ISSN 2085-4552

Pengembangan Algoritma *Advanced Encryption Standard* pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere

Sugiyanto, Rinci Kembang Hapsari
Jurusan Teknik Informatika, Institut Teknologi Adhi Tama, Surabaya, Indonesia
sugianto@itats.ac.id, rincikembang@itats.ac.id

Diterima 13 Desember 2016
Disetujui 30 Dember 2016

***Abstract*—Short Message Service (SMS) is working on a wireless network that allows the theft of the message contents. There are risks that could threaten the security of the contents of the message on SMS services, including SMS snooping, and SMS interception. Therefore, it takes security system messages on SMS services to maintain the security and integrity of the message content to cover the security messages. Algorithms Advanced Encryption Standard (AES) using a structure SPN (Substitution Permutation Network) structure, which has the disadvantage of encryption and decryption, so the safety level is low. To cover the security hole of these weaknesses, the researchers conducted the improvement of Advanced Encryption Standard (AES) algorithm security system based on android SMS using Vigenere algorithm, so that the level of security and integrity of the content of the short message becomes higher and difficult to solve. The results showed an average increase in percentage value of the avalanche effect from 37.24% to 42.96%.**

***Keywords*—Advanced Encryption Standard, android, message security, encryption.**

I. Pendahuluan

Perkembangan teknologi pada telepon seluler saat ini berkembang pesat. Hal ini dapat dilihat dengan munculnya berbagai sistem operasi yang lengkap layaknya komputer, diantaranya adalah android. Android ialah sebuah sistem operasi berbasis linux untuk perangkat telepon seluler yang mencakup sistem operasi, middleware, aplikasi dan menyediakan platform yang terbuka bagi para pengguna untuk menciptakan aplikasi mereka. Android berkembang begitu pesat karena mempunyai platform yang sangat lengkap, baik dalam sistem operasi, aplikasi dan tools pengembangannya, market aplikasi serta mendapat dukungan besar dari komunitas open source di dunia [1].

Meskipun android memiliki fitur yang lengkap, namun layanan SMS (Short Message Service) sebagai layanan pertukaran informasi atau pesan pendek menjadi komunikasi paling digemari karena penggunaannya yang mudah dan biaya yang relatif murah. Namun demikian SMS tidak menjamin integritas dan keamanan isi pesan yang kita kirimkan. Pesan yang sudah dikirim bersifat personal atau rahasia tidak terjamin sampai ke penerima tanpa diketahui informasinya oleh pihak yang tidak bertanggung jawab [2]. Beberapa resiko yang bisa mengancam keamanan dari isi pesan pada layanan SMS, misalnya SMS snooping dan SMS interception. SMS snooping sering terjadi karena kelalaian dari pengguna telepon seluler. Misalnya ketika seseorang meminjamkan telepon selulernya pada orang lain. Pada saat itulah orang tersebut dapat dengan sengaja atau tidak sengaja telah membuka isi dari pesan yang ada dalam kotak masuk SMS tersebut.

SMS interception adalah pencurian data pesan ketika dalam proses transmisi dari pengirim pesan ke penerima pesan. SMS bekerja pada jaringan nirkabel yang memungkinkan dapat terjadinya pencurian isi pesan. Hal ini yang pernah dilakukan oleh intelejen negara tetangga Indonesia seperti Malaysia dan Australia untuk mencari tahu

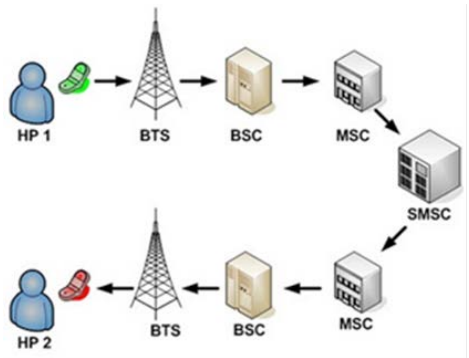
kondisi politik negara Indonesia. Oleh karena itu dibutuhkan sebuah sistem keamanan pesan pada layanan SMS yang dapat menjaga keamanan dan integritas isi pesan untuk bisa menutupi celah keamanan pesan terutama SMS snooping dan SMS interception. Agar isi dari pesan hanya bisa dimengerti maknanya oleh pengirim dan penerima.

Endriani [3] membuat implementasi algoritma enkripsi AES pada aplikasi SMS berbasis Android. Algoritma Advanced Encryption Standard (AES) menggunakan struktur SPN (Substitution Permutation Network) yang memiliki kelemahan perbedaaan dari struktur enkripsi dan dekripsi sehingga tingkat keamanannya juga berbeda. Dan muncul pula serangan baru yaitu algebra attack yang prinsip kerjanya mencari persamaan aljabar sederhana yang dikandung dari tabel S-Box AES. Dari hasil ulasan diatas terdapat kelemahan dari algoritma AES. Untuk menutupi celah keamanan tersebut, peneliti menambahkan algoritma Vigenere [4] agar tingkat keamanan dan integritas dari isi pesan singkat menjadi susah untuk dipecahkan. Isi pesan tersebut sebelum dikirim melalui layanan SMS terlebih dahulu harus dienkripsi dengan algoritma kriptografi, misalnya Vigenere dan Advanced Encryption Standard (AES).

II. TINJAUAN PUSTAKA

A. Short Message Service (SMS)

Layanan SMS merupakan komunikasi yang sering digunakan untuk mengirim dan menerima pesan singkat. SMS ini juga dapat digunakan pada teknologi jaringan GPRS dan CDMA [5]. Alur pengiriman SMS pada standar teknologi GSM (Global System for Mobile Communication) dapat dilihat pada gambar 1.



Gambar 1. Alur SMS

Keterangan:
BTS : Base Transceiver Station
BSC : Base Station Controller
MSC : Mobile Switching Center
SMSC : Short Message Service Center

Ketika pengguna telepon seluler mengirimkan SMS, maka pesan tersebut akan dikirim ke MSC melalui beberapa jaringan seluler yang sudah tersedia, yang pertama melalui tower BTS yang meng-handle komunikasi pengguna tersebut, lalu dilanjutkan ke BSC, kemudian sampai ke MSC. Dari MSC selanjutnya di-forward lagi SMS tersebut ke SMSC untuk disimpan. Kemudian SMSC mengecek melalui HLR (Home Location Register) untuk mengetahui apakah telepon seluler tujuan dalam keadaan aktif dan dimanakah telepon seluler tujuan tersebut. Jika telepon seluler dalam keadaan tidak aktif maka pesan tersebut tetap disimpan di SMSC itu sendiri, dan menunggu laporan dari MSC untuk memberitahukan bahwa telepon seluler sudah aktif kembali untuk kemudian SMS tersebut dikirim dengan batas waktu tunggu yaitu validity period dari pesan SMS tersebut. Jika telepon seluler tujuan aktif maka pesan langsung disampaikan MSC melewati jaringan yang meng-handle penerima pesan (BSC dan BTS).

B. Cryptography

Dalam masa teknologi informasi saat ini, keamanan dan kerahasiaan data atau pesan merupakan sesuatu hal yang sangat penting dan telah menjadi kebutuhan mendasar. Informasi penting tidak akan berguna lagi apabila ditengah jalan informasi tersebut disadap atau dibajak oleh orang yang tidak bertanggung jawab. Bahkan mungkin beberapa pengguna dari sistem itu sendiri, dapat mengubah data dari informasi yang dikirim menjadi sesuatu yang tidak diinginkan. Keamanan data atau pesan pada komputer tidak hanya tergantung pada teknologi saja, tetapi ada juga dari aspek prosedur dan kebijakan keamanan yang diterapkan. Jika firewall dan perangkat keamanan lainnya bisa dibobol oleh orang yang tidak berhak, maka yang berperan utama adalah kriptografi untuk mengamankan data atau pesan dengan menggunakan teknik enkripsi sehingga data atau pesan tidak bisa dibaca [2].

Kriptografi merupakan ilmu atau seni untuk menjaga kerahasiaan dari informasi atau pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya

[6]. Ada beberapa istilah yang penting dalam kriptografi adalah sebagai berikut :

a. Pesan (*message*) adalah data atau informasi yang dikirim yang dapat dibaca dan dipahami.
b. Plainteks (*plaintext*) adalah suatu pesan yang dapat dibaca dan memiliki makna (arti).
c. Cipherteks (*ciphertext*) adalah suatu pesan yang sudah disandikan atau melalui proses enkripsi, sehingga tidak bisa terbaca dan tidak memiliki makna (arti).
d. Enkripsi (*encryption*) adalah proses untuk mengubah plainteks menjadi cipherteks.
e. Kunci (*key*) adalah parameter yang digunakan untuk melakukan proses enkripsi dan dekripsi. Kunci dibagi menjadi dua bagian, yaitu kunci umum (*public key*) dan kunci pribadi (*private key*).
f. Dekripsi (*decryption*) adalah proses kebalikan dari enkripsi, yaitu pengubahan dari cipherteks menjadi plainteks.
g. Kriptoanalisis (*cryptoanalisys*) adalah suatu ilmu atau seni yang bertujuan untuk memecahkan pesan rahasia yang sudah dienkripsi tanpa mengetahui kunci yang telah digunakan.

C. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) dapat mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit [3]. Panjang kunci dan ukuran blok tersebut dapat dipilih secara independen [7]. Setiap blok yang dienkripsi dalam sejumlah putaran tertentu, seperti pada DES. Dengan panjang kunci 128 bit, maka dapat dihitung terdapat kemungkinan kunci sebanyak = 3,4 x . Jika menggunakan komputer tercepat yang dapat mencoba untuk menghitung 1 juta kunci setiap detik, maka akan dibutuhkan waktu selama 5,4 x tahun untuk mencoba seluruh kemungkinan kunci tersebut.

Garis besar dari algoritma AES yang beroperasi pada blok dan kunci 128 bit adalah sebagai berikut :

1. *AddRoundKey* : melakukan perhitungan XOR antara plainteks dengan *cipher* key. Tahap ini dapat disebut *initial round*.
2. Putaran sebanyak Nr-1 kali atau putaran pertama. Proses yang dilakukan pada setiap putaran adalah :
   a. *SubBytes* yaitu proses substitusi *byte* dengan menggunakan tabel *S-box.*
   b. *ShiftRows* yaitu proses pergeseran baris-baris *array state* secara *wrapping.*
   c. *MixColumns* yaitu proses mengacak data pada setiap kolom *array state.*
   d. *AddRoundKey* yaitu melakukan perhitungan XOR antara *arraystate* yang sekarang dengan *round key* atau *keyschedule*.
3. Final *round* yaitu proses putaran untuk yang terakhir :
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

D. Algoritma Vigenere

Algoritma Vigenere termasuk dalam kategori algoritma klasik yang berupa kode abjad majemuk (polyalphabetic substitution cipher) [8]. Teknik untuk menghasilkan cipherteks dapat dilakukan menggunakan substitusi angka maupun huruf pada bujur sangkar Vigenere. Namun dalam penelitian ini telah disesuaikan bahwa semua tanda baca yang biasanya digunakan pada layanan SMS dapat dienkripsi. Dimana menggunakan ASCII standar SMS yaitu dengan merubah mod 26 menjadi mod 128 sehingga rumusnya menjadi sebagai berikut :

Rumus enkripsi algoritma Vigenere :

$$Ci = (Pi + Ki) \bmod 128 \quad (1)$$

Rumus dekripsi algoritma Vigenere :

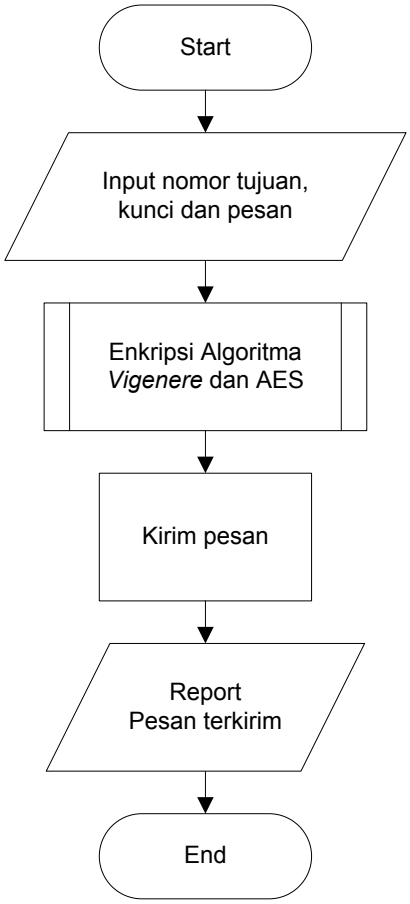
$$Pi = (Ci - Ki) \bmod 128 \quad (2)$$

Dimana :
Ci = nilai desimal karakter ciphertext ke-i
Pi = nilai desimal karakter plaintext ke-i
Ki = nilai desimal karakter kunci ke-ii

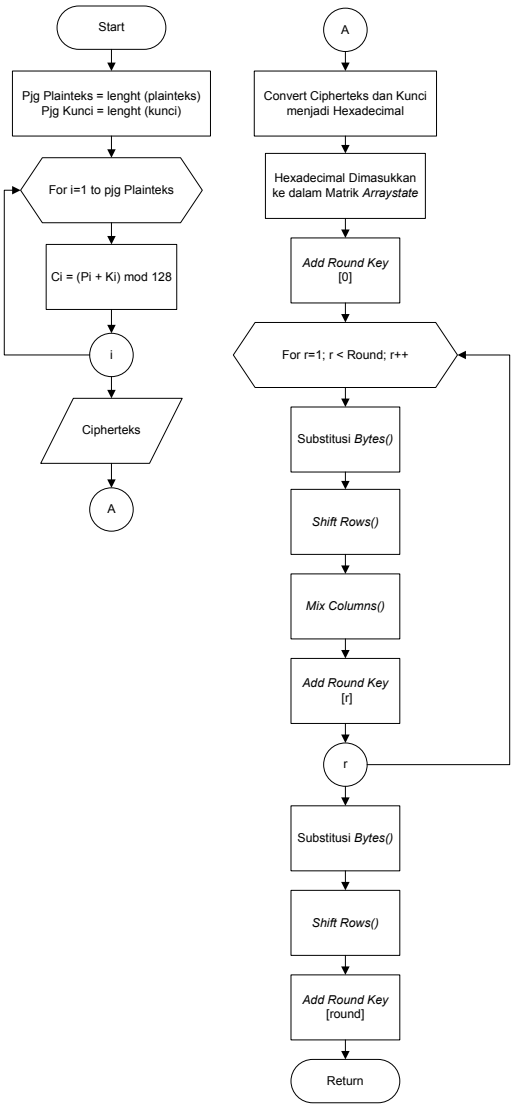
Standar tabel ASCII untuk layanan SMS berbeda dengan tabel ASCII untuk komputer, jika tabel ASCII untuk layanan SMS menggunakan tabel ASCII 7 bit yang jumlah karakternya 128, sedangkan tabel ASCII untuk komputer menggunakan tabel ASCII 8 bit yang jumlah karakternya 256.

III. METODOLOGI

Proses kerja enkripsi dan dekripsi akan digambarkan menggunakan flowchart. Proses enkripsi SMS dapat dilihat pada Gambar 2. Pada Gambar 2 menggambarkan pengirim dapat menulis pesan, mengenkripsi pesan, mengirim pesan, serta memilih keluar aplikasi. Untuk penerima dapat mengirim pesan, menerima SMS, mendekripsi pesan, serta memilih keluar aplikasi.



Gambar 2. Enkripsi Pesan SMS



Gambar 3. Enkripsi Algoritma Vigenere dan AES

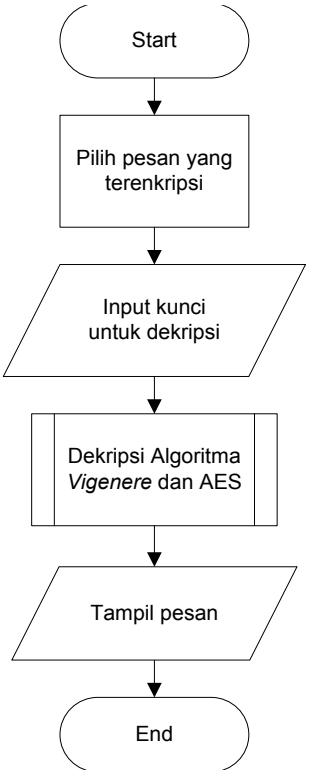
Tahapan proses enkripsi adalah sebagai berikut :

1. Pengguna memasukkan input berupa nomor tujuan, kunci dan pesan.
2. Lakukan enkripsi pesan singkat (SMS) dengan algoritma Vigenere dan AES seperti pada Gambar 3.
3. Pesan yang telah terenkripsi menjadi teks yang tidak terbaca.
4. Kemudian muncul report bahwa pesan telah terkirim.

Proses dekripsi pesan singkat (SMS) dapat dilihat pada gambar 4. Tahapan proses dekripsi adalah sebagai berikut :

1. Pengguna memilih pesan yang sudah

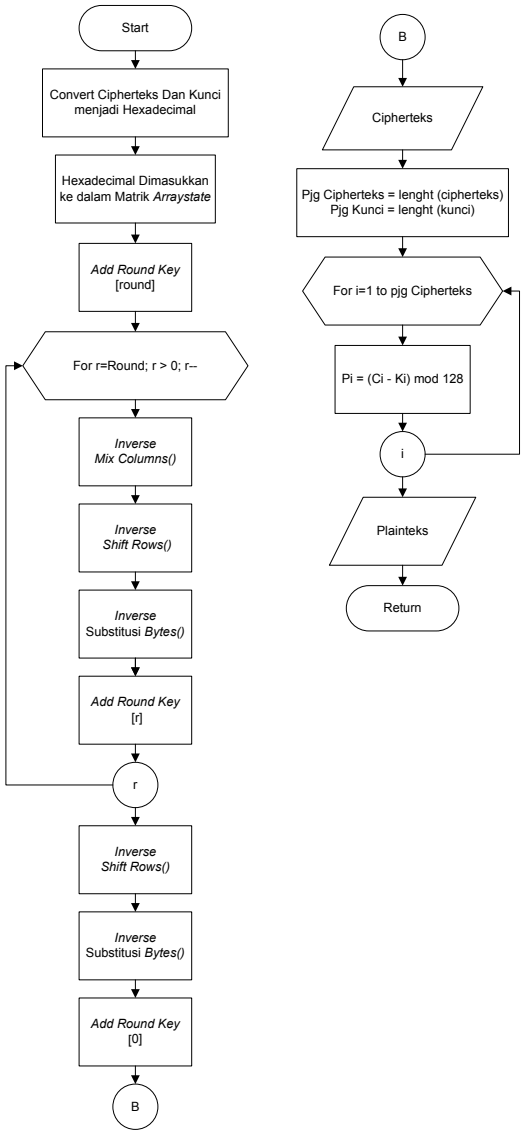
terenkripsi.
2. Masukkan kunci untuk dekripsi pesan.
3. Lakukan dekripsi pesan singkat (SMS) dengan algoritma Vigenere dan AES seperti pada Gambar 5.
4. Pesan yang sudah terdekripsi menjadi teks yang bisa terbaca.



Gambar 4. Dekripsi Pesan SMS

IV. HASIL DAN PEMBAHASAN

Dalam proses pengujian sistem ini peneliti menjalankan sekaligus menguji coba sistem yang telah dibuat dengan melakukan running pada emulator maupun handset android. Dan juga melakukan pengujian pengaruh perubahan bit yaitu avalanche effect. Avalanche effect dapat digunakan sebagai metrik untuk menganalisis kinerja dan keamanan dari suatu algoritma enkripsi kriptografi [9]. Avalanche Effect adalah perubahan kecil bit (misalnya, satu bit) baik pada plainteks maupun kunci yang akan menyebabkan perubahan signifikan terhadap hasil dari cipherteks. Rumus untuk menghitung avalanche effect menggunakan persamaan 3.



Gambar 5. Dekripsi Algoritma Vigenere dan AES

$$\text{Avalance effect} = \frac{\text{jumlah perubahan bit}}{\text{jumlah seluruh bit chiperteks}} \text{ x } 100\% \quad (3)$$

Pada umumnya bit pada cipherteks akan mengalami perubahan dari jumlah bit pada plainteks sebesar 50%. Suatu avalanche effect dikatakan baik jika perubahan bit yang dihasilkan berkisar antara 45-60% (sekitar separuhnya). Semakin banyak perubahan bit yang terjadi mengakibatkan akan semakin sulit algoritma kriptografi tersebut untuk dipecahkan [10].

Percobaan 1

Pengujian pertama yaitu merubah satu

karakter terakhir dari plainteks. Maka didapatkan kata "jayalahITATS2015" (merubah karakter '4' (00110100) menjadi '5' (00110101)). Hasil pengujian percobaan 1 dapat dilihat pada tabel 1. Tabel 1 menunjukkan perubahan bit dari algoritma AES yang telah dimodifikasi. Nilai avalanche effect algoritma modifikasi AES lebih besar dari algoritma AES yaitu sebesar 43.75%. Nilai ini lebih besar dibandingkan nilai avalance effect dari algoritma AES sebesar 42.97%. Contoh proses perhitungan dengan menggunakan rumus avalanche effect sebagai berikut :

$$\text{Avalance effect AES} = \frac{55}{128} \text{ x } 100\ \% = 42.97\ \%$$

$$\text{Avalance effect modifikasi AES} = \frac{56}{128} \text{ x } 100\ \% = 43.75\ \%$$

Tabel 1. Perubahan karakter terakhir dari plainteks

	Algoritma Enkripsi	
	AES	Modifikasi AES
Plainteks	jayalahITATS2014	jayalahITATS2014
Key	kampusunggul!*?#	kampusunggul!*?#
Enkripsi plainteks	pfAwaWLpyEYBj3Nv	NiYvZaiNqA8DBc6F
Modifikasi plainteks	jayalahITATS2015	jayalahITATS2015
Modifikasi enkripsi plainteks	/r5+VijilJ9SiGPW	0BWF1xHgo3sV8OlE
Perubahan bit	55	56
Avalanche effect	42.97%	43.75%

Percobaan 2

Pengujian terhadap kunci (key) yang ke-2 yaitu merubah satu karakter terakhir dari kunci. Maka didapatkan kunci (key) "kampusunggul!*?@" (merubah karakter '#' (00100011) menjadi '@' (01000000)). Perubahan karakter terakhir dari key pada percobaan 2 dapat dilihat pada tabel 2.

Tabel 2. Perubahan karakter terakhir dari key

	Algoritma Enkripsi	
	AES	Modifikasi AES
Plainteks	jayalahITATS2014	jayalahITATS2014
Key	kampusunggul!*?#	kampusunggul!*?#
Enkripsi plainteks	pfAwaWLpyEYBj3Nv	NiYvZaiNqA8DBc6F
Modifikasi plainteks	kampusunggul!*?@	kampusunggul!*?@
Modifikasi enkripsi plainteks	FtDAUFI+h3VKWmN2	qyWSO+pjvUqY9g9L
Perubahan bit	48	50
Avalanche effect	37.5%	39.06%

Tabel 2 menunjukkan perubahan bit dengan nilai avalance effect dari algoritma modifikasi AES sebesar 39.06%. Nilai ini lebih besar dibandingkan nilai avalance effect dari algoritma AES sebesar 37.5%.

Percobaan 3

Pengujian terhadap plainteks yang ke-3 yaitu merubah satu karakter yang ada ditengah dari plainteks. Maka didapatkan kata "jayalahIZATS2014" (merubah karakter 'T' (01010100) menjadi 'Z' (01011010)). Perubahan karakter yang ada di tengah plainteks dapat dilihat pada tabel 3.

Tabel 3. Perubahan karakter di tengah plainteks

	Algoritma Enkripsi	
	AES	Modifikasi AES
Plainteks	jayalahITATS2014	jayalahITATS2014
Key	kampusunggul!*?#	kampusunggul!*?#
Enkripsi plainteks	pfAwaWLpyEYBj3Nv	NiYvZaiNqA8DBc6F
Modifikasi plainteks	jayalahIZATS2014	jayalahIZATS2014
Modifikasi enkripsi plainteks	WoYeiYyP+fU82Yhn	lZ89FvhfYvk0jnNK
Perubahan bit	44	51
Avalanche effect	34.38%	39.84%

Tabel 3 menunjukkan perubahan bit yang cukup besar dari algoritma modifikasi AES dengan AES. Nilai dari avalanche effect algoritma modifikasi AES lebih besar yaitu sebesar 39.84%. Nilai ini lebih besar dibandingkan nilai avalance effect dari algoritma AES sebesar 34.38%.

Percobaan 4

Pengujian terhadap kunci (*key*) yang ke-4 yaitu merubah satu karakter yang ada ditengah dari kunci. Maka didapatkan kunci (*key*) "kampusumggul!*?#" (merubah karakter 'n' (01101110) menjadi 'm' (01101101)). Perubahan karakter yang ada di tengah dari key dapat dilihat pada tabel 4.

Tabel 4. Perubahan karakter di tengah dari key

	Algoritma Enkripsi	
	AES	Modifikasi AES
Plainteks	jayalahITATS2014	jayalahITATS2014
Key	kampusunggul!*?#	kampusunggul!*?#
Enkripsi plainteks	pfAwaWLpyEYBj3Nv	NiYvZaiNqA8DBc6F
Modifikasi plainteks	kampusumggul!*?#	kampusumggul!*?#
Modifikasi enkripsi plainteks	E7gmwUk71DsOyrav	p3XHFjCqi79OxlZm
Perubahan bit	44	57
Avalanche effect	34.38%	44.53%

Tabel 4 menunjukkan perubahan bit yang besar dari algoritma modifikasi AES dengan AES. Nilai avalanche effect dari algoritma modifikasi AES lebih besar yaitu sebesar 44.53%. Nilai ini lebih besar dibandingkan nilai avalance effect dari algoritma AES sebesar 34.38%.

	Algoritma Enkripsi	
	AES	Modifikasi AES
Plainteks	jayalahITATS2014	jayalahITATS2014
Key	kampusunggul!*?#	kampusunggul!*?#
Enkripsi plainteks	pfAwaWLpyEYBj3Nv	NiYvZaiNqA8DBc6F
Modifikasi plainteks	kampusunggul!*?@	kampusunggul!*?@
Modifikasi enkripsi plainteks	FtDAUFI+h3VKWmN2	qyWSO+pjvUqY9g9L
Perubahan bit	48	50
Avalanche effect	37.5%	39.06%

Percobaan 5

Pengujian terhadap plainteks yang ke-5 yaitu merubah satu karakter pertama dari plainteks. Maka didapatkan kata "kayalahITATS2014" (merubah karakter 'j' (01101010) menjadi 'k' (01101011)). Perubahan karakter pertama dari plainteks dapat dilihat pada tabel 5.

Tabel 5. Perubahan Karakter Pertama Dari Plainteks

	Algoritma Enkripsi	
	AES	Modifikasi AES
Plainteks	jayalahITATS2014	jayalahITATS2014
Key	kampusunggul!*?#	kampusunggul!*?#
Enkripsi plainteks	pfAwaWLpyEYBj3Nv	NiYvZaiNqA8DBc6F
Modifikasi plainteks	kayalahITATS2014	kayalahITATS2014
Modifikasi enkripsi plainteks	2LheAEaqmJmu6C6/	36uBCzyMMdS+8bPE
Perubahan bit	47	58
Avalanche effect	36.72%	45.31%

Tabel 5 menunjukkan perubahan bit lebih besar dari algoritma modifikasi AES dengan AES. Nilai avalanche effect dari algoritma modifikasi AES naik menjadi 45.31%. Nilai ini lebih besar dibandingkan nilai avalance effect dari algoritma AES sebesar 36.72%.

Percobaan 6

Pengujian terhadap kunci (*key*) yang ke-6 yaitu merubah satu karakter pertama dari kunci. Maka didapatkan kunci (*key*) "xampusunggul!*?#" (merubah karakter 'k' (01101011) menjadi 'x' (01111000)). Perubahan karakter pertama dari key dapat dilihat pada tabel 6.

Tabel 6. Perubahan karakter pertama dari key

	Algoritma Enkripsi	
	AES	Modifikasi AES
Plainteks	jayalahITATS2014	jayalahITATS2014
Key	kampusunggul!*?#	kampusunggul!*?#
Enkripsi plainteks	pfAwaWLpyEYBj3Nv	NiYvZaiNqA8DBc6F
Modifikasi plainteks	xampusunggul!*?#	xampusunggul!*?#
Modifikasi enkripsi plainteks	VHKAIXgaRXYnO+wS	d6tHnMfdrfx9evmg
Perubahan bit	48	58
Avalanche effect	37.50%	45.31%

Tabel 6 menunjukkan perubahan bit yang besar juga dari algoritma modifikasi AES dengan AES. Hasil presentase avalanche effectnya pun lebih besar. Dari hasil semua pengujian 1 sampai 6 diatas, maka didapatkan nilai rata-rata avalanche effect dari algoritma AES adalah sebagai berikut :

$$\frac{42.97 + 37.5 + 34.38 + 34.38 + 36.72 + 37.5}{6} x\ 100\ \% = 37.24\ \%$$

Sedangkan nilai rata-rata avalanche effect dari algoritma modifikasi AES adalah sebagai berikut :

$$\frac{45.75 + 39.06 + 39.84 + 44.53 + 45.31 + 45.31}{6} x\ 100\ \% = 42.96\ \%$$

Dari perhitungan rata-rata nilai *avalanche effect* diatas, menghasilkan nilai rata-rata dari algoritma modifikasi AES lebih besar daripada algoritma AES. Sehingga dapat disimpulkan bahwa algoritma kriptografi modifikasi AES lebih baik daripada algoritma kriptografi AES.

V. SIMPULAN

Berdasarkan dari penelitian yang telah dilakukan, maka dapat diambil kesimpulan bahwa aplikasi enkripsi SMS dapat mengimplementasikan algoritma Vigenere dan Advanced Encryption Standard dalam mengamankan pesan yang dikirim maupun diterima. Dari hasil perhitungan avalanche effect didapatkan nilai rata-rata dari algoritma Vigenere AES sebesar 42.96%, sedangkan algoritma AES hanya sebesar 37.24%. Hal tersebut menunjukkan bahwa algoritma kriptografi Vigenere dan Advanced Encryption Standard (AES) lebih baik dari pada algoritma kriptografi Advanced Encryption Standard (AES).

Beberapa saran pengembangan penelitian selanjutnya yang dapat dikerjakan antara lain menggunakan algoritma asimetris, karena kunci yang digunakan untuk enkripsinya berbeda dengan kunci untuk dekripsinya sehingga kunci akan lebih sulit dipecahkan. Untuk pengembangan selanjutnya diharapkan dapat melakukan proses enkripsi bukan hanya pada layanan pesan singkat (SMS), tapi juga dapat melakukan proses enkripsi pada layanan Multimedia Messaging Service (MMS) maupun e-mail. Selain itu diharapkan dapat dilakukan pada jenis handphone lainnya, seperti Blackberry OS, iOS dan Windows Phone.

DAFTAR PUSTAKA

[1] N. Safaat, "Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android," Bandung: Informatika Bandung, 2012.

[2] D. Ariyus, "Kriptografi Keamanan Data dan Komunikasi," Yogyakarta : Graha Ilmu, 2006.

[3] N. Endriani, "Implementasi Algoritma Enkripsi AES pada Aplikasi SMS berbasis Android," Yogyakarta: STMIK AMIKOM, 2014.

[4] A.K. Dwi, "Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android," Bandung: Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2012.

[5] S.E. Adib, N. Raissouni, "AES Encryption Algorithm Hardware Implementation: Throughput and Area Comparison of 128, 192 and 256-bits Key," International Journal of Reconfigurable and Embedded Systems (IJRES) Vol. 1, No. 2, 2012.

[6] R. Munir, "Kriptografi," Bandung: Informatika, 2006.

[7] D. Selent, "Advanced Encryption Standard," Insight: Rivier Academic Journal, Volume 6, Number 2, 2010.

[8] D. Ariyus, "Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi," Yogyakarta : Andi, 2008.

[9] Dafid, "Kriptografi Kunci Simetris dengan Menggunakan Algoritma Crypton," Palembang : STMIK MDP Palembang, 2006.

[10] Nikita, K. Ranjeet, "A Survey On Secret Key Encryption Technique," India : Department of Computer Science and Engineering, DAV University, 2014.