65	82	87	73	83
68	65	82	87	73	83	68	65	82	87	73	83	68	65	82	87
73	83	68	65	82	87	73	83	68	65	82	87	73	83	68	65
82	87	73	83	68	65	82	87	73	83	68	65	82	87	73	83
68	65	82	87	73	83	68	65	82	87	73	83	68	65	82	87
73	83	68	65	82	87	73	83	68	65	82	87	73	83	68	65
82	87	73	83	68	65	82	87	73	83	68	65	82	87	73	83
68	65	82	87	73	83	68	65	82	87	73	83	68	65	82	87
73	83	68	65	82	87	73	83	68	65	82	87	73	83	68	65
82	87	73	83	68	65	82	87	73	83	68	65	82	87	73	83
68	65	82	87	73	83	68	65	82	87	73	83	68	65	82	87
73	83	68	65	82	87	73	83	68	65	82	87	73	83	68	65
82	87	73	83	68	65	82	87	73	83	68	65	82	87	73	83
68	65	82	87	73	83	68	65	82	87	73	83	68	65	82	87

3) Selanjutnya tahap *Key Scheduling Algorithm* yaitu proses pengacakan kunci yang terjadwal, dengan pemberian nilai awal berdasarkan kunci yang digunakan dengan mencampur operasi menggunakan variable i dan j ke index array S[i] dan K[i]. Langkah pertama diberi nilai inisial untuk i dan j dengan 0. Operasi pencampuran adalah pengulangan rumusan (j+S[i]+K[i] mod 256) yang diikuti dengan pertukaran S[i] dengan S[j]. Iterasi dilakukan sampai 256 dengan hasil sebagai berikut:

Tabel 3. Hasil *Key Scheduling Algorithm*

68	134	218	52	129	217	35	107	197	37	120	214	38	116	212	58
147	247	77	161	7	115	210	60	152	242	94	208	53	165	7	103
217	81	188	50	154	0	120	246	103	227	81	189	59	191	54	184
44	158	34	172	41	177	43	163	45	189	64	206	78	204	92	242
123	15	149	25	175	75	218	116	0	138	38	200	93	253	143	31
193	105	4	170	66	216	128	46	207	123	25	181	99	23	190	112
20	182	106	36	209	137	51	219	149	85	8	198	118	36	228	170
99	39	221	145	87	35	226	172	104	34	238	192	133	85	23	215
169	129	76	34	234	176	136	102	55	19	225	173	139	111	70	40
252	206	178	156	121	97	59	19	253	237	208	190	158	124	108	98
75	63	37	9	255	251	234	228	208	186	182	184	173	173	159	143
145	153	148	154	146	136	144	158	159	171	169	165	179	199	206	224
228	230	250	20	33	57	67	75	101	133	152	182	198	212	244	26
51	87	109	129	167	211	242	28	56	82	126	176	213	5	39	71
121	177	220	18	58	96	152	214	7	67	113	157	219	31	86	152
204	254	66	140	201	17	75	131	205	29	96	174	238	44	124	210

4) Setelah itu, proses selanjutnya adalah mencari nilai biner dari hasil XOR *plaintext* terhadap *Pseudo-random Generation Algorithm*. Berikut merupakan hasil yang diperoleh:

Tabel 4. Hasil *Pseudo-random Generation Algorithm*

No	Kunci	Biner
1	164	10100100
2	155	10011011
3	165	10100101
4	141	10001101
5	151	10010111
6	147	10010011
7	138	10001010
8	147	10010011
9	147	10010011
10	138	10001010
11	156	10011100
12	165	10100101
13	147	10010011

14	150	10010110
15	136	10001000
16	152	10011000

5) Dari tahapan yang telah dilakukan maka dapat diketahui hasil enkripsi dari algoritma RC4 adalah sebagai berikut:

Tabel 4. Hasil Enkripsi RC4

No	Plaintext	Key	Ciphertext	Decimal	ASCII
1	10111001	10100100	00011101	29	↔
2	11011110	10011011	01000101	69	E
3	00010001	10100101	10110100	180	´
4	01010000	10001101	11011101	221	Ý
5	10110100	10010111	00100011	35	#
6	00011010	10010011	10001001	137	ë
7	00101101	10001010	10100111	167	§
8	00111011	10010011	10101000	168	¨
9	01000101	10010011	11010110	214	Ö
10	10010010	10001010	00011000	24	↑
11	11110100	10011100	01101000	104	H
12	00100111	10100101	10000010	130	‚
13	10011100	10010011	00001111	15	☼
14	01101100	10010110	11111010	250	Ú
15	10110010	10001000	00111010	58	:
16	11110010	10011000	01101010	106	J

4.4. Hasil Enkripsi Data

Dari penerapan algoritma AES dan RC4 dalam mengamankan data *Plaintext* berupa "Rp99000000000000" maka dapat diperoleh hasil enkripsi dari data tersebut yaitu: **↔ E´ Ý# ë§¨ Ö↑ H,** ☼ **Ú: J**. Dengan transformasi data yang dilakukan membentuk deretan kode rahasia tersebut maka akan menyulitkan pihak lainnya untuk membaca atau memodifikasi data transaksi yang tersimpan sehingga data tersebut tetap aman.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan maka diperoleh kesimpulan bahwa kombinasi algoritma AES dan RC4 telah mampu menghasilkan nilai enkripsi berupa kode tersembunyi untuk melindungi data *plaintext* yang disimpan. Dengan hasil ini maka dapat diketahui bahwa penerapan algoritma AES dan RC4 dapat membantu dalam pengamanan data digital dari transaksi yang dilakukan serta melindungi data dari serangan pembacaan data oleh pihak yang tidak bertanggung jawab.

REFERENSI

[1] A. Utama and R. F. Siahaan, "Penerapan Kriptografi untuk Pengamanan Data Transaksi Deposito pada Easy Tronik dengan Metode RC-5," vol. 3, no. 3, pp. 29–39, 2021.

[2] Widiarti, Azaanudin, and Elfitriani, “Implementasi Kriptografi Pengamanan Data Nilai Siswa,” vol. 21, no. 1, 2022.
[3] L. Mustika, “Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web,” vol. 7, no. 1, pp. 148–155, 2020.
[4] T. Hidayat, “Encryption Security Sharing Data Cloud Computing By Using Aes Algorithm : A Systematic Review,” vol. 2, no. 2, 2019.
[5] C. Kirana and E. Sugianto, “Penerapan Algoritma AES dan Konversi SMS ke dalam Bahasa Khek pada Aplikasi Enkripsi Berbasis Mobile Application,” vol. 5, no. 1, pp. 68–77, 2019.
[6] R. S. Siregar, M. S. Asih, and N. Wulan, “Penerapan Algoritma Rc4 Dan Rail Fence Untuk Enkripsi Database Mahasiswa Pada Kampus Poltekkes Kemenkes Medan,” vol. 7, no. 2, pp. 51–56, 2019.
[7] R. Rivaldi, T. Informatika, F. T. Informasi, U. B. Luhur, P. Utara, and K. Lama, “Implementasi Pengamanan Data Arsitektur Menggunakan Metode Kriptografi Dengan Algoritma,” vol. 4, no. 2, pp. 63–67, 2021.
[8] P. S. Ramadhan, “Penerapan Euclidean Probability Dalam Pendeteksian Penyakit Impetigo,” vol. 4, no. 1, pp. 11–16, 2019.
[9] D. Boneh and V. Shoup, “A Graduate Course in Applied Cryptography,” 2020.
[10] O. Dakhi, M. Masril, R. Novalinda, and J. Ambiyar, “Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Chiper,” vol. 20, no. 1, pp. 27–36, 2020.
[11] P. Burciu, “An Efficient (Low Resources) Modular Hardware Implementation of the AES Algorithm,” vol. 5, no. 17, pp. 1–10, 2019.
[12] C. Lin, G. Hu, C. Chan, and J. Yan, “applied sciences Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm,” 2021.
[13] T. M. Kumar, K. S. Reddy, S. Rinaldi, B. D. Parameshachari, and K. Arunachalam, “A Low Area High Speed FPGA Implementation of AES Architecture for Cryptography Application,” 2023.
[14] D. W. Ahmed, T. M. Jawad, and L. M. Jawad, “An Effective Color Image Encryption Scheme Based On Double Piecewise Linear Chaotic Map Method And Rc4 Algorithm,” vol. 16, no. 2, pp. 1319–1341, 2021.
[15] J. Zhang, H. Liu, and L. Ni, “A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR,” vol. 8, pp. 38995–39012, 2020.
[16] R. Saha, G. Geetha, W. J. Buchanan, and T. Kim, “MRC4 : A Modified RC4 Algorithm Using Symmetric Random Function Generator for Improved Cryptographic Features,” *IEEE Access*, vol. 7, pp. 172045–172054, 2019.