PENGAMANAN PESAN TEKS DENGAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB)

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika

Oleh:

Nisrina Ulfah

1501077

DEPARTEMEN PENDIDIKAN MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2020

PENGAMANAN PESAN TEKS DENGAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB)

Oleh
Nisrina Ulfah

Sebuah skripsi yang diajukan untuk memenuhi syarat memperoleh gelar Sarjana Matematika Program Studi Matematika Konsentrasi Terapan

Universitas Pendidikan Indonesia
Januari 2020

LEMBAR PENGESAHAN

NISRINA ULFAH

PENGAMANAN PESAN TEKS DENGAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB)

Disetujui dan disahkan oleh pembimbing

Pembimbing I

Dra. Hj. Rini Marwati, M.S.

NIP 196606251990012001

Pembimbing II

Ririn Sispiyati, S.Si., M.Si.

NIP 198106282005012001

Mengetahui,

Ketua Departemen Pendidikan Matematika

Dr. H. Dadang Juandi, M.Si.

NIP 196401171992021001

PENGAMANAN PESAN TEKS DENGAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB)

ABSTRAK

Suatu pengamanan data diperlukan untuk menjaga informasi yang bersifat rahasia. Terdapat metode untuk menjaga keamanan informasi tersebut, salah satunya dengan kriptografi dan steganografi. Penggabungan kriptografi dan steganografi ini bertujuan untuk meningkatkan keamanan pesan. Pada penelitian ini penulis akan mengkaji tentang penggabungan kriptografi AES dan steganografi LSB serta mengetahui cara pengimplementasian dalam mengamankan pesan. Metode yang digunakan adalah metode kriptografi AES-128 dengan steganografi LSB terurut. Proses enkripsi AES-128 memerlukan 10 ronde, setiap ronde AES membutuhkan satu kunci hasil dari pembangkitan kunci. Proses enkripsi AES setiap rondenya menggunakan 4 transformasi yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundkey*. Sedangkan proses dekripsi menggunakan *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundkey*. *Stego image* yang dihasilkan dari metode LSB memiliki gambar yang tidak terlihat perbedaannya dengan gambar yang asli. Dalam proses penggabungannya terdapat 3 tahapan, yaitu pembangkitan kunci, *encoding*, dan *decoding*. Selain itu, hasil pengimplementasiannya berupa program aplikasi komputer dengan bahasa pemrograman Python 3.7.

Kata Kunci: Pengamanan Pesan, Kriptografi, Steganografi, *Advanced Encryption Standard*, *Least Significant Bit.*

SECURING TEXT MESSAGES WITH ADVANCED ENCRYPTION STANDARD (AES) CRYPTOGRAPHY AND LEAST SIGNIFICANT BIT (LSB) STEGANOGRAPHY

ABSTRACT

Data security is required to keep the information confidential. There are methods for maintaining the security of that information, such as cryptography and steganography. The application of AES and LSB aims to improve message security. In this study we examines the combination of AES cryptography and LSB steganography and knows how to implement it in securing messages. The method used are the AES-128 cryptographic method with sequential LSB steganography. AES-128 encryption process requires 10 rounds, each round of AES requires one key outcome of key generation. AES encryption process each round using 4 transformation that is SubBytes, ShiftRows, MixColumns, and AddRoundkey. While the decryption process using InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundkey. Stego image generated from the LSB method has an image that does not look different from the original image. In the process of merging there are 3 stages, namely key generation, encoding, and decoding. In addition, the results of its implementation are in the form of a computer application program with the Python 3.7 programming language.

Keywords: *Securing Messages, Cryptography, Steganography, Advanced Encryption Standard, Least Significant*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Anonim. (2001). ASCII Codes Table. [Online]. Diakses dari: https://ascii.cl/.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis dan Implementasi.* Yogyakarta: Penerbit Andi.

Batarius, P., & Maslim M. (2012). *Perbandingan Metode dalam Teknik Steganografi*. Semarang: Seminar Nasional Teknologi Informasi & Komunikasi Terapan.

Fauji, S. A., Pradana, M. S., & Azhari, N. A. *PENERAPAN KODE HUFFMAN PADA ALGORITMA RSA (RIVEST-SHAMIR-ADLEMAN) UNTUK MENYANDIKAN PASSWORD EMAIL*. *Jurnal UJMC*, 2 (1), hlm. 41-49.

Kromodimoeljo, S. (2009). *Teori dan Aplikasi Kriptografi.* SPK IT Konsulting.

Mufadilah, A. T. (2019). *IMPLEMENTASI KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) YANG DITINGKATKAN DAN STEGANOGRAFI LEAST SIGNIFICANT BIT (LSB)*. Universitas Pendidikan Indonesia.

Muis, A. (2011). *STEGANOGRAFI METODE LEAST SIGNIFICANT BIT PADA CITRA BITMAP DENGAN TEKNIK KOMPRES DATA DAN EKSPANSI WADAH*. (Skripsi). Makassar: Universitas Islam Negeri Alauddin.

Munir, R. (2007). *Kriptografi*. Bandung: Penerbit Informatika.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). *IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD*. *Jurnal Informatika Mulawarman*, 10 (1), hlm. 20-31.

Sianipar, R.H. (2013). *Pemrograman MATLAB dalam Contoh dan Terapan*. Bandung: Informatika.

Suhardi. (2016). *APLIKASI KRIPTOGRAFI DATA SEDERHANA DENGAN METODE EXLUSIVE-OR (XOR). Jurnal Teknovasi*, 3 (1), hlm. 23-31.

Surian, D. (2006). *Algoritma Kriptografi AES Rijndael*. *Jurnal Teknik Elektro*, 97-101.

Sutoyo, T., dkk. 2009. Teori Pengolahan Citra Digital. Yogyakarta: Penerbit Andi.

Tarigan, P. B. (2010). *KRIPTOGRAFI MODERN*. 15-19

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). *Kriptografi Advanced Encryption Standart (AES) untuk Penyandian File Dokumen*. Bandung: Universitas Islam Bandung.

Velarosdela, R. N. (2019). *2 Tersangka Penipu Bermodus Retas Akun WhatsApp Dirut Tempo Ditangka*p. Retrieved Juli 12, 2019, from Kompas website: https://megapolitan.kompas.com/read/2019/07/12/14462061/2-tersangka-penipu-bermodus-retas-akun-whatsapp-dirut-tempo-ditangkap

Yuniati, V., Indriyanta, G., & Rachmat, A. (2009). *ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 256*. *Jurnal Informatika*, 5 (1), hlm. 22-31.