P-46

IMPLEMENTASI KRIPTOGRAFI PADA APLIKASI DIARY BERBASIS ANDROID MENGGUNAKAN ALGORITMA ONE TIME PAD

IMPLEMENTATION OF ONE TIME PAD ALGORITHM IN ANDROID DIARY APPLICATION

Nidia Enjelita Saragih[1*], Fitriana Harahap[2]
[1,2]Universitas Potensi Utama, Jl. KL Yos Sudarso Km 6.5 No. 3A Tanjung Mulia, Medan

[*]E-mail: nidia.1924@gmail.com

Diterima 07-10-2020	Diperbaiki 15-10-2020	Disetujui 7-12-2020

ABSTRAK

Kemunculan smartphone berbasis android yang digunakan oleh hampir seluruh lapisan masyarakat, membuat banyak aktivitas yang biasanya dilakukan secara manual, berpindah menuju platform digital. Salah satunya adalah kegiatan mengisi buku harian (diary). Pada umumnya, buku harian bersifat privat. Seorang penulis buku harian biasanya tidak mengizinkan semua orang untuk membacanya. Kebutuhan untuk merahasiakan isi dari buku harian ini, bisa terpenuhi dengan menerapkan algoritma kriptografi. Algoritma One Time Pad adalah salah satu algoritma yang tergolong aman. Algoritma ini merupakan algoritma simetris, dimana kunci enkripsi harus sama dengan kunci dekripsi. Setiap karakter pada kunci yang bersifat acak dipasangkan tepat pada satu karakter plainteks untuk menghasilkan ciphertеks yang juga acak.

Kata kunci: Android, Diary, Kriptografi, One Time Pad

ABSTRACT

Nowadays, android smartphone has been used by everyone from all over the world. This make so many human manual activities transform into digital.One of them is writing diary. A diary is a private thing of someone. The writer usually give no permission to others to reading theirs, which mean it need a security. The implementation of cryptography can solve this need. One Time Pad is a secure algorithm in cryptography. One Time Padis a symmetric algorithm that using the same key on encription and decription process. Every random character of key would processed with one character of plaintext ini producing the randomize ciphertext.

Keywords:Android, Diary, Cryptography, One Time Pad

PENDAHULUAN

Dewasa ini, perkembangan dunia teknologi menyentuh hampir setiap lini kehidupan.Terlebih lagi dengan kemunculan *smartphone* berbasis *android* yang digunakan oleh hampir seluruh lapisan masyarakat.

Banyak aktivitas yang biasanya dilakukan secara manual, berpindah menuju *platform* digital. Salah satunya adalah kegiatan mengisi buku harian (diary).

Buku Harian (bahasa Inggris: *diary*) adalah catatan kejadian yang kita alami sehari-hari. Menulis buku harian adalah sebuah sarana untuk mencatat peristiwa dan kejadian menarik yang pernah terjadi, untuk sewaktu-waktu bisa dibaca kembali. Pada umumnya, buku harian bersifat privat. Seorang penulis buku harian biasanya tidak mengizinkan sembarang orang untuk membacanya.

Kebutuhan untuk merahasiakan isi dari buku harian ini, bisa terpenuhi dengan menerapkan aplikasi kriptografi. Setiap catatan dalam buku harian, akan dienkripsi terlebih dahulu menggunakan algoritma kriptografi, sebelum disimpan. Sehingga, jika sewaktu-waktu *smartphone* yang berisi buku harian digital tersebut diakses

oleh orang selain penulisnya (pemilik awal), maka catatan-catatan yang ada di dalamnya tidak akan langsung bisa terbaca sebagaimana tulisan biasa.

Ada banyak algoritma Kriptografi yang berkembang saat ini. Salah satunya adalah algoritma One Time Pad(OTP). OTP adalah algoritma kriptografi yang diklaim sempurna. OTP (*pad* = kertas *blocknote*) berisi deretan karakter-karakter kunci yang dibangkitkan secara acak[1].

Teknik enkripsi ini menggunakan pasangan plaintext dengan sebuah kunci rahasia yang diperoleh secara acak. Kemudian setiap bit dari plaintext dienkripsi dengan mengkombinasikan dengan bit tambahan yang diperoleh dari kunci acak menggunakan penjumlahan modulo[2].

Beberapa penelitian di bidang kriptografi telah dilakukan sebelumnya. Seperti yang dilakukan oleh Giri Adi Nuryanto dalam penelitiannya tentang implementasi kriptografi pada aplikasi memo menggunakan algoritma RSA. Dalam penelitian tersebut dihasilkan sebuah aplikasi memo yang mengamankan setiap catatan yang tersimpan agar tidak langsung bisa diakses oleh orang lain[3].

Penelitian lain dilakukan oleh Hengky Mulyono pada penelitiannya tentang implementasi algoritma One Time Pad pada penyimpanan data berbasis Web. Peneliti menyimpulkan bahwa aplikasi penyimpanan data berbasis web yang mengimplementasikan algoritma *One Time Pad* ini mampu menjamin hanya pemilik data yang bisa mengakses data yang tersimpan.[4].

Berdasarkan penjelasan pada penelitian sebelumnya di atas, dalam penelitian ini diharapkan implementasi algoritma *One Time Pad* pada aplikasi diary mampu menjamin keamanan dan kerahasiaan data.

METODOLOGI

Tahap perancangan aplikasi dimaksudkan akan menentukan bentuk implementasi paling tepat untuk menyelesaikan permasalahan yang telah dijelaskan semuanya.

Algoritma One Time Pad yang akan diimplementasikan dalam penelitian ini merupakan pengembangan dari *Vernam Cipher*. Algoritma OTP merupakan bagiandari block cipher dalam kriptografi klasik menggunakan operasi XOR. OTP akan menjadi algoritmayangtidakterpecahkan apabila memenuhi syarat sebagai berikut:

a) Panjang kunci harus sama dengan panjang plainteks

b) Kunci yang digunakan harus acak dan hanya boleh digunakan satu kali saja[5].

Ciphertext diperoleh dengan melakukan penjumlahan modulo 256. Satu bit plaintextdipasangkan tepat dengan dengan satu bit kunci, seperti terlihat pada rumus di bawah ini[6]:

$$C = (P + K) mod\ 256 \ldots\ldots\ldots (1)$$

Di mana :

C = *Ciphertext* (pesan yang sudah dienkripsi/disandikan)

P = *Plaintext* (pesan yang ingin dienkripsi/disandikan)

K = Kunci acak

Untuk proses dekripsi, atau mengubah kembali cipherteks menjadi plainteks, persamaannya adalah:

$$P = (C - K) mod\ 256 \ldots\ldots\ldots (2)$$

Sebagai contoh, jika diberikan plainteks "ME".

Plainteks = "ME"

Nilai Ascii= 77 69

Algoritma One Time Pad membutuhkan kunci yang panjangnya sama dengan plainteks. Misalkan kunci yang diberikan = 12 15

Dengan menerapkan persamaan enkripsi pada One Time Pad, maka bisa ditentukan cipherteks dengan perhitungan berikut.

P = 77 69

K = 12 15

$c_i = (p_i + k_i) \bmod 256$

C(1) =(77+ 12) mod 256

=89(**Y**)

C (2) =(69+15) mod 256

=84(**T**)

Sehingga :

P = **"ME"**

K= 1215

C= **"YT"**

Cipherteks yang dihasilkan ini sudah tidak lagi memiliki makna yang sama dengan pesan asli.

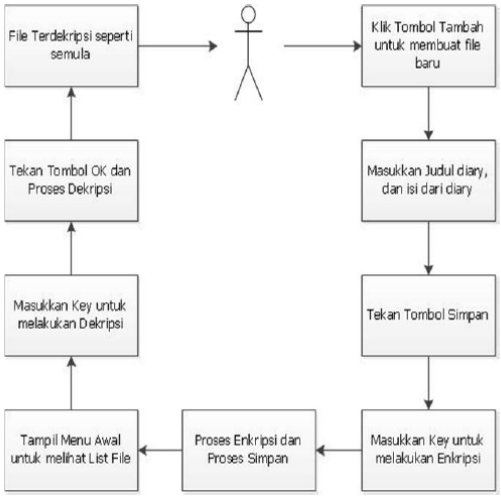
Karena itu, untuk bisa mengembalikan pesan tersandi atau cipherteks ini ke bentuk pesan asli, dibutuhkan proses dekripsi. Yaitu proses mengubah kembali cipherteks menjadi plainteks.

Dalam algoritma One Time Pad, kunci yang digunakan harus sama antara kunci enkripsi dengan kunci dekripsi untuk menjamin bahwa pesan akan kembali ke bentuk asli.

Cipherteks = **“ YT“**
Nilai Ascii = 89 84
K = 12 15
P(1) =(89 – 12) mod 256
=77(M)
P(2) =(84 – 15) mod 256
=69(E)
P = **“ ME”**

Dengan menggunakan kunci yang sama, maka pesan tersandi atau cipherteks bisa kembali menjadi bentuk semula.

Di bawah ini adalah skemaproses enkripsi dan dekripsi rancangan aplikasi *diary*yang akan dibuat:



Gambar 1. Alur Program Enkripsi dan Dekripsi

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini berisi tampilan aplikasi penerapan algoritma OTP pada teks diarymenggunakan android studio.

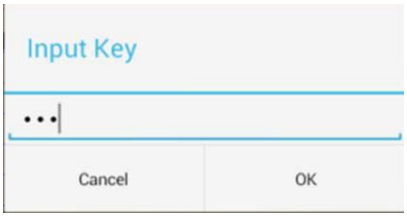
Berikut merupakan tampilan awal dari aplikasi saat pertama kali dijalankan.

Gambar 2. Tampilan buat file baru.

Untuk membuat file baru, pengguna mesti memilih tanda (+), kemudian diminta untuk memasukkan judul dan isi catatan sebagai berikut.

Gambar 3. Menu Menyimpan Catatan

Jika ingin menyimpan catatan, pengguna harus menekan simbol simpan, yang kemudian akan diminta untuk memasukkan kunci yang diinginkan. Catatan yang akan disimpan akan menjadi plainteks. Tampilannya input kunci terlihat gambar berikut .



Gambar 4. Menu Input Kunci.

Dalam algoritma OTP kunci harus sama panjang dengan plainteks, agar setiap karakter kunci bisa dipasangkan tepat dengan satu karakter plainteks. Oleh karena itu, jika kunci yang diinput kurang dari jumlah plainteks, maka kunci yang sama akan diulang secara otomatis mengikuti jumlah plainteks yang diinputkan.

Setelah catatan berhasil disimpan, aplikasi akan menampilkan *interface* berikut :

Gambar 5. Tampilan Setelah Catatan Tersimpan

Untuk mendekripsi file, pengguna tinggal menekan judul catatan yang ingin didekripsi, untuk kemudian mendapat tampilan permintaan kunci berikut :

Gambar 6. Tampilan Permintaan Kunci Dekripsi

Jika kunci yang diinputkan salah, maka catatan tidak akan kembali menjadi catatan asli. Akan tetapi menjadi bentuk lain sebagaimana tampilan berikut :

Gambar 7. Tampilan Dekripsi Salah Kunci

Sedangkan jika kunci benar, maka hasil dekripsi akan kembali menjadi teks asli catatan sebelum dienkrip, sebagaimana terlihat pada tampilan berikut :

Gambar 8. Tampilan Dekripsi

Dilakukan pula beberapa kali pengujian pada aplikasi dengan menggunakan beberapa pesan asli dan kunci pada proses enkripsi dan dekripsi. Hasil pengujian terlihat pada tabel berikut :

Tabel 1. Pengujian Aplikasi

Pengujian	Plainteks	Kunci	Hasil Enkripsi	Hasil Dekripsi
1	DIARY	ABC	...‹„“›	DIARY
2	NIDIA	KEY	™ Ž” †	NIDIA
3	INFORMATIKA		~™‹ ž’ Ÿ Ž š Œ	INFORMATIKA
4	POTENSI	UTAMA	¥£•’	POTENSI
5	KUNCI	ABC	Œ— ‘„‹	KUNCI

Berdasarkan hasil dan pengujian di atas, diketahui bahwa algoritma One Time Pad sebagai algoritma kriptografi simetris cukup tangguh untuk digunakan dalam menjamin kerahasiaan pesan. Catatan yang disimpan dalam aplikasi hanya akan bisa diakses kembali oleh *user* yang memiliki kunci enkripsi yang sama dengan kunci dekripsi. Sekalipun *smartphone* diakses oleh selain *user*

asli, pesan tidak akan bisa diubah kembali ke bentuk asli.

Hanya saja, dalam penerapannya *user* harus bisa mengingat kunci yang digunakan dalam melakukan enkripsi dan dekripsi agar bisa mengakses kembali tulisan yang pernah dibuat sebelumnya.

KESIMPULAN

Berdasarkan penjelasan diatas, dapat diambil kesimpulan bahwa penerapan algoritma one time pad pada aplikasi *diary* berbasis *android*ini terbukti mampu memenuhi aspek kerahasiaan dimana karakter yang dihasilkan dari proses enkripsi tak lagi sama dengan pesan asli. Aplikasi yang mengimplementasikan algoritma *One Time Pad* ini memiliki sistem pengamanan yang menjamin bahwa catatan yang tersimpan dalam *diary* aman dan tidak bisa diakses oleh selain pemiliknya.

SARAN

Setelah mengamati penerapan algoritma *One TimePad* pada aplikasi *diary* berbasis *android*, penulis memiliki beberapa saran untuk menjamin keamanan algoritma tersebut. Antara lain, dalam hal manajemen kunci, pengguna bisa menggunakan kunci yang sama dalam beberapa kali enkripsi, untuk memudahkan mengingat kunci saat ingin melakukan dekripsi. Penambahan menu login dalam aplikasi juga bisa semakin meningkatkan keamanan dari aplikasi.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada yayasan Potensi Utama dan seluruh pihak yang berperan dalam memudahkan penyelesaian penelitian ini.

DAFTAR PUSTAKA

[1] 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), doi: 10.22146/jnteti.v7i3.436.

[2] R. Aulia, A. Zakir, and M. Zulhafiz, “Penerapan Algoritma One Time Pad & Linear Congruential Generator Untuk Keamanan Pesan Teks,” *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 4, no. 1, pp. 37–41, (2019), doi: 10.30743/infotekjar.v4i1.1590.

[3] G. A. Nuryanto *et al.*, “Implementasi Kriptografi Pada Aplikasi Memo Berbasis Android,” pp. 978–979, 2019).

[4] H. Mulyono, “Berbasis Web,” *Peranc. SI Kesehat. web*, (2013), doi: 10.1093/molbev/msm049.

[5] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, “Kombinasi Algoritma One Time Pad Dan Chaotic Sequence Dalam Optimasi Enkripsi Gambar,” *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 8, no. 2, p. 483, (2017), doi: 10.24176/simet.v8i2.1323.

[6] A. Adrian and K. B. Y. Bintoro, “Penerapan Konsep Somatic Hypermutation Dalam Algoritma Enkripsi One-Time Pad,” *J. Ilmu Komput.*, vol. 11, no. 1, p. 1, (2018), doi: 10.24843/jik.2018.v11.i01.p01.