

Aplikasi Pengamanan Data dan Disisipkan Pada Gambar dengan Algoritma RSA Dan Modified LSB Berbasis Android

Muhammad Ridwan Rambe¹, Edy Victor Haryanto², Adil Setiawan³

^{1,2,3}Universitas Potensi Utama

Jl.K.L. Yos Sudarso Km. 6,5 No 3A Tanjung Mulia Medan

Email : ridwan.eno@gmail.com, edyvictor@gmail.com

Abstrak

Menyimpan username dan password beberapa akun yang kita miliki didalam smartphone tentu bukan pilihan tepat mengingat hal tersebut dapat jatuh ketangan orang lain untuk disalahgunakan. Dibutuhkan sebuah aplikasi yang dapat mengamankan teks dalam perangkat android agar keamanan username dan password yang kita simpan didalam smartphone dapat terjaga. Metode kriptografi dapat digunakan untuk merubah teks menjadi bentuk yang tidak bermakna dengan melakukan perhitungan matematika. Namun perubahan bentuk tersebut menimbulkan kecurigaan oleh pihak lain. Metode steganografi hadir untuk menyembunyikan teks kedalam sebuah media agar teks tersebut tidak diketahui oleh orang lain. Dengan melakukan dua kombinasi antara kriptografi dan steganografi diharapkan dapat menjamin keamanan data username dan password setiap akun yang disimpan didalam smartphone berbasis android.

Kata Kunci : Kriptografi, Steganografi, Android, LSB, RSA

1. Pendahuluan

Keamanan untuk menyimpan teks yang berupa username dan password dalam perangkat android tentu harus menjadi perhatian khusus saat ini. Disamping penggunaan smartphone yang sudah meluas, penyalahgunaan teknologi juga ikut meluas mengikuti perkembangan para penggunanya. Diperlukan sebuah aplikasi yang dapat mengamankan teks berisi username dan password akun penggunanya yang disimpan dalam smartphone berbasis android mereka.

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Kriptografi mengubah informasi asli (*plaintext*) melalui proses enkripsi menjadi informasi acak (*ciphertext*) menggunakan algoritma dan kunci tertentu, lalu setelah diterima oleh penerima informasi, *ciphertext* akan diubah kembali menjadi *plaintext* melalui proses dekripsi menggunakan algoritma dan kunci yang sama dengan proses enkripsi [1]. Hal ini membuat pesan yang sudah di enkripsi hanya dapat diketahui oleh sipenerima pesan yang memiliki kunci untuk melakukan proses dekripsi. Namun kriptografi dinilai dapat mengundang kecurigaan oleh pihak lain karena perubahan bentuk menjadi tak bermakna sangat mengundang kecurigaan, oleh karena itu dibutuhkan cara agar dapat menyembunyikan hasil enkripsi kriptografi menjadi tidak diketahui oleh orang lain.

Steganografi lahir dari perkembangan kriptografi dimana ia berperan untuk menyembunyikan pesan kedalam sebuah media agar tidak dapat diketahui keberadaannya oleh orang lain. Steganografi menggunakan teknik substitusi dan mengganti nilai bit – bit terendah pada tiap byte dalam *cover-object* dengan pesan yang ingin disembunyikan adalah metode LSB (*Least Significant Bit*). Metode LSB mengganti nilai bit terkecil yang perubahannya tidak signifikan sehingga menghasilkan *stego-image* yang secara kasat mata terlihat sama dengan *cover-object* [2].

2. Metode Penelitian

a. Teknik Pengumpulan Data

Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis memakai teknik :

1. Penelitian kelapangan

Pada metode ini penulis terjun langsung kelapangan untuk mengumpulkan data yang berkaitan dengan pelaksanaan penelitian yang dikutip dari pengamatan langsung, wawancara, dan *sampling*.

a. Pengamatan langsung (Observation)

Melakukan pengamatan secara langsung ke tempat objek pembahasan yang ingin diperoleh yaitu bagian – bagian terpenting dalam pengambilan data yang diperlukan berkaitan tentang kriptografi dan steganografi.

b. Sampling

Meneliti dan memilih data – data yang tersedia sesuai dengan bidang ilmu yang dipilih sebagai berkas lampiran.

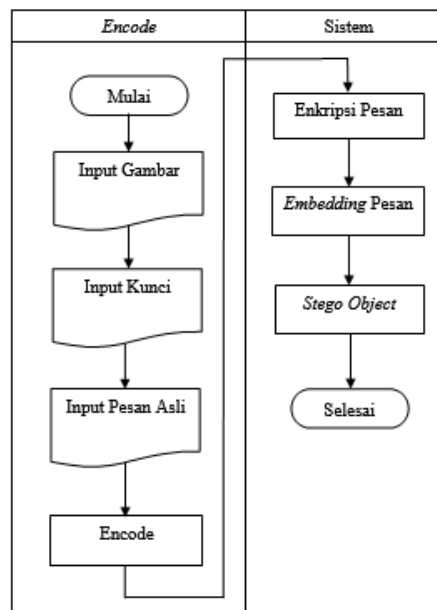
2. Penelitian perpustakaan

Pada metode ini penulis menguti dari beberapa bacaan yang berkaitan dengan pelaksanaan penelitian yang berupa teori – teori yang sudah ada.

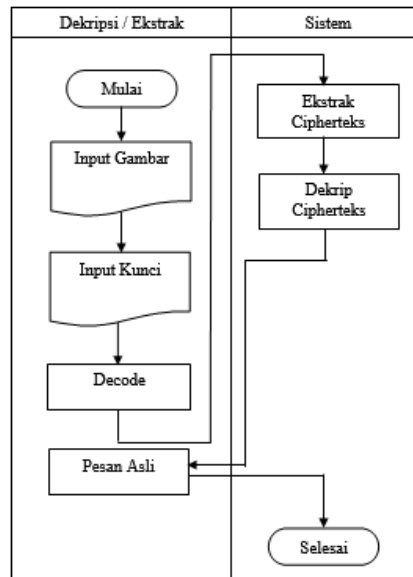
3. Hasil dan Pembahasan

3.1. Penerapan Algoritma RSA dan Metode *Modified* LSB

Pada perancangan aplikasi ini dibutuhkan beberapa perhitungan yang sesuai dengan algoritma dan metode yang digunakan. Adapun bentuk flowchart sistem encode dan decode yang digunakan sebagai berikut :



Gambar 1. Flowchart sistem Encode



Gambar 2. Flowchart sistem Decode

Pada algoritma RSA, dibutuhkan pasangan kunci yang disebut *public key* untuk proses enkripsi dan *private key* untuk proses dekripsi. Berikut adalah rumus pembangkitan kunci :

- a. Menentukan 2 buah bilangan prima.
 Kedua bilangan tidak boleh bernilai sama ($P1 \neq P2$).
- b. Mencari nilai n
 $n = P1 \times P2$
- c. Mencari nilai Φn
 $\Phi n = (P1 - 1) \times (P2 - 1)$
- d. Mencari nilai e
 $e = 2$
 While $\Phi n \bmod e \neq 0$
 $e = e + 1$
 End While
- e. Mencari nilai d
 $U_1 = 1$
 $U_2 = 0$
 $U_3 = \Phi n$
 $V_1 = 0$
 $V_2 = 1$
 $V_3 = e$
 While $V_3 = 0$
 $Q = \text{Int}(U_3 / V_3)$
 $N_1 = U_1 - (Q \times V_1)$
 $N_2 = U_2 - (Q \times V_2)$
 $N_3 = U_3 - (Q \times V_3)$
 $U_1 = V_1$
 $U_2 = V_2$
 $U_3 = V_3$
 $V_1 = N_1$
 $V_2 = N_2$
 $V_3 = N_3$

End While

Tampilan Menu Utama

Tampilan yang diberikan sistem untuk menampilkan Menu Utama dapat dilihat pada gambar 3 berikut :



Gambar 3. Tampilan Menu Utama

1. Tampilan Menu Encode

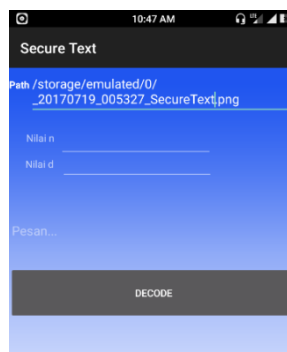
Tampilan yang diberikan sistem untuk menampilkan Menu Encode dapat dilihat pada gambar 4 berikut :



Gambar 4. Tampilan Menu Encode

2. Tampilan Menu Decode

Tampilan yang diberikan sistem untuk menampilkan Menu Decode dapat dilihat pada gambar 5 berikut :





Gambar 5. Tampilan Menu Decode

3.2. Uji Coba

Uji coba aplikasi dilakukan dengan menggunakan aspek *recovery*, dimana data yang disisipkan pada saat dilakukan proses *encode*, akan sama dengan data yang dihasilkan pada proses *decode*. Hal ini bertujuan untuk memastikan bahwa aplikasi yang dibangun sudah berada pada kondisi siap pakai. Berikut adalah hasil pengujian sistem :

Tabel 1. Pengujian sistem dengan aspek *recovery*

No.	Stego Object	Cipherteks Encode	Cipherteks Decode	Kunci	Plainteks Decode
1.	 <p>Name : Butterfly.png</p>	<pre>>?>}@>C}AB@}?>B }A@A}E=}CAE}AB @}>?}=}CE}>}CAE}C <B}DE@}>D=}>?=} A@A}@>C}CAE}A B@}C<B}>?}>?}=}C E}>}E<}CE}>}C<B}A< <}>D=}D<=}C<B}?>E }A@A}DB}CE}>}D<C} AB@}><C}=<?}=<?}</pre>	<pre>>?>}@>C}AB@}?>B }A@A}E=}CAE}AB @}>?}=}CE}>}CAE}C <B}DE@}>D=}>?=} A@A}@>C}CAE}A B@}C<B}>?}>?}=}C E}>}E<}CE}>}C<B}A< <}>D=}D<=}C<B}?>E }A@A}DB}CE}>}D<C} AB@}><C}=<?}=<?}</pre>	d=587 n=943	Universitas Potensi Utama Top Sekali.!!
2.	 <p>Name : Cloud.png</p>	<pre>=@ @<}=ABC}=@> }>@BE}=<=>}>@B E}==<>}=DCE}@D@ }D>@}>@BE}CB@} =>=?}=DCE}=>BD}>EC >A<@}=<=A}>@BE}> @A=}=?E}><E?}>=<E} >@BE}D>@}>@AD}>@ BE}=>=?}=@<A}=@>@ }>@BE}>EC}=@>@}>@ AD}>=?}>@BE}><@} @DC}D><}>}BA?}>@ BE}=D??}BA?}</pre>	<pre>=@ @<}=ABC}=@> }>@BE}=<=>}>@B E}==<>}=DCE}@D@ }D>@}>@BE}CB@} =>=?}=DCE}=>BD}>EC >A<@}=<=A}>@BE}> @A=}=?E}><E?}>=<E} >@BE}D>@}>@AD}>@ BE}=>=?}=@<A}=@>@ }>@BE}>EC}=@>@}>@ AD}>=?}>@BE}><@} @DC}D><}>}BA?}>@ BE}=D??}BA?}</pre>	d=343 n=2501	TIF A Pagi Stambuk 2013 is the best (y) :D XD

4. Kesimpulan

Berdasarkan pembahasan dari penelitian yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Proses *encoding* menggunakan metode *modified* LSB dilakukan dengan menyisipkan bit – bit cipherteks ke dalam byte – byte *cover object*, dimana bit terakhir pada tiap byte *cover object* yang mengalami perubahan. Selanjutnya proses *decoding* dilakukan dengan mengekstrak bit terakhir dari tiap byte *cover object*.
2. Pembangkitan kunci menggunakan bilangan prima yang acak membuat algoritma RSA sulit untuk diketahui karena harus memfaktorkan nilai n yang merupakan perkalian dari bilangan prima p dan q. Untuk menyembunyikan cipherteks hasil enkripsi algoritma RSA, maka dilakukan penyembunyian pada objek gambar menggunakan metode LSB yang sudah dimodifikasi yang penyisipannya dilakukan pada bit – bit terakhir setiap byte.
3. Kombinasi metode keamanan menggunakan metode kriptografi RSA dan steganografi *modified* LSB pada perangkat android yang dibuat dengan pemrograman Eclipse berhasil mencapai tujuan untuk mengamankan data pada perangkat android.

DAFTAR PUSTAKA

- [1] Akbar, M.B. and Haryanto, E.V., 2016. Aplikasi Steganografi dengan Menggunakan Metode F5. *JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi*, 4(2), pp.165-175
- [2] Amin, M. M. (2015). Image Steganography dengan Metode Least Significant Bit (LSB). *CSRID (Computer Science Research and Its Development Journal)*, 6(1), 53-64.
- [3] Arif, Muhammad Husnul, and Ahmad Zainul Fanani. "Kriptografi Hill Cipher dan Least Significant Bit untuk Keamanan Pesan pada Citra." *CSRID (Computer Science Research and Its Development Journal)* 8.1 (2016): 60-72.
- [4] Gede Wisnu Bhaudhayana, dkk, 2015. Implementasi Algoritma Kriptografi AES 256 Dengan Metode Steganografi LSB Pada Gambar Bitmap. *Jurnal Ilmiah Komputer Universitas Udayana*. Vol. 8, No. 2.
- [5] Haryanto, E.V., 2015. Penerapan Metode Adaptif Dalam Penyembunyian Pesan Pada Citra. *Proceedings Konferensi Nasional Sistem dan Informatika (KNS&I)*.
- [6] Haryanto, E. V. (2015). Analisis Masalah Keamanan Jaringan Wireless Komputer Menggunakan Cain. *CSRID (Computer Science Research and Its Development Journal)*, 6(1), 43-52.
- [7] Hutagalung, B. T., & Syahputra, A. (2015). Watermarking Citra Digital Dengan Information Dispersal Algorithm (IDA) Dan Algoritma Huffman. *CSRID (Computer Science Research and Its Development Journal)*, 7(2), 91-104.
- [8] Joko Dewanto, dkk, 2013. Pembuatan Aplikasi RSA Dengan Android. *Forum Ilmiah*, Vol. 10, No. 2.
- [9] S. E. V. Haryanto, M. Y. Mashor, A. S. A. Nasir and H. Jaafar, "A fast and accurate detection of Schizont plasmodium falciparum using channel color space segmentation method," *2017 5th International Conference on Cyber and IT Service Management (CITSM)*, Denpasar, 2017, pp. 1-4.
- [10] S. E. V. Haryanto, M. Y. Mashor, A. S. A. Nasir and H. Jaafar, "Malaria parasite detection with histogram color space method in Giemsa-stained blood cell images," *2017 5th International Conference on Cyber and IT Service Management (CITSM)*, Denpasar, 2017, pp. 1-4.