APPLICATION VERNAM CIPHER AND SECURITY SYSTEM ROT13 SMS (Short Message Services)

[1] *Firlian Okto Hari Pratama (1110651102)*
[2] *Lutfi Ali Muharom,S.Si* [3]*Hardian Oktavianto,S.Si*
Informatic Engineering Program, Engineering Program
Jember Muhammadiyah University
Email : firlianpratama04@gmail.com

ABSTRACT

Algorithm One Time Pad (OTP) algorithm which is relatively easy to learn and has been declared by experts cryptography as "the perfect encryption algorithm". While ROT13 is a substitution code by shifting as much as k = 13. Combined with engineering algorithms base64 encoding characters. Base64 is an encoding characters that represent binary data in ASCII string format to translate into representation 64. By using the Vernam Cipher Algorithm ROT13 as pengamankan text and SMS (Short Message Services) which was implemented in SMS Security Systems obtained the results that this system can perform encryption sms message well to secure messages sent to another number. However, this SMS Message Encryption System can not describe the message that amounted to 160 characters upwards due to the process of message encryption will become more of a plaintext message so that the message delivery process will be deducted per 160 characters (long SMS messages to a maximum of 160 characters) that occurred failure of due process is not complete and the system is very influential on the random key, if randomly generated key can decode and perfectly mengmodulus then the message can be described as good and vice versa.

Keywords: ***SMS, Random, Key, ROT13, OTP.***

PENERAPAN *VERNAM CIPHER* DAN *ROT13* PADA SISTEM KEAMANAN SMS (*Short Message Services*)

Firlian Okto Hari Pratama (1110651102)[1], *Lutfi Ali Muharrom,S.Si*[2], *Hardian Oktavianto,S.Si*[3],

Jurusan Teknik Informatika, Fakultas Teknik

Universitas Muhammadiyah Jember

Email : firlianpratama04@gmail.com

ABSTRAK

Algoritma One Time Pad (OTP) yang merupakan algoritma yang relatif gampang untuk dipelajari dan sudah dinyatakan oleh para ahli kriptografi sebagai "perfect encryption algorithm". Sedangkan ROT13 adalah subtitusi kode dengan melakukan pergeseran sebanyak k=13. Digabungkan dengan teknik algoritma encoding karakter base64. Base64 adalah sebuah encoding karakter yang mewakili data biner dalam format string ASCII dengan menerjemahkannya ke dalam representasi 64. Dengan menggunakan Algoritma Vernam Cipher dan rot13 sebagai pengamankan teks SMS (Short Message Services) yang diimplementasikan pada Sistem Pengamanan SMS didapat hasil bahwa Sistem ini dapat melakukan enkripsi pesan sms dengan baik untuk melakukan pengamanan pesan yang dikirim ke nomor lain. Akan tetapi Sistem Enkripsi Pesan SMS ini tidak dapat mendeskripsikan pesan yang berjumlah 160 karakter ke atas yang dikarenakan pada proses enkripsi pesan akan menjadi lebih banyak dari plainteks pesan sehingga proses pengiriman pesan akan dipotong per 160 karakter (panjang pesan untuk SMS maksimal 160 karakter) sehingga terjadi kegagalan proses karena tidak lengkap serta sistem ini sangat berpengaruh pada random key, jika random key yang dihasilkan dapat mendekode maupun mengmodulus secara sempurna maka pesan dapat dideskripsi secara baik dan sebaliknya.

Kata Kunci **: *SMS, Random, Key, ROT13, OTP.***

1. Pendahuluan

Telepon seluler merupakan alat komunikasi yang umum dipakai oleh sebagian besar umat manusia di dunia. Telepon seluler juga menyediakan media komunikasi yang beragam, salah satunya adalah SMS. Penggunaan SMS menjadi popular di kalangan masyarakat karena dengan begitu mudahnya kita dapat saling bertukar informasi tanpa batasan jarak dan

waktu. Celah keamanan terbesar pada komunikasi via SMS adalah pesan yang dikirimkan akan disimpan di SMSC (Short Message Service Center), yaitu tempat dimana SMS disimpan sebelum dikirim ke tujuan. Pesan yang sifatnya plaintext ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. Akibatnya, informasi penting seperti password, nomer pin, dan lain-lain dapat dibaca oleh orang yang tidak berhak untuk mengetahuinya. Proyek akhir ini akan memberikan alternatif untuk menyelesaikan masalah ini.

Dengan semakin majunya teknologi pada telepon seluler, implementasi suatu algoritma menjadi mungkin dilakukan. Macam-macam algoritma enkripsi antara lain : Vegenere, ROT13, DES, IDEA, AES, Vernam Cipher, Blowfish dan masih banyak lagi.

One Time Pad (OTP) ditemukan pada tahun 1917 oleh G. Vernam dan Major Joseph Mauborgne. OTP sering disebut "Vernam Cipher". OTP merupakan algoritma yang relatif gampang untuk dipelajari dan sudah dinyatakan oleh para ahli kriptografi sebagai "perfect encryption algorithm". Sebelumnya pernah melakukan penelitian tentang penggunaan algoritma OTP untuk sistem pengamanan access database server. Cipher yang tidak dapat dipecahkan dikatakan memiliki tingkat kerahasiaan yang sempurna (perfect secrecy). Satu-satunya algoritma kriptografi sempurna, aman dan tidak dapat dipecahkan adalah One Time Pad.

ROT13 adalah subtitusi kode dengan melakukan pergeseran sebanyak k=13. Digabungkan dengan teknik algoritma encoding karakter base64. Base64 adalah sebuah encoding karakter yang mewakili data biner dalam format string ASCII dengan menerjemahkannya ke dalam representasi 64.

Dengan menggunakan kombinasi 2 algoritma yaitu *One Time Pad* dan *ROT13*, keamanan data menjadi lebih baik karena penyusup harus melewati 2 *layer* keamanan yaitu *ROT13* dan *One Time Pad*. Dari kedua algoritma tersebut, penulis mengimplementasikannya dengan membangun sebuah aplikasi yang dapat meng-*enkripsi* teks pada SMS (*Short Message Services*) sehingga

teks yang terkirim ke nomor tujuan adalah teks yang telah ter-*enkripsi*.

2. Metode Penelitian

2.1. Algoritma One Time Pad

Algoritma ini ditemukan pada tahun 1917 oleh Mayor Joseph Mauborgne dan Gilbert Vernam. Cipher ini termasuk ke dalam kelompok algoritma kriptografi simetri. Cipher ini diimplementasikan melalui sebuah kunci yang terdiri dari sekumpulan random karakter-karakter yang tidak berulang. Setiap huruf kunci dijumlahkan modulo 26 dengan huruf pada plaintext. Pada One Time Pad, tiap huruf kunci digunakan satu kali untuk satu pesan dan tidak digunakan kembali. Panjang stream karakter kunci sama dengan panjang pesan. One time pad (pad = kertas bloknot) berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Satu pad hanya digunakan sekali (one time) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan.

Misalkan, kita akan mengenkripsi kata ‘O N E’ menggunakan algoritma one time pad. Yaitu :

Dimana P adalah plain teks, K adalah kunci, dan C adalah cipher teks. Misalkan A = 0, B = 1, …, Z = 25.

Sehingga :

Plainteks : O N E

Kunci : G N R

Cipherteks : U A V

Yang didapat dari :

(O + G) mod 26 = U, yaitu (14 + 6) mod 26 = 20

(N + N) mod 26 = O, yaitu (13 + 13) mod 26 = 0

(E + R) mod 26 = V, yaitu (4 + 17) mod 26 = 21

Proses dekripsinya dilakukan dengan menggunakan kunci yang sama dengan yang dipakai untuk enkripsi, dengan langkah sebagai berikut :

(U - G) mod 26 = O, yaitu (20 - 6) mod 26 = 14

(A - N) mod 26 = N, yaitu (0 - 13) mod 26 = 13

(V - R) mod 26 = E, yaitu (21 - 17) mod 26 = 4

Algoritma ini memiliki beberapa kelemahan. Yaitu kunci yang dipakai

haruslah benar-benar acak. Menggunakan pseudorandom generator tidak dihitung, karena algoritma ini memiliki bagian yang tidak acak. Panjang kunci juga harus sama dengan panjang pesan, sehingga hanya cocok untuk pesan berukuran kecil. Selain itu, karena kunci dibangkitkan secara acak, maka 'tidak mungkin' pengirim dan penerima membangkitkan kunci yang sama secara simultan. Dan karena kerahasiaan kunci harus dijamin, maka perlu ada perlindungan selama pengiriman kunci. Oleh karena itu, algoritma ini hanya dapat digunakan jika tersedia saluran komunikasi kedua yang cukup aman untuk mengirim kunci.

2.2. Caesar Cipher ROT13

Caesar Cipher ROT13 adalah fungsi yang menggunakan kode Kaisar dengan pergeseran k=13. ROT13 didesain untuk keamanan pada sistem operasi UNIX yang sering digunakan pada forum online, berfungsi untuk menyelubungi isi artikel sehingga hanya orang yang berhak yang dapat membacanya. Sistem enkripsi ROT13 kali ini dengan menggeser maju karakter sebanyak 13 kali, terhitung 1 adalah karakter didepannya, dan pergeseran karakter berdasarkan urutan karakter pada tabel ASCII. Sebagai dekripsinya, dengan menggeser mundur karakter sebanyak 13 kali.

2.3. Base64

Base64 sebenarnya bukanlah algoritma enkripsi, melainkan suatu metoda encoding (penyandian) terhadap data binary ASCII menjadi format 6-bit karakter. Base64 digunakan ketika ada kebutuhan menggabungkan, menyimpan, atau mentransfer data binary dengan data teks. Hal ini untuk memastikan bahwa data tetap utuh tanpa perubahan selama pengiriman. Pada umumnya base64 digunakan pada beberapa aplikasi yaitu email melalui MIME (Multipurpose Internet Mail Extention), dan penyimpanan data yang kompleks dalam XML. Berikut cara kerja base64 dalam melakukan penyandian.

3. Hasil dan Pembahasan

3.1. Rekomendasi Penggunaan Sistem

Rekomendasi minimum perangkat lunak maupun perangkat

keras untuk menjalankan sistem ini sebagai berikut.

• Sistem Operasi : Windows 7 framework 4 (Win 7 Sp1)
• Ms. Office : 2007
• Gammu : Gammu 1.31.90
• Database : MYSQL 5
• Connector : MYSQL Connector Net
• Prosessor : Intel® Pentium® Processor G3220 (3M Cache, 3.00 GHz)
• RAM : 2 GB
• Modem/HP Support : modem/HP yang support untuk SMS gateway dapat dilihat di http://wammu.eu/phones/

4. Kesimpulan Dan Saran

4.1. Kesimpulan

Setelah dilakukan pengujian sistem kedalam 5 kali pengujian, maka dapat disimpulkan bahwa.

1. Sistem ini dapat melakukan enkripsi pesan sms dengan baik untuk melakukan pengamanan pesan yang dikirim ke nomor lain.
2. Sistem enkripsi pesan SMS ini tidak dapat mendekripsikan pesan yang berjumlah 160 karakter ke atas yang dikarenakan pada proses enkripsi pesan akan menjadi lebih banyak dari *plainteks* pesan sehingga proses pengiriman pesan akan dipotong per 160 karakter (panjang pesan untuk SMS maksimal 160 karakter) sehingga terjadi kegagalan proses karena tidak lengkap.
3. Sistem enkripsi pesan SMS ini sangat berpengaruh pada random key, jika random key yang dihasilkan dapat mendekode maupun meng modulus secara sempurna maka pesan dapat didekripsi secara baik dan sebaliknya.
4. Dengan adanya aplikasi ini mampu memberikan keamanan bagi pengguna dalam menggunakan SMS agar orang yang tidak berhak tidak bisa membaca informasi yang ada pada SMS tersebut sehingga

keamanan dan kerahasiaan yang dikirim melalui SMS dapat terjaga.

5. Dan Hasil yang didapatkan pada aplikasi ini cukup baik dikarenakan adanya random kunci yang ada pada aplikasi ini hanya bisa di ketahui oleh pengguna (user) dan si penerima. Dan orang yang tidak berhak tidak bisa mengetahui informasi dari SMS tersebut.

4.2. Saran

Berdasarkan kesimpulan yang telah dikemukakan di atas, penulis akan memberikan beberapa saran yang kiranya dapat menjadi bahan tambah untuk mengembangkan sistem ini lebih lanjut.

Adapun saran-saran tersebut adalah sebagai berikut :

1. Diharapkan untuk pengembangan kedepannya, sistem ini dapat digunakan untuk mengenkripsi pesan yang ada di media sosial seperti facebook, bbm, twitter dan sebagainya.
2. Diharapkan akan ada pengembangan lebih lanjut ke dalam versi mobile(smartphone).
3. Diharapkan untuk pengembangan selanjutnya terdapat fasilitas untuk menguji key agar pengiriman pesan dapat didekripsi secara sempurna.

5. Daftar Pustaka

1. Anggraini.2012. ”Pengamanan Jaringan”. Informatika: Bandung.
2. Ariyus, D. 2008. “Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi”. Andi: Yogyakarta.
3. Ariyus, D. 2009. “Keamanan Multimedia”. Andi: Yogyakarta.Barus,
4. Felix, Fidens. 2006. “Dasar Kriptografi, (online),http://www.ilmukomputer.com”,(diakses Maret 2011).

5. Elveny, M. 2011. “Implementasi Algoritma Elgamal untuk Keamanan Pesan Teks dalam Pengiriman Email”. Skripsi. Universitas Sumatera Utara.
6. Kurniawan, Y. 2004. “Kriptografi: Keamanan Internet dan Jaringan Komunikasi” .Informatika: Bandung.
7. Munir, R. 2006. “Kriptografi.Informatika” : Bandung.
8. Parlindungan, Maulud.2012. “Analisis Dan Perancangan Perangkat Lunak Pemesanan Tiket Pesawat Berbasis Sms Gateway”. Medan : Universitas Sumatera Utara.
9. Wahana, K. 2003. “Memahami Model Enkripsi & Security Data”. Andi: Yogyakarta.
10. Wahana Komputer, 2011. “Panduan Aplikatif dan Solusi (PAS) Mirosoft Visual Basic 2010 dan MySQL Untuk Aplikasi Point Of Sales”. Andi:Yogyakarta