ISSN : 1411-1624
e-ISSN: 2621-8089

IMPLEMENTASI *CAESAR CIPHER AND ADVANCED ENCRYPTION STANDARD* (AES) PADA PENGAMANAN DATA PAJAK BUMI BANGUNAN

Fitri Nuraeni [1], Yoga Handoko Agustin [2], Angga Eka Purnama [3]
Dosen STMIK Tasikmalaya [1,2], Mahasiswa STMIK Tasikmalaya [3]
Jalan RE Martadinata 272a Indihiang Tasikmalaya
Sur-el: nenk.ufit@gmail.com[1], abeogink@gmail.com[2], anggaekapurnama4@gmail.com[3]

Abstract : *Property tax as one source of local revenue has an important role in the progress of the village. Management of property Tax data in general at the village level still uses the usual number management application. While the property tax data needs to be secured because it is classified as confidential data, which has the potential to cause damage if accessed by unauthorized persons. To maintain the security aspects of the information, a cryptographic system can be used which provides encryption and data description facilities. The cryptographic system used is Caesar Cipher's super encryption and Advanced Encryption Standard (AES) -128-EBC. To test the encryption quality of this cryptographic system an experimental method is used, by comparing the ciphertext file size, encryption time, entropi value, correlation value, histogram graph and avalanche effect. The test results obtained by Caesar Cipher and Advanced Encryption Standard (AES) -128-EBC cryptographic systems, have good correlation and entropy values with better avalanche effect values compared to the AES algorithm alone.*

Keywords*: aes-128-ebc, caesar cipher, confidential, encryption, tax*

Abstrak : *Pajak Bumi dan Bangunan sebagai salah satu sumber pendapatan asli daerah memiliki peranan penting dalam kemajuan desa. Pengelolaan data Pajak Bumi dan Bangunan secara umum di tingkat desa masih menggunakan aplikasi pengelola angka biasa. Sedangkan data Pajak Bumi dan Bangunan (pbb) perlu diamankan karena tergolong ke dalam data confidential, yang mana berpotensi menimbulkan kerusakan apabila diakses oleh orang yang tidak berwenang. Untuk menjaga aspek kemananan informasi tersebut, dapat digunakan sistem kriptografi yang didalamnya menyediakan fasilitas enkripsi dan deskripsi data. Sistem kriptografi yang digunakan adalah super enkripsi Caesar Cipher dan Advanced Encryption Standart (AES)-128-EBC. Untuk menguji kualitas enkripsi sistem kriptografi ini digunakan metode eksperimen, dengan membandingkan ukuran file cipherteks, waktu enkripsi, nilai entropi, nilai korelasi, grafik histogram dan avalanche effect. Hasil pengujian didapat sistem kriptografi Caesar Cipher dan Advanced Encryption Standart (AES)-128-EBC ini, memiliki nilai korelasi dan entropi yang tergolong bagus dengan nilai avalanche effect yang lebih baik dibandingkan dengan algoritma AES saja.*

Kata kunci*: aes-128-ebc, caesar cipher, enkripsi, pajak, rahasia*

1. PENDAHULUAN

Pajak Bumi dan Bangunan sebagai salah satu sumber pendapatan asli daerah memiliki peranan penting dalam kemajuan desa. Data ini tergolong ke dalam data confidential yang mana berpotensi menimbulkan kerusakan apabila diakses tanpa ijin. Kerusakan yang ditimbulkan berupa ketidak-sesuaian data yang ada. Berdasarkan kasus yang telah dipublikasikan oleh tribun jatim dan kabar jatim dimana nama pemilik tanah (Wajib Pajak) mengalami perubahan. Hal ini disebabkan karena wajib pajak tidak membayar (tidak mengurus) pajak selama beberapa tahun. Dengan mengetahui kondisi area yang tidak diperhatikan lagi oleh

ISSN : 1411-1624
e-ISSN: 2621-8089

pemilik, identitas pemilik asli dan kondisi pajak yang tidak dibayarkan dalam kurun waktu lama terutama didukung oleh bocornya data pajak yang berisi NOP (Nomor Objek Pajak) yang mana terdiri dari 15 digit angka dengan fungsi tertentu. Dengan mengetahui NOP ini, seseorang dapat mengetahui identitas pemilik, serta riwayat pembayaran pajak. Keterbengkalaian tanah dan kondisi data pajak yang ada ini dimanfaatkan oleh makelar tanah untuk mengambil alih nama pemilik sebelumnya (yang asli) menjadi miliknya sendiri atau milik orang lain (*client*) untuk dijual kembali. Selain itu, data pajak ini bersifat privasi bagi setiap daerah (karena pengelolaannya berada di tingkat daerah). Tentunya data ini akan dijadikan referensi ketika terjadi sengketa tanah. Dimana dalam data pajak desa terdapat riwayat mutasi NOP dari pemilik awal ke pemilik lainnya. Selain itu, data pengguna yang telah diretas (tanpa pengamanan) dapat dijual melalui deepweb seperti yang terjadi pada salah satu perusahaan unicorn besar di Indonesia baru-baru ini.

Berdasarkan kasus diatas jelas dampak yang dirasakan oleh masyarakat ataupun pihak desa bahwa ketidaksinkronan dan pemanfaatan data yang dilakukan oleh oknum yang tidak memiliki akses/diluar tanggungjawab membuat kerugian tersendiri. Untuk menghindari dampak yang ditimbulkan ini maka data pajak bumi dan bangunan perlu dilakukan pengamanan. Terlebih lagi pengelolaan data pajak bumi dan bangunan yang dilakukan di tingkat desa masih dilakukan dengan menggunakan aplikasi pengelola angka biasa. Hal ini dinilai terlalu rentan dalam hal keamanan data. Dengan demikian perlu dibangun suatu sistem informasi dengan pengamanan data di dalamnya. Penggunaan login dalam sistem masih belum cukup untuk mengamankan data, sehingga diperlukan teknik pengamanan lain yang dapat meningkatkan keamanan data yang berada pada sistem.

Untuk mengamankan data dan informasi terdapat berbagai macam teknik yang dapat diterapkan, salah satunya dengan menggunakan teknik kriptografi ke dalam suatu sistem informasi. Kriptografi menjadi solusi yang ekonomis, efektif dan efisien, karena penggunaannya relatif lebih mudah daripada teknik yang lainnya serta tidak menghabiskan sumber daya yang banyak. Dalam penerapannya kriptografi memiliki berbagai macam algoritma, dimulai dari yang sederhana sampai rumit. Kriptografi sangat erat kaitannya dengan matematika dan logika, sehingga dapat diterima oleh semua orang dan sudah terbukti kemutakhirannya.

Berdasarkan penelitian yang telah dilakukan oleh Agustin Siburian didapatkan hasil bahwa penggunaan metode kriptografi dapat digunakan untuk mengamankan data pada database. Namun masih terdapat kekurangan karena operasi yang digunakan masih terlalu sederhana[1]. Selanjutnya Syaiful anwar menggunakan algoritma AES untuk menyisipkan teks ke dalam suatu gambar didapatkan hasil penyandian yang lebih kompleks namun tidak terlalu memakan waktu [2]. Kemudian dengan algoritma utama yang sama (AES) Fitri Nuraeni dalam penelitiannya mendapatkan kualitas hasil enkripsi yang lebih baik daripada penelitian sebelumnya, hanya saja waktu pemrosesan yang

ISSN : 1411-1624
e-ISSN: 2621-8089

dilakukan masih tergolong lama. Hal ini dikarenakan proses pencarian/ pencocokan pada array indeks yang bergantung pada panjangnya data yang akan diamankan[3]. Berdasarkan penelitian terkait yang telah dilakukan maka penulis mengusulkan metode gabungan antara Caesar Cipher dengan operasi sederhana dan AES dengan kekuatan/kualitas enkripsinya. Sehingga kedua metode ini diasumsikan mampu mendapatkan kualitas enkripsi yang baik dan cepat untuk mengamankan data pajak bumi dan bangunan pada sistem informasi pajak untuk tingkat desa.

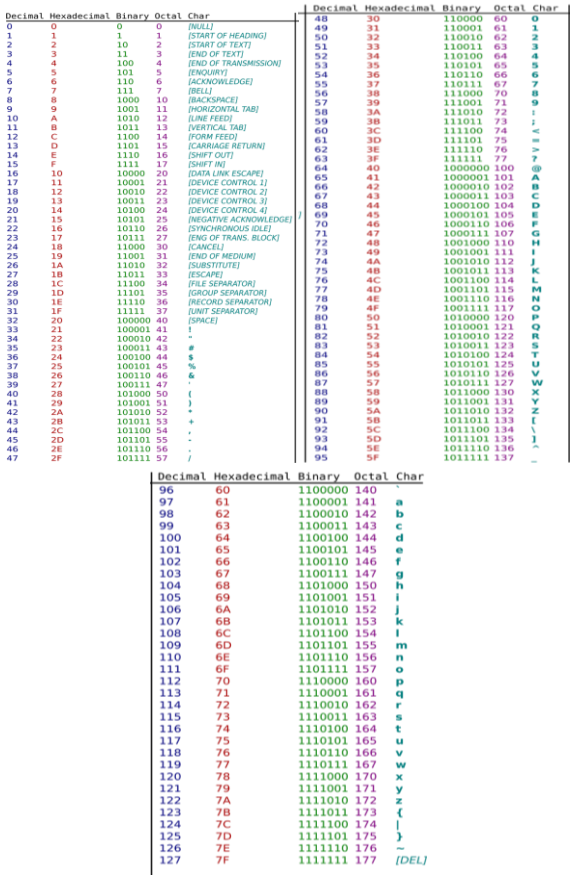
2. METODOLOGI PENELITIAN

2.1 *Caesar Cipher*

Caesar Cipher merupakan algoritma substitusi huruf tunggal yang tergolong pada kritografi klasik. Algoritma ini sangat sederhana dengan ukuran kunci yang pendek, kemudian membuat table subsitusi dengan proses menggeser huruf pada alfabet/ himpunan symbol yang digunakan sebanyak kunci.

Enkripsi *Caesar Cipher* dengan cara menukarkan karakter asli dengan karakter pasangannya pada table substitusi[4]. Kombinasi keduanya akan menghasilkan Cipher pada baris dan kolom yang dipilih.

Sedangkan Teknik lainnya menggunakan proses perhitungan dilakukan dengan menggunakan angka desimal. Sehingga nantinya karakter yang ada akan dikonversikan terlebih dahulu ke dalam bentuk decimal. Untuk konversi karakter ke angka dapat menggunakan tabel ASCII[5] seperti pada gambar 1.



Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	[NULL]
1	1	1	1	[START OF HEADING]
2	2	10	2	[START OF TEXT]
3	3	11	3	[END OF TEXT]
4	4	100	4	[END OF TRANSMISSION]
5	5	101	5	[ENQUIRY]
6	6	110	6	[ACKNOWLEDGE]
7	7	111	7	[BELL]
8	8	1000	10	[BACKSPACE]
9	9	1001	11	[HORIZONTAL TAB]
10	A	1010	12	[LINE FEED]
11	B	1011	13	[VERTICAL TAB]
12	C	1100	14	[FORM FEED]
13	D	1101	15	[CARRIAGE RETURN]
14	E	1110	16	[SHIFT OUT]
15	F	1111	17	[SHIFT IN]
16	10	10000	20	[DATA LINK ESCAPE]
17	11	10001	21	[DEVICE CONTROL 1]
18	12	10010	22	[DEVICE CONTROL 2]
19	13	10011	23	[DEVICE CONTROL 3]
20	14	10100	24	[DEVICE CONTROL 4]
21	15	10101	25	[NEGATIVE ACKNOWLEDGE]
22	16	10110	26	[SYNCHRONOUS IDLE]
23	17	10111	27	[ENG OF TRANS. BLOCK]
24	18	11000	30	[CANCEL]
25	19	11001	31	[END OF MEDIUM]
26	1A	11010	32	[SUBSTITUTE]
27	1B	11011	33	[ESCAPE]
28	1C	11100	34	[FILE SEPARATOR]
29	1D	11101	35	[GROUP SEPARATOR]
30	1E	11110	36	[RECORD SEPARATOR]
31	1F	11111	37	[UNIT SEPARATOR]
32	20	100000	40	[SPACE]
33	21	100001	41	!
34	22	100010	42	"
35	23	100011	43	#
36	24	100100	44	$
37	25	100101	45	%
38	26	100110	46	&
39	27	100111	47	'
40	28	101000	50	(
41	29	101001	51	)
42	2A	101010	52	*
43	2B	101011	53	+
44	2C	101100	54	,
45	2D	101101	55	-
46	2E	101110	56	.
47	2F	101111	57	/
48	30	110000	60	0
49	31	110001	61	1
50	32	110010	62	2
51	33	110011	63	3
52	34	110100	64	4
53	35	110101	65	5
54	36	110110	66	6
55	37	110111	67	7
56	38	111000	70	8
57	39	111001	71	9
58	3A	111010	72	:
59	3B	111011	73	;
60	3C	111100	74	<
61	3D	111101	75	=
62	3E	111110	76	>
63	3F	111111	77	?
64	40	1000000	100	@
65	41	1000001	101	A
66	42	1000010	102	B
67	43	1000011	103	C
68	44	1000100	104	D
69	45	1000101	105	E
70	46	1000110	106	F
71	47	1000111	107	G
72	48	1001000	110	H
73	49	1001001	111	I
74	4A	1001010	112	J
75	4B	1001011	113	K
76	4C	1001100	114	L
77	4D	1001101	115	M
78	4E	1001110	116	N
79	4F	1001111	117	O
80	50	1010000	120	P
81	51	1010001	121	Q
82	52	1010010	122	R
83	53	1010011	123	S
84	54	1010100	124	T
85	55	1010101	125	U
86	56	1010110	126	V
87	57	1010111	127	W
88	58	1011000	130	X
89	59	1011001	131	Y
90	5A	1011010	132	Z
91	5B	1011011	133	[
92	5C	1011100	134	\
93	5D	1011101	135	]
94	5E	1011110	136	^
95	5F	1011111	137	_
96	60	1100000	140	`
97	61	1100001	141	a
98	62	1100010	142	b
99	63	1100011	143	c
100	64	1100100	144	d
101	65	1100101	145	e
102	66	1100110	146	f
103	67	1100111	147	g
104	68	1101000	150	h
105	69	1101001	151	i
106	6A	1101010	152	j
107	6B	1101011	153	k
108	6C	1101100	154	l
109	6D	1101101	155	m
110	6E	1101110	156	n
111	6F	1101111	157	o
112	70	1110000	160	p
113	71	1110001	161	q
114	72	1110010	162	r
115	73	1110011	163	s
116	74	1110100	164	t
117	75	1110101	165	u
118	76	1110110	166	v
119	77	1110111	167	w
120	78	1111000	170	x
121	79	1111001	171	y
122	7A	1111010	172	z
123	7B	1111011	173	{
124	7C	1111100	174	|
125	7D	1111101	175	}
126	7E	1111110	176	~
127	7F	1111111	177	[DEL]

Gambar 1. himpunan karakter pada ASCII

Pada penelitian ini, digunakan karakter pada ASCII yang dapat dicetak atau ditampilkan pada layer, yaitu karakter mulai dari decimal 32 sampai 127 sejumlah 94 karakter. Sehingga proses Enkripsi *Caesar Cipher* secara matematis dapat ditulis dalam bentuk:

$$C_i = 32 + ((P_i + k) mod\ N) \quad (1)$$

Sedangkan Deskripsi *Caesar Cipher* secara matematis dapat ditulis dalam bentuk:

$$P_i = 32 + ((C_i - k) mod\ N) \quad (2)$$

Keterangan :

Ci = Cipherteks indeks ke-i

Pi = Plainteks indeks ke-i

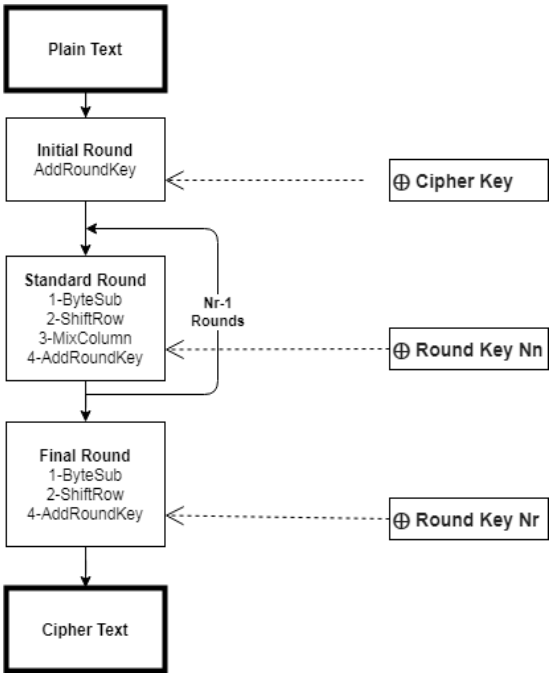
k = Kunci pergeseran indeks

N = Jumlah *array alphabet*

ISSN : 1411-1624
e-ISSN: 2621-8089

2.2 *Advanced Encryption Standard* (AES)

Algoritma AES terdiri dari 3 tahapan utama dan 4 operasi dasar. Hal tersebut dapat dilihat pada Gambar 2.

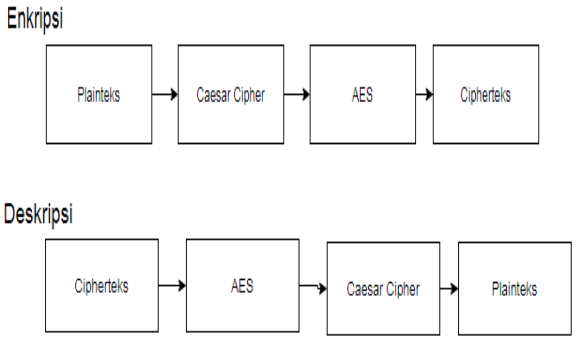


Gambar 2. Algoritma AES

Untuk AES-128 bit, banyaknya putaran pada proses enkrpisi sebanyak 10 kali[6]. Berdasarkan gambar 2 tahapan pertama yang dilakukan adalah *initial round*. Pada inisialisasi ini dilakukan operasi *AddRoundKey* antara Plaintext dengan *Cipher Key* (kunci) menggunakan XOR. Kunci awal (*initial vector*), nantinya pada *standard round* (1-9) dan *final round* (10) diperlukan kunci yang berbeda-beda. Proses untuk mendapatkan kunci ini dinamakan *Key Expansion*. Matriks kunci yang berbeda-beda ini terdiri dari 44 (0 s/d 3 diambil dari *Cipher Key* awal), dimulai dari (4 s/d 43 dilakukan *generate*) yang terdiri dari 10 blok, tiap blok terdiri dari 4 *word*[7].

2.3 Super enkripsi *Caesar Cipher* + *Advanced Encryption Standard* (AES)

Pada penelitian ini dirancangan suatu sistem kriptografi dengan menggunakan 2 (dua) kali proses enkripsi agar dapat meningkatkan kualitas enkripsi dan keamanan data pada sistem informasi. Proses perancangan Enkripsi dan Deskripsi pada penggabungan algoritma *Caesar Cipher* dan *Advanced Enkripsi Standard* (AES) diantaranya :



Gambar 3. Proses Enkripsi dan Deskripsi

Alur dari enkripsi dan deskripsi untuk super enkripsi Caesar dan AES, yaitu kunci disimpan pada tabel dengan pengamanan *hashing standard*. Pengguna (kolektor desa dan kepala desa) hanya menginputkan kunci sebanyak satu kali yakni ketika login. Plainteks inputan akan diproses terlebih dahulu oleh algoritma *Caesar Cipher*.

Selanjutnya Cipherteks yang dihasilkan dijadikan plainteks pada algoritma AES. Setelah diproses sedemikian rupa, pada akhirnya Cipherteks akhir (*Super Enkripsi Caesar Cipher* dan *AES*) disimpan ke dalam database. Penggabungan dua algoritma ini bertujuan untuk memperkuat keamanan dari cipherteks yang dihasilkan.

ISSN : 1411-1624
e-ISSN: 2621-8089

Contoh plainteks pada data Pajak Bumi dan Bangunan:

Tabel 1. Plainteks data pajak

Kode	:	3209200016001000102020
Data Tagihan	:	ENTIN BIN AWHSAR|NASOL|450|0|7500
Status Nop	:	BELUM DIBAYAR

Maka, ketika dilakukan Super Enkripsi akan menghasilkan cipherteks sebagai berikut:

Tabel 2. Cipherteks data pajak

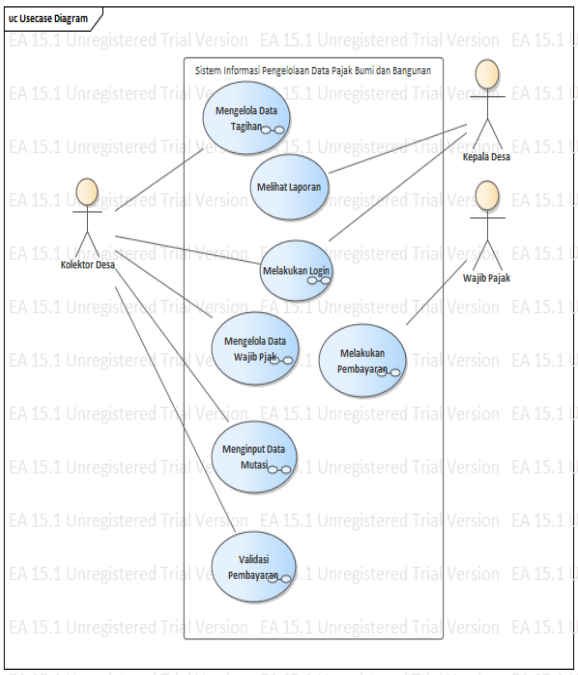
Kode	:	C$x&W&T(O*i+6,9+=.>. S0Z1S252)4%5e5]6j76819 w:h$=X>VAa@!CiDND
Data Tagihan	:	H$d&b(X(](0)K*+-<,_.D/5/}0M1%3I5@ 5A7n6s8m9f:Zw?:BmAN CME[DvFDF?I&IbISJ^KVNVM >OoObQ.Q7R!U
Status Nop	:	&%%&w#k):*V*t*o+8. Q.d.@/#1I2?273

Dengan menggunakan penggabungan dua buah algoritma (Super Enkripsi) antara Caesar Cipher dengan AES. Didapatkan cipherteks yang lebih kuat dibandingkan hanya dengan mengandalkan sebuah algoritma saja. Berdasarkan ilustrasi diatas dapat kita lihat bahwa antara cipherteks dengan plainteks bentuknya sangat jauh berbeda.

3. HASIL DAN PEMBAHASAN

Untuk dapat mengimplementasikan sistema kriptografi dengan superenkripsi ini, maka dibuatkan suatu fungsi enkripsi dan dekripsi yang ditambahkan pada suatu sistem informasi pengelolaam data pajak bumi dan bangunan.

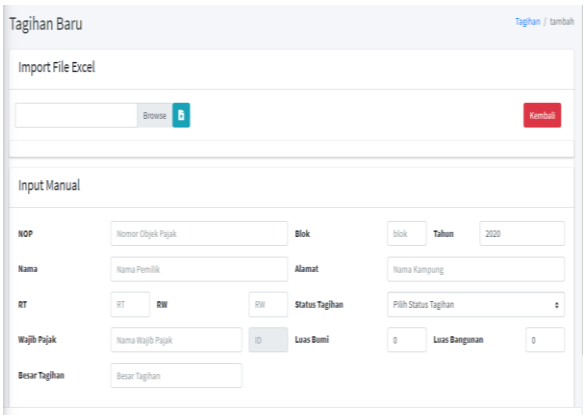
Gambar 4 merupakan alur yang terdapat di rekam medis dengan data yang terenkripsi pada database. Kolektor desa dapat mengelola data dengan melakukan login dan menginput kunci enkripsi satu kali pada halaman login. Kunci enkripsi disimpan pada salah satu tabel di database dengan hashing. Kepala desa dan kolektor desa sama-sama mengetahui kunci algoritma. Sedangkan wajib pajak hanya memasukan username dan password saja (karena kunci ini bersifat rahasia).



Gambar 4. Diagram *usecase* sistem informasi pengelolaan data pajak

Sistem informasi menyediakan fasilitas untuk menginputkan data seperti pada tampilan kolektor desa untuk data wajib pajak, tagihan pajak dan data mutasi, serta input pembayaran tagihan pajak pa tampilan wajib pajak. Setiap proses input data akan diikuti dengan proses enkripsi, sehingga data yang tersimpan pada database adalah cipherteks atau data yang terenkripsi (*encyrpted data*).

ISSN : 1411-1624
e-ISSN: 2621-8089



Gambar 5. Form input tagihan pajak bagi kolektor desa

Contoh form input pada gambar 5 merupakan tampilan depan dari sistem informasi yang digunakan oleh kolektor desa untuk menginput data tagihan pajak. Setelah data diinput, maka data akan dienkripsi menggunakan super enkripsi *caesar cipher* dan AES. Kemudian hasilnya dikirim ke server untuk disimpan pada database. Data terenkripsi pada database dapat dilihat pada gambar 6 dibawah ini.

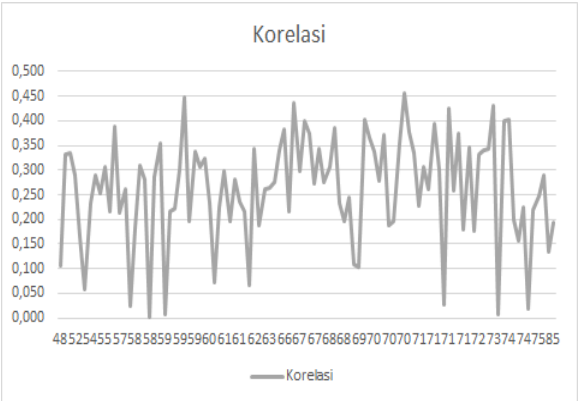
Gambar 6. data terenkripsi disimpan pada database

Sedangkan untuk mengetahui kualitas enkripsi dari sistem kriptografi ini, dilakukan uji-coba perhitungan entropi dan korelasi dengan menggunakan 100 plainteks. Yang diharapkan dari hasil pengujian ini adalah semakin rendah korelasi antar variable dan semakin tinggi entropinya, semakin aman sistem enkripsinya[7].

No	Plainteks	Ukuran Plainteks	Kunci	Waktu Enkripsi	Ukuran Cipherteks	Entropy	Korelasi
1	32092000160010010|ENTIN BIN AWHSAR|NASOL|20204|50|0|||7500	59	sindangsari2020	3,474	258	3,447	0,007
2	32092000160010020|ANDA BIN SOBARI|NASOL|2020|430|0|||7500	58	sindangsari2020	3,670	244	3,409	0,023
...	...	...	...	...	...	...	...
99	32092000160010990|IDING|KP SETIAMULYA|2020|429|0|042|16|7500	61	sindangsari2069	3,269	128	5,932	0,280
100	32092000160010100|SARMA|KP SETIAMULYA|2020|490|0|041|16|7500	61	sindangsari2070	3,719	128	5,888	0,237
Mean		65,180		3,872	128,360	5,750	0,262

Gambar 7. Pengujian Ukuran Cipherteks, Waktu Enkripsi, Entropi dan Korelasi

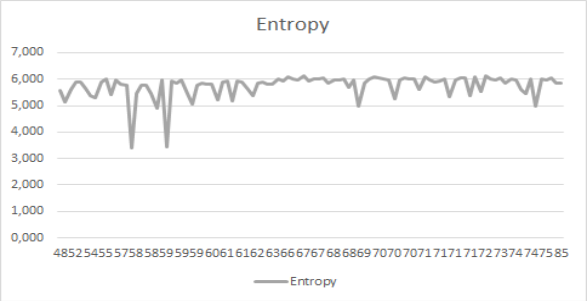
Data pengujian dikumpulkan pada Gabar 7, kemudian dianalisis per parameter kualitas enkripsi. Seperti Gambar 8 dimana dapat dilihat nilai korelasi mengalami kenaikan dan penurunan secara fluktuatif, dimana nilai terkecilnya 0 sedangkan terbesarnya 0,45 dengan rata-rata 0,262. Nilai ini mendekati 0, sehingga dapat dikatakan bahwa koefisien korelasi rendah. Pada kualitas enkripsi, semakin rendah koefisien korelasi maka akan semakin tidak berkorelasi antara plainteks dengan cipherteks.



Gambar 8. Grafik fluktuasi nilai korelasi

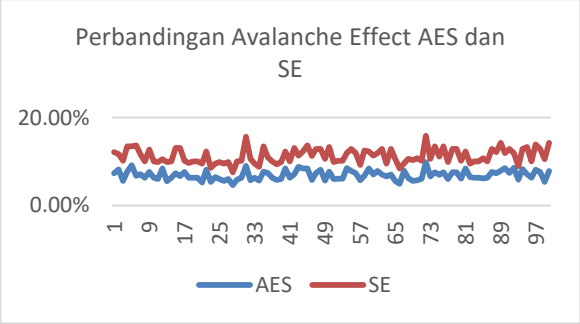
Nilai entropi mengalami kenaikan dan penurunan, namun lebih konstan dapat dilihat pada gambar 9.

ISSN : 1411-1624
e-ISSN: 2621-8089



Gambar 9. Grafik fluktuasi nilai entropi

Rata-rata entropi yang dihasilkan adalah 5,75. Entropi merupakan nilai rata-rata perkiraan dari jumlah bit rata-rata yang digunakan untuk mengkodekan elemen pesan. Nilai tertinggi dari entropi adalah 8. Nilai yang didapatkan pada penelitian ini mendekati 8, dengan demikian entropi yang dihasilkan tergolong bagus. Dengan meratanya karakter yang berada pada cipherteks, maka hal ini akan mempersulit kriptanalis untuk memecahkan hasil enkripsi melalui analisis frekuensi.



Gambar 10. Grafik perbandingan *avalanche effect* AES dengan Super Enkripsi

Gambar 10 diatas menjelaskan tentang plainteks yang digunakan untuk menguji avalanche effect dalam menentukan jumlah putaran yang akan digunakan dalam proses enkripsi, jumlah perubahan bit-bit karakter dari plainteks awal ke plainteks yang baru menghasilkan 1 bit perubahan saja. Pengujian *avalanche effect* dilakukan untuk mencari seberapa besar pengaruh perubahan plainteks terhadap cipherteks. Secara visual dari pengujian yang dilakukan peningkatan *avalanche effect* AES dengan nilai ratarata 6,90% sementara *avalanche effect* Super Enkripsi dengan nilai rata-rata 11,30%. Dari data diatas nilai *Avalanche Effect* SE 2 kali lipat lebih besar dari AES. Namun nilai ini masih tergolong kecil, yakni dibawah 50%. Dengan demikian perubahan cipherteks tidak terlalu signifikan ketika satu bit data pada plainteks berubah. Perubahan cipherteks yang terjadi ketika satu bit diubah adalah sebesar 80 bit. Nilai ini konstan karena AES beroperasi pada mode blok, sehingga semakin panjang plainteks yang digunakan maka semakin kecil nilai *avalanche effect* yang didapatkan.

4. KESIMPULAN

Berdasarkan hasil dari implementasi *Caesar Cipher* dan AES pada pengamanan data pajak bumi dan bangunan pada tingkat desa, dapat disimpulkan bahwa :

1. Dengan dibangunnya Sistem Informasi, data pajak bumi dan bangunan menjadi lebih mudah dikelola.
2. Dengan dibangunnya Super Enkripsi dalam pengamanan data pajak bumi dan bangunan dapat menjaga keamanan data yang ada pada database. Data yang disimpan dalam database tidak dapat dibaca secara langsung, sehingga kebocoran data akan dapat diminimalisir.
3. Algoritma *Caesar Cipher* dan AES-128 CBC menjadi algoritma yang bagus untuk

ISSN : 1411-1624
e-ISSN: 2621-8089

mengamankan data dengan korelasi sebesar 0,257 dan entropy 5,75. Namun nilai *avalanche effect* yang kecil yakni 11,30%.

Untuk pengembangan yang lebih baik lagi bagi penelitian selanjutnya di kemudian hari, dapat diperhatikan beberapa hal diantaranya sebagai berikut:

1. Penelitian sebelumnya sudah membahas mengenai implementasi Vigenere Cipher dan AES. Begitupula pada penelitian ini telah diuji coba Caesar Cipher dan AES. Sehingga nantinya dapat dilakukan penelitian lebih lanjut mengenai metode manakah yang terbaik untuk mengamankan data teks diantara keduanya.
2. Penggunaan AES128-EBC dapat dimodifikasi outputnya menjadi range yang lebih luas, sehingga entropy meningkat dengan distribusi frekuensi yang lebih merata.
3. Kunci untuk proses enkripsi dan deskripsi masih statis. Dianjurkan bukan hanya data login saja yang dapat diubah, melainkan kunci untuk enkripsi dan deskripsi. Hal ini dapat meningkatkan keamanan sistem menjadi lebih tinggi lagi.

DAFTAR PUSTAKA

[1] A. Siburian and A. P. Harianja, "Perancangan Aplikasi Pengamanan Basis Data Menggunakan Algoritma Caesar Cipher," vol. 02, no. 479, pp. 1–6, 2017.

[2] S. Anwar, "Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES," *Jurnal*, vol. 6, pp. 2089–5615, 2017.

[3] I. H. Fitri Nuraeni, Yuda Purnama Putra, "Implementasi kriptografi superenkripsi vigenere cipher dan advanced encrytion standard (aes) pada pengamanan data riwayat pasien rumah sakit."

[4] M. L. L. Wijaya, K. Yulianti, and H. S. Husain, "Kriptografi Dengan Komposisi Caesar Cipher Dan Affine Cipher Untuk Mengubah Pesan Rahasia," *J. EurekaMatika*, vol. 5, no. 1, pp. 30–45, 2017.

[5] E. Handayani, W. L. Pratitis, A. Nur, S. A. Mashuri, and B. Nugroho, "Perancangan Aplikasi Kriptografi Berbasis Web Dengan Algoritma Double Caesar Cipher Menggunakan Tabel ASCII," *SEMNASTEKNOMEDIA ONLINE*, vol. 5, no. 1, pp. 1–2, 2017.

[6] A. Arif and P. Mandarani, "Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit Pada Sistem Keamanan Short Message Service (SMS) Berbasis Android," *J. TeknoIf*, vol. 4, no. 1, 2016.

[7] J. Simarmata, Sriadhi., and R. Rahim, *Kriptografi Teknik Keamanan Data & informasi*. ANDI, 2019.