Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878

IMPLEMENTASI ALGORITMA AES DAN ALGORITMA XOR PADA APLIKASI PENGAMANAN TEKS BERBASIS MOBILE

RESTI AMALIA
PERANI ROSYANI
Program Studi Teknik Informatika
Fakultas Teknik, Universitas Pamulang
Emali: dosen00850@unpam.ac.id, dosen00837@unpam.ac.id

Abstrak. Kriptografi banyak digunakan untuk menjaga aspek keamanan informasi. Pada penelitian ini penulis mengkombinasikan dua kriptografi modern dengan tujuan untuk memperkuat keamanan pengiriman pesan. Pada kriptografi modern pertama, peneliti menggunakan algoritma *XOR* dikarenakan tidak sulit secara komputasional dan mudah diimplementasikan. Pada kriptografi modern kedua, peneliti memilih algoritma *AES* dikarenakan proses algoritma ini cepat serta kuat. Proses pengamanannya pertama-tama menggunakan kriptografi XOR terlebih dahulu kemudian baru di enkripsi lagi menggunakan algoritma AES.. Sedangkan untuk proses dekripsi, tahap awal cipherteks didekripsi dengan algoritma *AES* untuk mendapatkan *cipherteks*. Kemudian *cipherteks* didekripsi lagi dengan algoritma *XOR* untuk menghasilkan *plainteks* kembali. Hasil dari penelitian ini diharapkan agar pesan text dapat terjaga kerahasiaan, keutuhan dan keaslian pesan ketika dikirim ke si penerima dan dapat mengetahui seberapa cepat proses enkripsi kombinasi algoritma sebelum pesan terkirim.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, *XOR, AES, Android*

Abstract*. Cryptography is a lot to access aspects of information. In this study the author combines two modern cryptography with the aim of initiating the sending of messages. In the first modern cryptography, researchers used the XOR algorithm because it is not difficult computationally and easily implemented. In both modern cryptography, researchers chose the AES algorithm that allows this algorithm to be fast and powerful. The security process first uses XOR cryptography first and then encrypts it again using the AES algorithm. The process for the decryption process, the initial stage of the ciphertext is decrypted with the AES algorithm to get the ciphertext. Then the ciphertext is decrypted again with the XOR algorithm to return the plaintext. The results of this study are expected so that text messages can delight confidentiality, integrity and authenticity of messages sent sent to the recipient and can be found.*

Key Word :*Criptography, Encryption, Decription, XOR, AES, Android*

PENDAHULUAN

Untuk berkomunikasi selain menggunakan lisan, kita juga sering menggunakan tulisan sebagai sarana bertukar informasi. Seiring perkembangan jaman pertukaran informasi menggunakan tulisan menjadi banyak dilakukan dikarenakan penyampaiannya lebih menghemat waktu dan tingkat keamannya jauh lebih baik dibandingkan berkomunikasi menggunakan lisan secara langsung. Pengamanan pengiriman pesan itu sendiri bisa menggunakan berbagai teknik kriptografi diantaranya kriptografi klasik dan juga kriptografi modern.

Kriptografi banyak digunakan untuk menjaga aspek keamanan informasi. Ada empat tujuan mendasar dari ilmu kriptografi yaitu *confidentiality* (kerahasiaan), integrity (keutuhan), authentication (keaslian pesan), dan *non-repudiation* (tak terbantahkan)(Mollin, 2007). Kriptografi diambil dari bahasa yunani, terdapat dua kata gabungan yaitu dari kata *crypto* dan *graphia* yang artinya penulisan dan rahasia'(Setyaningsih, 2015). Menurut terminologinya,

Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878

kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain(Ariyus, 2008).

Beberapa tahun terakhir ini perkembangan teknologi berkembang dengan pesat. Perkembangan teknologi ini tidak lepas dari perkembangan ilmu pengetahuan itu sendiri. Ilmu pengetahuan digunakan untuk menciptakan teknologi yang mempermudah pekerjaan manusia. Salah satunya adalah perkembangan telepon seluler. Smarthphone saat ini telah berkembang menjadi sebuah alat yang bisa melakukan banyak hal. Smartphone digunakan untuk mengakses internet, mengecek *email*, bermain game, membaca buku, mengirim pesan *instant*, mendengarkan musik, sampai menonton film ataupun video. Singkatnya, smarthphone kini telah berevolusi dari yang hanya telepon seluler menjadi smartphone atau menjadi sebuah telepon pintar.

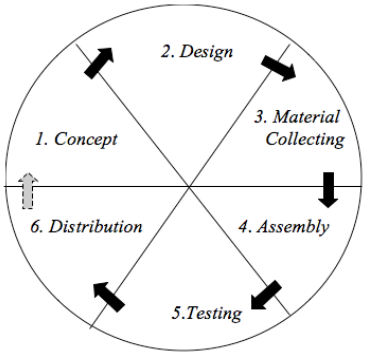
Semakin berkembangnya teknologi *smartphone* tersebut maka dari itu vdibutuhkan juga keamanan dalam penggunaannya, khususnya keamanan pesan. Kriptografi adalah suatu ilmu dan sekaligus suatu seni untuk menjaga kerahasiaan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2008). Kriptografi terbagi menjadi dua cara dalam penyajiannya yaitu dengan kriptografi klasik dan juga kriptografi modern. Kriptografi klasik umumnya beroperasi dalam mode karakter sedangkan kriptografi modern beroperasi pada mode bit. Contoh kriptografi klasik adalah algoritma *XOR* dan kriptografi moderen adalah algoritma AES. Algoritma *XOR* adalah algoritma sederhana yang menggunakan prinsip operator logika *XOR* . Proses dalam melakukan enkripsinya adalah dengan meng- *XOR*-kan *plaintext* dengan kunci sehingga didapatkan *ciphertext*-nya. Sebaliknya untuk proses dekripsi adalah dengan meng-*XOR*-kan *ciphertext* dengan kunci sehingga didapatkan *plaintext*-nya kembali. Untuk kriptografi klasik, penulis memilih algoritma ini dikarenakan mudah diimplementasikan dan operasi *XOR* tidak sulit secara komputasional. Karenanya algoritma *XOR* masih sering digunakan untuk mengamankan informasi atau pesan dan kemudian dilengkapi dengan suatu mekanisme keamanan tambahan yang dalam hal ini peneliti menambahkan algoritma AES(Safaat, 2014).
AES merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok ciphertext simetrik yang dapat mengenkripsi dan dekripsi informasi. Algoritma AES Algoritma AES is mengunkan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits(Pabokory, Astuti, & Kridalaksana, 2015).

Dengan melhat permasalahan yang ditemukan di atas, dalam penelitian ini penulis mecoba membuat sualtu aplikasi kriptografi klasik dengan modern yaitu algoritma *XOR* dan algoritma *AES*.. Kombinasi algoritma kriptografi *XOR* dan *AES* dalam penelitian ini diharapkan dapat mengamankan informasi dengan baik.

METODE

Menurut Luther pengembangan sistem multimedia mempunyai enam tahap yaitu *concept, design, material collecting, assembly, testing,* dan *distribution* (Sutopo, 2003). Tahapan menggunakan metodologi pengembangan multimedia tersebut bias dilakukan secara acak atau tidak perlu berurutan. Keenam tahapannya dapat saling bertukar posisi namun tetap dimulai dari tahap konsep dahulu dan diakhiri dengan tahap distribusi. Semua tahapan dari metode Luther dimulai dari Konsep dan diakhiri dengan tahap Distribusi. Sedangkan tahap *Material Collecting* dapat dikerjakan scara paralel dengan tahap *Assembly*. Tahapan versi Luther adalah sebagai berikut:

Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878



Gambar 1 Model Pengembangan Multimedia

1. Konsep (*Concept)*
Tahap konsep adalah untuk menentukan tujuan dan siapa yang akan menggunakan program. Selain itu menentukan jenis dari aplikasi dan juga tujuan aplikasi. Peraturan untuk perancangan juga ditentukan pada tahap konsep, misalnya ukuran aplikasi, target, dan lain-lain.
2. Perancangan (*Design)*
Design (perancangan) adalah suatu tahapan yang membuat spesifikasi mengenai gaya, arsitektur, tampilan, program, antar muka dan kebutuhan bahan untuk program. Spesifikasi dibuat selengkap mungkin sehingga pada tahap berikutnya pengambilan keputusan baru tidak diperlukan lagi. Tahap ini biasanya menggunakan papan cerita untuk menggambarkan deskripsi tiap tahap, dengan mencantumkan semua objek multimedia dan tautan ke tahap lain dan bagan alir untuk menggambarkan aliran dari satu tahap ke tahap lain. Disarankan untuk tahapan ini pengerjaan spesifikasinya dilakukan lengkap mungkin karena akan berpengaruh di tahapan selanjutnya.
3. Pengumpulan Bahan (*Material Collecting*)
Material Collecting adalah tahap dimana pengumpulan bahan yang sesuai dengan kebutuhan produk multimedia yang dikerjakan seperti gambar, teks, dan audio. Tahap ini dapat dikerjakan paralel dengan tahap *assembly*. Pada berbagai kasus, tahap *Material Collecting* dan tahap *Assembly* selalu dikerjakan secara linear dan tidak paralel.
4. Pembuatan (*Assembly*)
Assembly adalah tahap dimana semua objek atau bahan multimedia dibuat. Pembuatan aplikasi didasarkan pada tahap *design*, seperti *story board* dan struktur navigasi.
5. Pengujian (*Testing*)
Testing Dilakukan setelah selesai tahap pembuatan (*assembly*) dengan dijalankannya aplikasi dan keudian dilihat apakah ada masih ada kesalahan atau tidak. Tahap ini disebut dengan pengujian alpha, dimana pengujiannya dilakukan oleh sipembuat, setelah itu dilakukan betha test yang kemudian melibatkan pengguna akhir. Fungsi dari tahap ini adalah melihat hasil pembuatan aplikasi apakah sesuai dengan yang diharapkan atau tidak.
6. Distribusi (*Distribution*)
Tahapan dimana aplikasi disimpan dalam suatu media penyimpanan untuk didistribusikan ke pengguna akhir atau *client*. Pada tahap ini jika media penyimpanan tidak cukup untuk menampung aplikasinya, maka dilakukan kompresi terhadap aplikasi tersebut. Pada tahap ini juga akan dilakukan evaluasi sebagai masukan(Binanto, 2010).

HASIL DAN PEMBAHASAN

Analisis Sistem

Sekenario pengiriman SMS dengan aplikasi kriptografi dimulai dari sipengirim pesan membuka aplikasi yang sudah terinstal di smartphone android kemudiang mengetikan nomor tujuan, isi

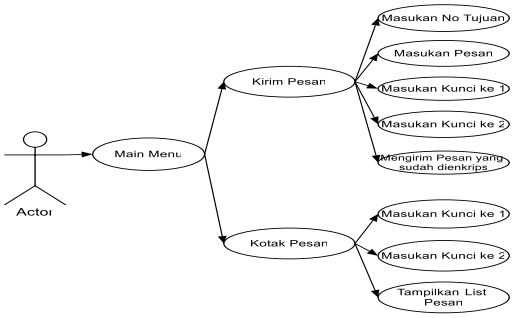
Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878

pesan, kunci pertama, kunci kedua dan diakhiri dengan menekan tombol kirim pesan yang sekaligus secara bersamaan akan meampilkan hasil pesan yang sudah disandikan atau dienkripsi dan juga penghitungan waktu proses waktu enkripsi.

Gambar 2 Sekenario Pengiriman Pesan Menggunakan Aplikasi Kriptografi

Isi pesan yang sudah terenkripsi akan otomatis masuk di smartphone si penerima, dan hanya bisa dibuka menggunakan aplikasi kriptografi yang sama dan dengan kata kunci yang juga sama dengan si pengirim.

UseCase Diagram



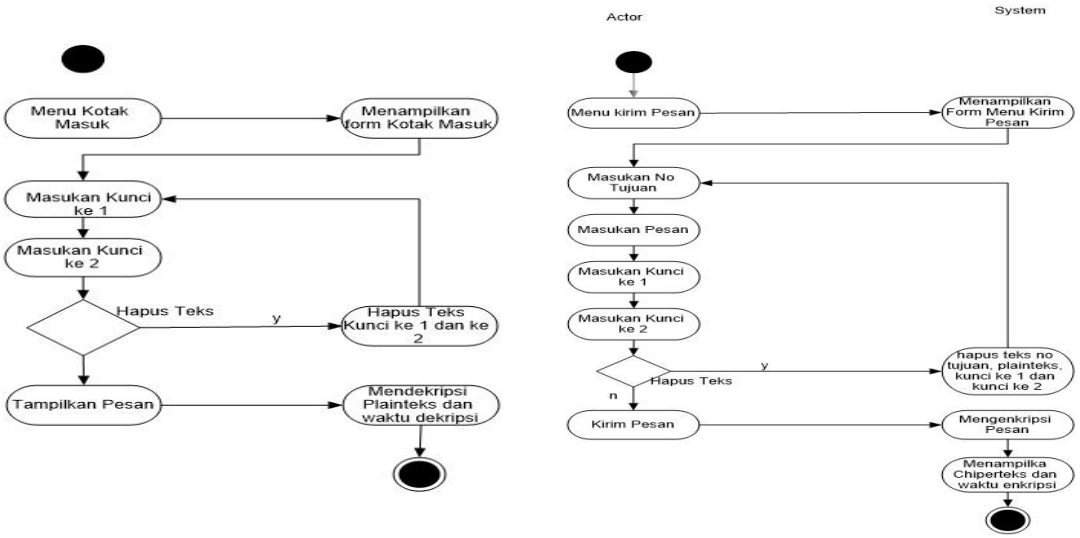
Gambar 3 *UseCase Diagram*

Dari Gambar 3 dijelaskan bahwa ketika *actor* memilih main utama, sudah otomatis *include* pilihan menu "Kirim Pesan" dan juga menu " Kotak Masuk'. Dimana jika si *actor* memilih menu Kirim pesan maka akan tampil form menu yang berisikan untuk memasukan no tujuan si penerima, isi pesan, kunci pertama, kunci kedua dan tombol kirim pesan untuk mengirimkan pesan ke si penerima pesan.

Activity Diagram

Activity diagram adalah suatu diagram aktivitas yang menjelaskan proses kerja dalam sebuah sistem yang saat ini sedang berjalan. *Activity diagram* bertujuan untuk membantu menggambarkan interaksi antara beberapa *usecase* dan jyga memahami keseluruhan proses. *Activity diagram* sistem ini terbagi dua, yaitu *activity diagram* proses enkripsi dan *activity diagram* proses dekripsi. *Activity diagram* prose enkripsi dan dekripsi dapat dilihat pada Gambar 4.

Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878



Gambar 4 *Activity Diagran* Proses Enckripsi dan Dekripsi

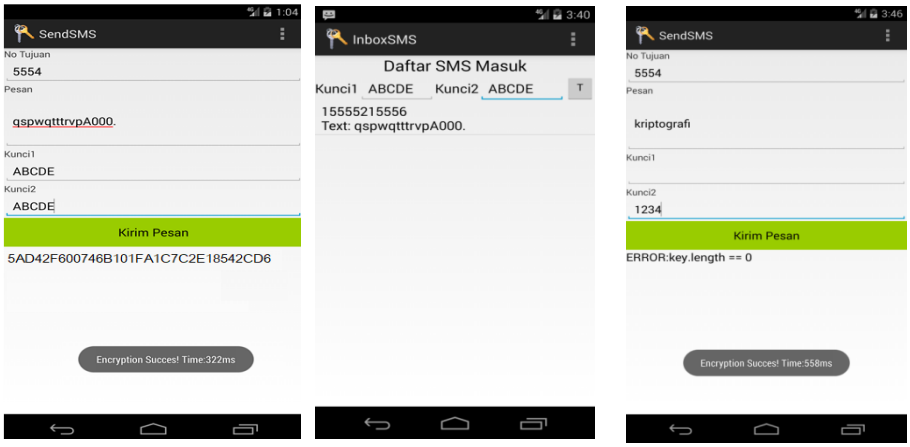
Pengujian

Pengujian sistem merupakan tahap lanjutan setelah perancangan dan pengimplementasi sistem. Pengujian sistem bertujuan untuk membuktikan sistem yang dibangun telah berjalan dengan baik atau belum. Pengujian dilakungan menggunakan emulator 5556 dan 5554.

Pada tahap ini, penulis melakukan pengujian dengan cara membandingkan
hasil dari proses enkripsi dan dekripsi yang dihasilkan oleh sistem yang dibangun terhadap hasil proses enkripsi dan dekripsi yang diperoleh melalui perhitungan manual. Selain itu pengujian dilakukan terhadap penanganan sistem ketika terjadi kesalahan, serta lamanya waktu proses enkripsi maupun dekripsi untuk mengetahui apakah kombinasi algoritma XOR dan algoritma AES lebih efisien dibandingkan proses enkripsi dan dekripsi algoritma tersebut secara terpisah atau masing-masing. Pengujian tersebut dilakukan dengan panjang plaintext yang bervariasi. Misalnya pesan yang akan dienkripsi adalah “qspwqtttrvpA000.”dengan kunci XOR dan AES adalah “ABCDE”.

Pengujian Enkripsi dan dekripsi dengan Sistem

Pengujian sistem yang dibangun dengan chiperteks diatas akan menhasilkan *plainteks* “5AD42F600746B101FA1C7C2E18542CD6” bersamaan dengan waktu proses enkripsi . hasil lengkap proses enkripsi dan dekripsi ditujukan pada Gambar dibawah ini.



Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878

Gambar 6 Pengujian dengan sistem

Jika user menekan tombol 'Kirim Pesan' sedangkan *plainteks* masih kosong atau salah satu kunci kosong, maka sistem akan menampilkan pesan error di dalam isi pesan.

Sekenario Enkripsi XOR

Diketahui *Plainteks* = 'qspwqtttrvpA000.'. Dengan kunci = 'ABCDE'.Panjang kunci XOR akan melakukan padding untuk mengenkripsi plain teks.

- *Plainteks* = qspwqtttrvpA000.
- Kunci *padding* = ABCDEABCDEABCDEA

Nilai karakter-karakter tersebut akan dikonversi kedalam kode biner kemudian dilakukan oprasi XOR pada tiap-tiap karakter antara plaintek terhadap kuncinya, sehingga didapat hasil sebagai berikut:

q	s	p	w	q	
0111 0001	0111 0011	0111 0000	0111 0111	0111 0001	
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	
0011 0000	0011 0001	0011 0011	0011 0011	0011 0100	
0	1	2	3	4	
t	t	t	r	v	
0111 0100	0111 0100	0111 0100	0111 1100	0111 1100	
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	
0011 0101	0011 0110	0011 0111	0011 1000	0011 1001	
5	6	7	8	9	
p	A	0	0	0	.
0000 0000	0000 0000	0000 0000	0000 0000	0000 0000	0000 0111
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	0100 0001
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101	0100 0110
A	B	C	D	E	F

Dari hasil operas diatas didapat plainteks baru dari cipherteks yang dihasilkan dari operasi XOR yaitu: '0123456789ABCDEF'

Sekenario Enkripsi AES

Misalkan sebuah plainteks memiliki kunci seperti berikut:

Plaiteks : 0 1 2 3 4 5 6 7 8 9 A B C D E F
Dalam HEX : 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46
Kunci : A B C D E F G H I J K L M N O P
Dalam HEX : 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50

Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878

a. *AddRoundKey*

30	34	38	43	XOR	41	45	49	4D	=	71	71	71	0E
31	35	39	44		42	46	4A	4E		73	73	73	0A
32	36	41	45		43	47	4B	4F		71	71	0A	0A
33	37	42	46		44	48	4C	50		77	1F	0E	16

b. *SubBytes*

71	71	71	0E	=	A3	A3	A3	AB
73	73	73	0A	*SubByte*	8F	8F	8F	67
71	71	0A	0A		A3	A3	67	67
77	1F	0E	16		F5	C0	AB	47

c. *SiftRow*

A3	A3	A3	AB
8F	8F	8F	67
A3	A3	67	67
F5	C0	AB	47

A3	A3	A3	AB
8F	8F	67	8F
67	67	A3	A3
47	F5	C0	AB

d. *MixColoms*

A3	A3	A3	AB
8F	8F	67	8F
67	67	A3	A3
47	F5	C0	AB

02	03	01	01	X	A3	=	07	07	B5	67	96
01	02	03	01		8F		06	06	41	CC	2A
01	01	02	03		67		2B	2B	B1	91	69
03	01	01	02		47		FB	FB	E3	9A	A8

Ambil 4 *byte* terakhir , yaitu 4D 4E 4F 50 , lalu geser *byte* pertama menjadi *byte* terakhir. Hasilnya 4E 4F 50 5D. substitusikan dengan s-box, hasilnya adalah 2F 84 53 E3.

Selanjutnya XOR kan dengan konstatnta nilai tertentu dari pengguna.

2F XOR 01=0010 1111 XOR 0000 0001 = 0010 1110 = 2E

84 XOR 00=1000 0100 XOR 0000 0000 = 1000 0100 = 84

53 XOR 00= 0101 0011 XOR 0000 0000 = 0101 0011 = 53

E5 XOR 00=1110 0011 XOR 0000 0000 = 1110 0011 = E5

Langkah terakhir XOR-kan 2E 84 53 E5 dengan 4 *byte* pertama kunci awal yaitu 41 42 43 44.

2E XOR 41= 0010 1110 XOR 0100 0001 = 0110 1111 = 6F

84 XOR 2 = 1000 0100 XOR 0100 0010 = 1100 0110 = C6

53 XOR 43= 0101 0011 XOR 0100 0011 = 0001 0000 = 10

E5 XOR 44= 1110 0011 XOR 0100 0100 = 1010 0111 = A7

Hasil proses XOR diatas adalah 6F C6 10 A7 yang merupakan 4 *byte* pertama dari kunci yang baru untuk *byte*. Untuk 4 *byte* ke 2, kita tinggal melakukan operasi xor antara 4 *byte* operasi XOR antara 4 *byte* kunci selanjutnya dengan 6F C6 10 A7.

Demikian seterusnya hingga didapatkan 16 *byte* set kunci yang baru. Ekspansi keseluruhan dapat dilihat padac tabel-tabel dibawah ini

Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878

Round 1

6F	2A	63	2E
C6	80	CA	8B
10	57	1C	53
A7	EF	A3	F3

Round 2

50	7A	19	37
2B	AB	61	EA
1D	4A	56	5
96	79	DA	29

Round3

D3	49	80	87
40	EB	8A	60
B8	F2	A4	A1
0C	75	AF	86

Round 4

0B	A2	12	95
72	99	13	73
FC	0E	AA	0B
1B	6E	C1	47

Round 5

94	36	24	b1
59	C0	D3	F3
5C	52	F8	F3
31	5F	9E	D9

Round 6

54	62	46	F7
44	84	57	F7
69	3B	C3	30
F9	A6	38	E1

Round 7

7C	1E	58	AF
40	C4	93	64
91	AA	69	59
91	32	0F	EE

Round 8

BF	A1	F9	56
8B	4F	DC	B8
B9	13	7A	23
E8	DF	D0	3E

Round 9

C8	69	90	C6
AD	E2	3E	86
0B	18	62	41
59	86	56	68

Round 10

BA	D3	43	85
2E	CC	F2	74
4E	56	34	75
ED	6B	3D	55

Tabel 1 Ekspand Cipherteks

Round	Mulai				Setelah SubByte				Setelah Shift Row				Setelah MixColomns					Nilai Roundkey			
0	30	34	38	43													⊕	41	45	49	4D
	31	O3	39	44														42	46	4A	4E
	32	36	41	45														43	47	4B	4F
	33	37	42	46														44	48	4C	50
1	71	71	71	0E	A3	A3	A3	AB	A3	A3	A3	AB	O7	B5	67	96	⊕	6F	2A	63	2E
	73	73	73	0A	8F	8F	8F	67	8F	8F	67	8F	O6	41	CC	2A		C6	80	CA	8B
	71	71	0A	0A	A3	A3	67	67	67	67	A3	A3	2B	B1	91	69		10	57	1C	53
	77	1F	0E	16	F5	C0	AB	47	47	F5	C0	AB	FB	E5	9A	AB		A7	EF	A3	F3
2	68	9F	O4	B8	45	DB	F2	6C	45	DB	F2	6C	C1	9B	26	ED		50	7A	19	37
	C0	C1	O6	A1	BA	78	6F	32	78	6F	32	BA	E4	7C	OC	EE		2B	AB	61	EA
	3B	E6	8D	3A	E2	8E	5D	80	5D	80	E2	8E	28	OF	BF	O8		1D	4A	56	O5
	5C	OC	39	5B	4A	FE	12	39	39	4A	FE	12	60	3F	6A	A4		96	79	DA	29
3	91	E1	3F	DA	81	F8	75	57	81	F8	75	57	4F	59	DC	A8	⊕	D3	49	B0	87
	CF	D7	6D	O4	8A	OE	3C	F2	0E	3C	F2	8A	C8	67	D9	5A		EB	EB	8A	60
	35	45	D9	0D	96	6E	35	D7	35	D7	96	6E	FD	8C	51	B7		B8	F2	A4	A1
	F6	46	B0	8D	42	5A	E7	5D	5D	42	5A	E7	FD	6B	0A	DE		0C	75	AF	86

Faktor Exacta 11 (4): 369-378, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v11i4.2878

4	9C	F0	6C	2F	DE	8C	50	15	DE	8C	50	15	2E	4B	35	O7	⊕	OB	A2	12	95
	88	8C	53	3A	C4	64	ED	80	64	ED	80	C4	E9	1F	94	32		72	99	13	73
	45	7E	F5	16	6E	F3	E6	47	E6	47	6E	F3	63	8C	71	D2		5C	52	F8	F3
	F1	1E	A5	58	A1	72	O6	6A	6A	A1	72	O6	3D	54	A4	C2		1B	6E	C1	47
5	25	E9	27	92	3F	1E	CC	4F	3F	1E	CC	4F	22	FC	E0	79	⊕	94	36	24	B1
	9B	86	87	41	14	44	17	83	44	17	83	14	49	58	C2	BD		59	C0	D3	A0
	34	6D	DB	D9	18	3C	B9	35	B9	35	18	3C	F7	9E	7B	1C		5C	52	F8	F3
	26	3A	65	85	F7	80	4D	97	97	F7	80	4D	1B	O3	BA	63		31	5F	9E	D9
6	B6	CA	C4	C8	4E	74	1C	E8	4E	74	1C	E8	FE	9D	58	D5	⊕	54	62	46	F7
	10	98	11	10	CA	46	82	CA	46	82	CA	CA	86	9B	76	61		44	84	57	F7
	AB	CC	83	EF	62	4B	EC	DF	EC	DF	62	48	OE	O3	96	BF		69	3B	C3	30
	2A	5C	24	BA	E5	A4	36	F4	F4	E5	4A	36	56	A0	15	BE		F9	A6	38	E1
7	AA	FF	1E	22	AC	16	72	93	AC	16	72	93	30	F3	BF	CC	⊕	7C	1E	58	AF
	C2	1F	21	96	25	C0	FD	90	C0	FD	90	25	43	BA	30	DD		40	C4	93	64
	66	38	55	8F	33	O7	FC	73	FC	73	33	O7	CA	C1	4D	CB		91	AA	69	59
	AF	O6	2D	5F	79	6F	D8	CF	CF	79	6F	D8	C8	BE	51	74		91	32	OF	EE
8	4C	ED	E7	63	29	55	94	FB	29	55	94	FB	7E	28	71	3E	⊕	BF	A1	F9	56
	O3	7E	A3	B9	7B	F3	OA	56	F3	OA	56	7B	26	4A	9A	B8		8B	4F	DC	B8
	5B	6B	24	92	39	7F	36	4F	36	4F	39	7F	FA	DB	BA	39		B9	13	7A	23
	59	89	5E	9B	CB	A7	58	14	14	CB	A7	58	15	C3	7D	39		E8	DF	DO	3E
9	C1	89	88	68	78	A7	C4	45	78	A7	C4	45	68	70	4B	B3	⊕	C8	69	90	C6
	AD	O5	46	OO	95	6B	5A	63	6B	5A	53	95	F9	F6	F1	1F		AD	E2	3E	86
	43	C8	CO	1A	1A	E8	BA	A2	BA	A2	1A	E8	DF	OD	BA	F1		OB	18	62	41
	FD	1C	AD	O7	54	9C	95	C5	C5	54	9C	95	O1	6F	17	DC		59	86	56	68
10	A0	19	DB	75	E0	O4	B9	9D	E0	D4	B9	9D					⊕	BA	D3	43	85
	54	14	CF	99	20	FA	8A	EE	FA	8A	EE	2O						2E	CC	F2	74
	D4	15	D8	B0	48	59	61	E7	61	E7	48	59						4E	56	34	75
	58	E9	41	B4	6A	1E	83	8D	8D	6A	1E	83						ED	6B	3D	55
	55	O7	FA	18																	
	D4	46	1C	54																	
	2F	B1	7C	2C																	
	60	O1	2E	D6																	

Output ari keseluruhan *Round* adalah:
54 D4 2F 60 07 46 B1 01 FA 1C 7C 2E 18 54 2C D6
Dari proses:

E0 XOR BA = 1110 0000 1011 1010 = 54
FA XOR 2E = 1111 1010 0010 1110 = D4
61 XOR 4E = 0110 0001 0100 1110 = 2F
8D XOR ED = 1000 1101 1110 1101 = 60

D4 XOR D3 = 1101 0100 1101 0011 = 07
8A XOR CC = 1000 1010 1100 1100 = 46
E7 XOR 56 = 1110 0111 0101 0110 = B1
6A XOR 6B = 0110 1010 0110 1011 = 01

B9 XOR 43 = 1011 1001 0100 0011 = FA
EE XOR F2 = 1110 1110 1111 0100 = 1C
48 XOR 34 = 0100 1000 0011 1101 = 7C
1E XOR 3D = 0001 1110 0011 1101 =2E

9D XOR 85 = 1001 1101 1000 0101 = 18
20 XOR 74 = 0010 0000 0111 0100 = 54
59 XOR 75 = 0101 1001 0111 0101 = 2C
83 XOR 55 = 1000 0011 0101 0101 = D6

Pengujian Waktu Hasil Enkripsi dan Dekripsi Pesan

Pengujian berikutnya adalah pengujian terhadap lamanya waktu enkripsi dan dekripsi menggunakan aplikasi berdasarkan panjang plainteks yag bervariasi dan menggunakan kunci yang sama yaitu “12345” untuk XOR dan “12345”untuk AES. Pengujian ini bertujuan untuk mengetahui apakah kombinasi algoritma XOR dan algoritma AES lebih efisien dibandingkan proses enkripsi dan dekripsi algoritma tersebut aecara terpisah atau masing-masing.

a. Pengujian lama waktu enkripsi

Tabel 2 Hasil pengujian lamanya waktu proses enkripsi

No	Panjang Plainteks	Waktu enkripsi (detik) Kombinasi Algoritma XOR dan AES	Algoritma XOR	Algoritma AES
1	100	1,3	1,3	1,3
2	120	1,3	1,3	1,3
3	130	1,4	1,3	1,4
4	140	1,5	1,4	1,4
Total		5,15	4,13	4,14

Berdasarkan hasil pada Tabel 5.2, lamanya waktu proses enkripsi kombinasi algoritma XOR dan algoritma AES lebih efisien dibandingkan dengan penjumlahan proses enkripsi masing-masing algoritma tersebut, yaitu 5,15 detik dan 4,13 + 4,14 = 8,27 detik dengan selisih 3,12 detik. Selain itu lama waktu enkripsi berbanding lurus dengan panjang *plaintteks.* Semakin panjang plainteks, maka semakin lama pula waktu yang dibutuhkan untuk proses enkripsi.

PENUTUP

Simpulan

Berdasarkan pembahasan dan hasil penelitian, maka diperoleh beberapa kesimpulan sebagai berikut:

1. Implementasi algoritma kriptografi, yaitu kombinasi algoritma XOR dan algoritma AES untuk pengamanan teks pada perangkat Android berhasil dilakukan. Aplikasi yang dihasilkan berjalan sesuai dengan algoritma yang digunakan. Plaintext yang diacak dapat dikembalikan ke bentuk semula dengan menjaga keaslian dan keutuhan pesan tersebut setelah dikirim.
2. Waktu pemrosesan enkripsi dari kombinasi algoritma XOR dan algoritma AES ternyata lebih efisien dibandingkan dengan penjumlahan waktu proses enkripsi masing-masing algoritma tersebut. Untuk proses enkripsi selisihnya adalah 3,12 detik.

Saran

Saran untuk pengembangan lebih lanjut terhadap penelitian ini adalah penelitian ini masih mencakup proses enkripsi dan dekripsi data teks selanjutnya peneliti dapat mengembangkan data seperti gambar, video, file dan lain-lain.

DAFTAR PUSTAKA

Ariyus, D. (2008). Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi. *Journal of Chemical Information and Modeling*. https://doi.org/10.1017/CBO9781107415324.004

Binanto, I. (2010). Multimedia Digital - Dasar Teori dan Pengembangannya. *C.V Andi Offset*. https://doi.org/10.1890/0012-9615(1997)067[0109:SOFAAE]2.0.CO;2

Mollin, R. A. (2007). An Introduction to Cryptography. *Florida: Chapman &; Hall/CRC.*, *Edisi ke-2*.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawariman*. https://doi.org/10.1080/10408398.2011.606379

Safaat, H. N. (2014). *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. *Informatika*. https://doi.org/10.1007/s13398-014-0173-7.2

Setyaningsih, E. (2015). Kriptografi dan Implementasinya Menggunakan Matlab. *Andi*.