IMPLEMENTASI KRIPTOGRAFI *RIVEST SHAMIR ADLEMAN* (RSA) YANG DITINGKATKAN DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB)

SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika

oleh:

Andika Triani Mufadilah

1503869

PROGRAM STUDI MATEMATIKA

DEPARTEMEN PENDIDIKAN MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2019

IMPLEMENTASI KRIPTOGRAFI *RIVEST SHAMIR ADLEMAN* (RSA) YANG DITINGKATKAN DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB)

Oleh

Andika Triani Mufadilah

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

Universitas Pendidikan Indonesia

Mei 2019

LEMBAR PENGESAHAN

ANDIKA TRIANI MUFADILAH

IMPLEMENTASI KRIPTOGRAFI *RIVEST SHAMIR ADLEMAN* (RSA)
YANG DITINGKATKAN DAN STEGANOGRAFI
LEAST SIGNIFICANT BIT (LSB)

disetujui dan disahkan oleh pembimbing

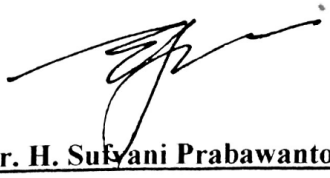
Pembimbing I

Dra. Hj. Rini Marwati, M.S.
NIP 196606251990012001

Pembimbing II

Ririn Sispiyati, S.S., M.Si.
NIP 198106282005012001

Mengetahui
Ketua Departemen Pendidikan Matematika



Dr. H. Sufyani Prabawanto, M. Ed.
NIP 196008301986031003

IMPLEMENTASI KRIPTOGRAFI *RIVEST SHAMIR ADLEMAN* (RSA) YANG DITINGKATKAN DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB)

ABSTRAK

Seiring perkembangan teknologi, kejahatan pada dunia maya semakin marak. Oleh sebab itu, keamanan dalam berkomunikasi perlu ditingkatkan. Penggabungan antara kriptografi dan steganografi bertujuan untuk meningkatkan keamanan pesan. Kriptografi asimetris memiliki tingkat keamanan yang lebih tinggi dibandingkan kriptografi simetris, karena pada proses enkripsi dan dekripsi kriptografi asimetris menggunakan kunci yang berbeda. Salah satu kriptografi asimetris yaitu *Rivest Shamir Adleman* (RSA). Kriptografi RSA menggunakan dua buah bilangan prima untuk membangkitkan kunci. Metode steganografi yang keamanannya tetap terjaga salah satunya adalah *Least Significant Bit* (LSB). Metode LSB menghasilkan gambar yang tidak terlihat perbedaannya dengan gambar aslinya sehingga sulit untuk diketahui keberadaan pesannya. Dalam penelitian ini disajikan penggabungan kriptografi RSA dan steganografi LSB. Dalam penggabungan tersebut, dilakukan peningkatan keamanan dengan membangkitkan kunci kriptografi RSA yang membutuhkan tiga buah bilangan prima. LSB yang digunakan merupakan LSB secara acak. Bilangan acak yang dibangkitkan menggunakan *pseudorandom number generator* (PRNG). Selain itu, hasil penelitian diimplementasikan menjadi suatu program aplikasi komputer menggunakan bahasa pemrograman Python versi 3.7.

Kata kunci: Kriptografi, steganografi, RSA, RSA yang ditingkatkan, *Least Significant Bit*

THE IMPLEMENTATION OF IMPROVED RIVEST SHAMIR ADLEMAN (RSA) CRYPTOGRAPHY AND STEGANOGRAPHY LEAST SIGNIFICANT BIT (LSB)

ABSTRACT

Along with the development of technology, cyber crimes increase widely. Therefore, security in communications need to be improved. The purpose of the combination of cryptography and steganography is to improve the security of message. The safety of asymmetric cryptography is higher than cryptography symmetric because the process encryption and decryption of asymmetric cryptography use different key. RSA is an example of asymmetric cryptography. RSA cryptography uses two prime number to generate keys. One of the most secure method of steganography is Least Significant Bit (LSB). LSB method produce image that has no different with the original image, so the existence of message is unknown. This research used the combination of the RSA cryptography and steganography LSB. With this combination, its process improved the security of message with three primes number were needed to generate keys of RSA. The random LSB was used for this research. The random numbers are generated by pseudorandom number generator (PRNG). In addition, the results of the study were implemented into a computer application program using the Python programming language version 3.7.

Keywords: Cryptography, steganography, RSA, improved RSA, *Least Significant Bit*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

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

Anonim. (2001). *Python (Programming Language)*. [*Online*]. Diakses dari: https://en.wikipedia.org/wiki/Python_(programming_language).

Anonim. (2011). *Spyder (Software)*. [*Online*]. Diakses dari: https://en.wikipedia.org/wiki/Spyder_(software).

Arifin, R., & Oktoviana, L. T. (2013). *Implementasi Kriptografi dan Steganografi Menggunakan Algoritma RSA dan Metode LSB*. Malang: Universitas Negeri Malang.

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

Boucinha, F. (2011). *A Survey of Cryptanalitic Attacks on RSA*. (Tesis). Lisbon: Instituto Superior Tecnico.

Cameron, P. J. (2003). *Notes on Cryptography*. London: University of London.

Durfee, G. (2002). *Cryptanalysis of RSA using Algebraic and Lattice Methods*. (Disertasi). Standford: Standford University.

Firdaus, J. (2017). *Penyandian Pesan Menggunakan Kombinasi Algoritma yang Ditingkatkan dan Algoritma ElGamal*. (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia.

Hermawati, M., Pangestu, A.D., & Prasetyo, L. A. (2017). *Implementasi Steganografi dan Kriptografi pada Media Gambar dengan Menggunakan Metode Least Significant Bit dan Algoritma Vigenere Cipher.* Jakarta: Universitas Indraprasta PGRI.

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

Kusumanto, RD., & Tompunu, A. N. (2011). *Pengolahan Citra Digital untuk Mendeteksi Obyek Menggunakan Pengolahan Warna Model Normalisasi RGB*. Semarang: Seminar Nasional Teknologi Informasi & Komunikasi Terapan.

Mardhatillah, D. (2017). *Implementasi Steganografi Least Significant Bit dan Algoritma Super Enkripsi pada File Citra*. (Skripsi). Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sumatera Utara.

Munir, R. (2006). *Kriptografi*. Bandung: Informatika.

Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An introduction to the theory of numbers.* John Wiley & Sons, Inc.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices, Fourt Edition*. Prentice Hall.

Stinson, D. (2006). *Cryptography: theory and practice.* CRC Press, Inc.

Wirdasari, D. (2008). Prinsip Kerja Kriptografi dalam Mengamankan Informasi. *Jurnal Saintikom*, 5 (2), hlm. 174-184. doi: https://prpm.trigunadharma.ac.id/public/fileJurnal/42481-OK-Jurnal6-DW-Comsec2-174-184.pd