Perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma One Time Pad Berbasis Android

Suvita Sari

[1,] *STMIK Budi Darma Medan Jl. Sisingamangaraja No.338 Simpang Limun Medan, Indonesia*

ARTICLE INFORMATION

Received: February 23,2019
Revised: March 19,2019
Available online: April 08,2019

KEYWORDS

Android, enkripsi, deskripsi, kriptografi, algoritma One Time Pad (OTP)

CORRESPONDENCE

Phone: +62813978623754

E-mail: vitapipet@gmail.com

A B S T R A K

Sistem operasi untuk perangkat mobile semangkin berkembang. Android merupakan salah satu sistem operasi mobile yang kini sangat populer dan banyak digunakan orang-orang. Android juga merupakan sistem operasi yang berbasis perangkat lunak yang dapat dikembangkan secara open source sehingga banyak pengembang yang kini turut serta ikut mengembangkan aplikasi untuk android. Untuk keperluan aspek keamanan, android juga telah menyediakan khusus untuk fungsi-fungsi kriptografi, seperti enkripsi, deskripsi, dan sebagainya. Shost message service (SMS) adalah sebuah teknologi komunikasi yang sangat populer. Dengan menggunakan SMS seseorang dapat saling bertukar informasi. Dalam hal ini SMS yang dikirimkan akan dienkripsi pada pengembangan sebuah program telepon seluler (ponsel) berbasis android untuk pengiriman pesan SMS. Hasil tes menunjukkan bahwa pemanfaatan algoritma One Time Pad (OTP) dapat melakukan enkripsi pesan singkat dengan teks ke nomor tujuan. Aplikasi dapat membantu pengguna untuk mengirim pesan singkat di tempat yang aman, cepat, dan mudah.

1. PENDAHULUAN

Perkembangan teknologi dibidang komunikasi semangkin tahun semangkin maju. Salah satunya adalah telepon seluler (ponsel) dengan banyak fitur dan juga memiliki sistem yang sama dengan komputer. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman pesan singkat melalui Short Message Service (SMS) [1].

Sebagian besar orang lebih sering menggunakan layanan SMS dari pada layanan telepon dikerenakan biaya yang dipakai tergolong mudah dan mudah digunakan. Dalam mengatasi permasalahan pengiriman pesan, penulis mencoba membuat pengamankan pesan dengan algoritma one time pad untuk mengenkripsi pesan yang berjalan pada sistem operasi android sehingga pemilik telepon seluler (ponsel) yang berbasis android dapat melakukan pertukaran pesan dengan lebih aman dan nyaman. One-time pad berisi deretan karakter-karakter kunci yang dibangkitkan secara acak[2].

Berdasarkan uraian masalah pada latar belakang di atas, maka yang menjadi rumusan masalah dari penelitian ini adalah :
1. Bagaimana proses enkripsi dan dekripsi pengamanan pesan?
2. Bagaimana mengimplementasikan algoritma one time pad (OTP) untuk mengamankan pesan teks?
3. Bagaimana merancang aplikasi pengamanan pesan teks berbasis android?

Batasan masalah dalam adalah sebagai berikut :
1. Panjang kunci harus sama dengan panjang plainteks yang akan dienkripsikan.
2. Batas maksimal ukuran plainteks 128 karakter dalam bentuk abjad, angka, dan simbol.
3. Aplikasi ini dapat berjalan minimal di sistem operasi versi Android 2.3
4. Dalam merancang sistem menggunakan software eclipse.

Tujuan dari penulisan skripsi ini adalah sebagai berikut :
1. Menjelaskan proses enkripsi dan dekripsi pengamanan pesan teks.
2. Mengimplementasikan algoritma one time pad untuk mengamankan aplikasi pesan teks berbasis android.
3. Merancang aplikasi pengamanan pesan teks berbasis android dengan penerapan algoritma one time pad.

2. LANDASAN TEORI

2.1 Kriptografi

Kata kriptografi berasal dari bahasa Yunani, "kryptós" artinya "secret" (rahasia) sedangakan *"graphein"* artinya *"writing"* (tulisan). Jadi, kriptografi berarti *"secret writing"* (tulisan rahasia). Ada beberapa defenisi kriptografi yang telah dikembangkan didalam berbagai literatur. Defenisi yang dipakai didalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya[3].

2.2. Algoritma One Time Pad

One Time Pad merupakan klaim yang dibuat oleh kriptografer terhadap algoritma kroptografi yang dirancang. Kriptografer sering disebut bahwa cipher yang dirancang tidak dapat dipecahkan. Jelas terlihat bahwa cipher subsititusi (dengan segala varsinya) dan cipher transposisi pada akhirnya dapat dipecahkan juga[3][4], [5]. Kasus Queen Mary pada abad 18 dan Enigma pada PD II adalah pelajaran betapa klain unbreakable cipher mudah dipatahkan. Untuk merancang unbreakable cipher, ada 2 syarat yang harus dipenuhi:

1. Kunci harus dipilih secara acak yaitu setiap kunci harus mempunyai peluang yang sama untuk terpilih
2. Panjang kunci harus sama dengan panjang plainteks yang akan dienkripsikan.
3. Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci one time pad.
   C1= (p1+k1) mod 26 . . (I)

Yang dalam hal ini , P1 adalah planteks ke-i, k1 adalah huruf kunci ke-i. Panjang kunci sama dengan panjang plainteks, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi. Setelah pengirim mengenkripsikan pesan dengan kunci, ia menghancurkan kunci tersebut. Penerima pesan menggunakan kunci yang sama untuk mendekripsikan karakter-karakter cipherteks menjadi karakter-karakter plainteks dengan persamaan.
P1= (c1+k1) mod 26 . . (II)

Meskipun OTP merupakan cipher yang aman, namun faktanya ia tidak digunakan secara universal dalam aplikasi kriptografi sebagai satu-satunya sistem cipher yang tidak dapat dipecahkan (hanya sedikit sistem komunikasi yang menggunakan OTP)[5][6].

3. HASIL DAN PEMBAHASAN

3.1 Analisa

Analisa masalah bertujuan untuk menguraikan dan menyelesaikan permasalahan yang ada pada sistem aplikasi.

a. Proses Enkripsi Pesan Teks

Dalam proses enkripsi pesan teks dalam One Time Pad, cipherteks diperoleh dengan melakukan penjumlahan modulo 26 dari satu bit plainteks dengan satu bit kunci, seperti terlihat pada rumus
Ci= (pi+ki) mod 26
Dimana :
Ci= cipherteks
Pi = plainteks
Ki = kunci
Sebagai contoh enkripsi, untuk plainteks SUVITASARI dengan kata kunci KRIPTOGRAF, akan menghasilkan cipherteks sebagai berikut :
Plainteks : SUVITASARI
Kunci : KRIPTOGRAF
Cipherteks : CLDXMOYRRN
Yang mana diperoleh sebagai berikut (A = 0, B = 1, ..., Z = 25) :
(S+K) mod 26 = C
(U+R) mod 26 = L
(V+I) mod 26 = D
(I+P) mod 26 = X
(T+T) mod 26 = M
(A+O) mod 26 = O
(S+G) mod 26 = Y
(A+R) mod 26 = R

(R+A) mod 26 = R
(I+F) mod 26 = N

b. Proses Deskripsi Pesan Teks

Sedangkan dalam proses dekripsi, untuk mendapatkan kembali plainteks, diperoleh dengan melakukan penjumlahan modulo 26 dari satu bit cipherteks dengan satu bit kunci :

Pi= (Ci-ki) mod 26

Contoh proses dekripsi, untuk cipherteks SLDXMOYRRN dengan kata kunci KRIPTOGRAF adalah sebagai berikut :

Cipherteks : CLDXMOYRRN
Kunci : KRIPTOGRAF
Plainteks : SUVITASARI

Yang mana diperoleh sebagai berikut (A = 0, B = 1, ..., Z = 25) :

(C-K) mod 26 = S
(L-R) mod 26 = U
(D-I) mod 26 = V
(X-P) mod 26 = I
(M-T) mod 26 = T
(O-O) mod 26 = A
(Y-G) mod 26 = S
(R-R) mod 26 = A
(R-A) mod 26 = R
(N-F) mod 26 = I

c. Algoritma Enkripsi OTP

Algoritma ini melakukan enkripsi terhadap plainteks yang diinputkan seperti berikut:

Input :
Pi ← Plaintext
Ki←Kunci
Output :
Ci←Cipherteks
Proses :
Ci =(Pi+Ki) mod 26

d. Algoritma Deskripsi Pesan

Algoritma ini melakukan deskripsi terhadap plainteks yang diinputkan seperti berikut:

Input :
C←Chipertext
K←Key
Output :
Plaintext
Proses :
Pi = (Ci+Ki) mod 26

5. KESIMPULAN

Dengan adanya aplikasi ini, proses enkripsi dan deskripsi dapat memberikan kemudahan bagi pengguna dalam mengamankan pesan teks. Algoritma One Time Pad (OTP) pada aplikasi pengamanan pesan teks dapat diterapkan sehingga proses enkripsi pesan SMS dapat lebih mudah. 3. Aplikasi enkripsi SMS berbasis mobile android dapat membantu pengguna mengenkripsikan pesan SMS sebelum dikirimkan. Algoritma OTP dapat dikembangkan dengan metode-metode terbaru untuk proses enkripsi dan deskripsi pengamanan pesan teks. Oleh kerena itu penulis menyarankan agar pengembangan selanjutnya dengan fitur-fitur terbaru yang mengikuti perkembangan zaman. Algoritma yang digunakan dalam pengamanan atau enkripsi SMS ini masih dapat digunakan dengan algoritma yang lain misalnya algoritma vigenere cipher

DAFTAR PUSTAKA

[1] T. Limbong and H. D. Hutahaean, "PERANCANGAN SISTEM INFORMASI KEHADIRAN DOSEN DAN JADWAL PENGGANTI PERKULIAHAN DALAM PENINGKATAN KUALITAS LAYANAN PROGRAM

STUDI BERBASIS SHORT MESSAGE SERVICE (SMS)," in *Seminar Nasional Inovasi dan Teknologi Informasi*, 2014.

[2] J. Simarmata, "Aplikasi mobile commerce menggunakan PHP dan MySQL," *Yogyakarta Andi*, 2006.

[3] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.

[4] N. E. Saragih, "IMPLEMENTASI ALGORITMA ONE TIME PAD PADA PESAN," *J. Ilm. Matrik*, vol. 20, no. 1, pp. 31–40, 2018.

[5] F. Diani and Y. Widhiyasana, "Enkripsi SMS dengan Menggunakan One Time Pad (OTP) dan Kompresi Lempel-Ziv-Welch (LZW)," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 7, no. 3, pp. 3–8, 2018.

[6] L. E. Pratiwi, R. Marwati, and I. Yusnita, "APLIKASI KRIPTOGRAFI KOMPOSISI ONE TIME PAD CIPHER DAN AFFINE CIPHER | Firdaus | Jurnal EurekaMatika." [Online]. Available: https://ejournal.upi.edu/index.php/JEM/article/view/9597. [Accessed: 06-Dec-2019].