IMPLEMENTASI STEGANOGRAFI KOMBINASI *LEAST SIGNIFICANT BIT* DAN *BLUM BLUM SHUB* DENGAN KRIPTOGRAFI VIGÈNERE *CIPHER* UNTUK PENYISIPAN PESAN RAHASIA DALAM GAMBAR

SKRIPSI

Diajukan untuk memenuhi syarat untuk memperoleh gelar Sarjana Matematika

Oleh:

Rizky Firman Ardhiansyah

1702308

PROGRAM STUDI MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2023

LEMBAR HAK CIPTA

IMPLEMENTASI STEGANOGRAFI KOMBINASI *LEAST SIGNIFICANT BIT* DAN *BLUM BLUM SHUB* DENGAN KRIPTOGRAFI VIGÈNERE *CIPHER* UNTUK PENYISIPAN PESAN RAHASIA DALAM GAMBAR

Oleh :

Rizky Firman Ardhiansyah

NIM 1702308

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Agustus 2023

LEMBAR PENGESAHAN

RIZKY FIRMAN ARDHIANSYAH

IMPLEMENTASI STEGANOGRAFI KOMBINASI *LEAST SIGNIFICANT BIT* DAN *BLUM BLUM SHUB* DENGAN KRIPTOGRAFI VIGÈNERE *CIPHER* UNTUK PENYISIPAN PESAN RAHASIA DALAM GAMBAR

Disetujui dan disahkan oleh pembimbing:

Pembimbing I

Dra. Hj. Rini Marwati, M.S.

NIP. 196606251990012001

Pembimbing II,

Dr. Al Azhary Masta, M.Si.

NIP. 199006102015041001

Mengetahui,

Ketua Program Studi

Dr. Kartika Yulianti, M.Si.

NIP. 198207282005012001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Implementasi Steganografi Kombinasi *Least Significant Bit* dan *Blum Blum Shub* dengan kriptografi Vigenère *Cipher* untuk penyisipan pesan rahasia dalam gambar." ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, 6 Agustus 2023

Yang Membuat Pernyataan,

Rizky Firman Ardhiansyah

NIM. 1702308

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan memanjatkan puji syukur kehadirat Allah SWT, serta rahmat shalawat dan salam untuk junjungan besar Nabi Muhammad SAW penulis dapat menyelesaikan skripsi yang berjudul: "Implementasi Steganografi Kombinasi *Least Significant Bit* dan *Blum Blum Shub* dengan kriptografi Vigenère *Cipher* untuk penyisipan pesan rahasia dalam gambar".

Penulisan skripsi ini diajukan untuk memenuhi sebagian persyaratan untuk memperoleh gelar sarjana matematika di Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia. Penulis menyadari di dalam penulisan ini masih terdapat kekurangan-kekurangan yang disebabkan oleh keterbatasan dan kemampuan penulis. Oleh karena itu, penulis sangat mengharapkan saran dan kritik yang membangun untuk menyempurnakan skripsi ini.

Semoga Allah SWT melimpahkan rahmat dan karunia-Nya serta membalas kebaikan semua pihak yang telah membantu penulis dalam penyusunan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi penulis khususnya dan bagi pembaca pada umumnya.

Wassalamu'alaikum Wr. Wb.

Bandung, 6 Agustus 2023

Rizky Firman Ardhiansyah

NIM. 1702308

UCAPAN TERIMA KASIH

Dengan memanjatkan puji syukur kehadirat Allah SWT, serta rahmat shalawatdan salam untuk junjungan besar Nabi Muhammad SAW penulis dapat menyelesaikan skripsi dengan tepat waktu. Selesainya skripsi ini tidak terlepas dari dukungan, bantuan dan doa berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua tercinta Ibu Titi Sumiati dan Bapak Sukirno Ardianto, kakak-kakak penulis Iis Susanti dan Fitriana Liniawati yang telah memberikan dorongan serta doa dan kasih sayang agar selalu berusaha dengan maksimal dan senantiasa bersyukur.
2. Yth. Ibu Dra. Hj. Rini Marwati, M.S. selaku Pembimbing I yang telah meluangkan waktunya untuk memberikan arahan yang sangat membantu penyusunan dari awal hingga akhir penulisan skripsi ini;
3. Yth. Bapak Dr. Al Azhary Masta, M.Si. selaku Pembimbing II yang telah meluangkan waktunya untuk memberikan arahan yang sangat membantu penyusunan dari awal hingga akhir penulisan skripsi ini;
4. Yth. Ibu Dr. Khusnul Novianingsih, M.Si. selaku dosen Pembimbing Akademik yang telah memberikan arahan serta motivasi selama penulis menjalani perkuliahan S1;
5. Yth. Ibu Dr. Kartika Yulianti, M.Si. selaku Ketua Program Studi Matematika Universitas Pendidikan Indonesia;
6. Yth. Ibu Ririn Sispiyati, S.Si., M.Si. selaku Ketua KBK Terapan Program Studi Matematika Prodi Matematika Universitas Pendidikan Indonesia;
7. Seluruh Civitas Akademika Prodi Matematika dan Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Matematika;
8. Teman-teman Matematika C 2017 yang tidak bisa disebutkan namanya satu persatu, tetapi selalu menjadi teman seperjuangan terbaik yang saling mendukung, menyemangati, dan mendo'akan satu sama lain.
9. Teman-teman *Discord* Bella Saufika Pratiwi, N.Lingharsa Putra, Muhammad Rafi Parama Artha, Zikry Maulana Hamdani, Andre Syahril,

Mochammad Renara Auzar, Hilman Lukman Nulhakim, Alexander Vitorio Napitupulu dan Maulana Firman Nurdiansyah yang telah memberi dukungan, bantuan dan do’a

ABSTRAK

"IMPLEMENTASI STEGANOGRAFI KOMBINASI *LEAST SIGNIFICANT BIT* DAN *BLUM BLUM SHUB* DENGAN KRIPTOGRAFI VIGÈNERE *CIPHER* UNTUK PENYISIPAN PESAN RAHASIA DALAM GAMBAR"

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 simetris, seperti Vigènere *Cipher*, menjadi salah satu pilihan dalam menjaga kerahasiaan pesan. Kriptografi simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sehingga meminimalkan kerentanan pada proses pertukaran kunci. Metode steganografi yang tetap menjaga keamanan pesan adalah *Least Significant Bit* (LSB). Metode LSB memanfaatkan *bit-bit* terakhir dalam data gambar untuk menyembunyikan pesan rahasia. Dalam hal ini, pesan disisipkan secara acak pada *bit-bit* tersebut dengan memanfaatkan algoritma *Blum Blum Shub*, sehingga sulit dideteksi keberadaannya oleh pihak lain. Dalam penelitian ini, dilakukan penggabungan antara kriptografi Vigènere dan steganografi LSB. Tujuannya adalah untuk meningkatkan keamanan pesan dengan memanfaatkan Vigènere *Cipher* sebagai metode enkripsi pesan dan LSB menggunakan algoritma *Blum Blum Shub* sebagai metode steganografi. Kunci kriptografi Vigènere yang digunakan dapat dibangkitkan dengan menggunakan beberapa kunci acak yang sesuai dengan panjang pesan. Bilangan acak yang digunakan dalam proses steganografi LSB dihasilkan *Blum Blum Shub*. *Blum Blum Shub* memungkinkan pembangkitan bilangan acak secara deterministik berdasarkan nilai-nilai awal yang ditentukan. Dengan demikian, penggunaan *Blum Blum Shub* pada metode LSB dapat meningkatkan keamanan pesan. Penelitian ini diimplementasikan menjadi program aplikasi komputer menggunakan bahasa pemrograman *Python* versi 3.9.13

Kata Kunci: *kriptografi, steganografi, Vigènere cipher, LSB acak blum blum shub, Python.*

ABSTRACT

"IMPLEMENTATION OF STEGANOGRAPHY USING A COMBINATION OF LEAST SIGNIFICANT BIT AND BLUM BLUM SHUB WITH VIGÈNERE CIPHER CRYPTOGRAPHY FOR EMBEDDING SECRET MESSAGES IN IMAGES"

With the advancement of technology, cybercrime has become increasingly prevalent. Therefore, the security of communication needs to be enhanced. The integration of cryptography and steganography aims to improve message security. Symmetric cryptography, such as the Vigènere Cipher, is one of the options for preserving message confidentiality. Symmetric cryptography utilizes the same key for the encryption and decryption processes, minimizing vulnerabilities in key exchange. The Least Significant Bit (LSB) method is a steganography technique that maintains message security. LSB exploits the least significant bits in image data to conceal secret messages. In this case, the message is randomly embedded in these bits, utilizing the Blum Blum Shub algorithm, making it difficult to detect by unauthorized parties. This research involves the combination of Vigènere cryptography and LSB steganography. The objective is to enhance message security by employing the Vigènere Cipher as the message encryption method and LSB with the Blum Blum Shub algorithm as the steganography method. The cryptographic key for the Vigènere encryption can be generated using several random keys corresponding to the message length. Random numbers utilized in the LSB steganography process are generated using the Blum Blum Shub algorithm. Blum Blum Shub enables the deterministic generation of random numbers based on predefined initial values. Thus, the use of Blum Blum Shub in the LSB method can enhance message security. Furthermore, the findings of this research are implemented in a computer application program using Python programming language version 3.9.13.

Keywords: *cryptography, steganography, Vigenère cipher, random LSB, Python.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Atqiya, S. N. (2023). *Implementasi Kriptografi Dalam Pengamanan Data Pada File Excel Dengan Diffie-Hellman-RSA* (Repository UPI) 05 Mei 2023

Bharti, S. S., Gupta, M., & Agarwal, S. (2019). A novel approach for audio steganography by processing of amplitudes and signs of secret audio separately. *Multimedia Tools and Applications*, *78*(16), 23179-23201. https://doi.org/10.1007/s11042-019-7630-4

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital watermarking and steganography*. Morgan kaufmann.

Durbin, J. R. (2009). *Modern Algebra: An Introduction, 6th ed.* (L. R. S. Corliss (ed.); 6th ed.). Laurie Rosatone.

Enterprise, J. (2017). *Otodidak Pemrograman Python*. Elex Media Komputindo.https://books.google.co.id/books?id=K-M8DwAAQBAJ&printsec=frontcover&hl=id#v=onepage&q&f=false

Harahap, M. K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, *1*(1), 61-64. http://dx.doi.org/10.30645/j-sakti.v6i1.432

Hikmah, A. N. (2020). *Penyandian Pesan Dengan Menggunakan Kriptografi Hybrid Autokey Vigènere Cipher Dan Algoritma Elgamal* (Skripsi).

Jaya, S. F. B., Kuway, S. M., & Syarifudin, G. (2020). Perancangan Perangkat Lunak Steganografi Menggunakan Least Significant Bit Dengan Enkripsi Vigenere Cipher. *E-JURNAL JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi*, *9*(1), 52-64. https://dx.doi.org/10.36774/jusiti.v9i1.643

Lubis, F. I. (2020). *Analisis Kinerja Modifikasi Algoritma LSB dengan Invers BIT dan Penyisipan Berdasarkan Panjang Pesan* (Tesis).

Maulana, P. A. (2019). Proses enkripsi dan dekripsi pada polinomial dengan menggunakan metode Affine Cipher. http://etheses.uin-malang.ac.id/id/eprint/15009

Mufadilah, A. T. (2019). *Implementasi Kriptografi Rivest Shamir Adleman (RSA) Yang Ditingkatkan Dan Steganografi Least Significant Bit (LSB)* (Skripsi).

Mulyadi, A. Y. (2018). *Implementasi Algoritma AES 128 Dan SHA-256 Dalam Pengkodean Pada Sebagian Frame Video CCTV MPEG-2* (Skripsi)

Mustaqim, D., Suratman, F. Y., & Kurniawan, E. (2015). Perancangan Dan Implementasi Garasi Pribadi Dengan Pintu Otomatis Berdasarkan Pengenalan Plat Kendaraan Berbasis Pengolahan Citra Digital. *eProceedings of Engineering*, *2*(3). https://doi.org/10.14710/jtsiskom.5.3.2017.115-122

Munir, R. (2004). *Teori Bilangan (Number Theory).* Bandung:Departemen Teknik Informatika Institut Teknologi Bandung.

Munir, R. (2010). MATEMATIKA DISKRIT (3rd ed.). *Informatika Bandung*

Munir, Rinaldi. (2019). Bahan Kuliah Pengantar Kriptografi. *Program Studi Informatika, Institut Teknologi Bandung*.

Ndruru, E., & Zebua, T. (2022). Pembangkitan Kunci Beaufort Cipher dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital. *Bulletin of Information Technology (BIT)*, *3*(2), 149-154. https://doi.org/10.47065/bit.v3i2.302

Naufal, M. F., Marwati, R., & Sispiyati, R. (2021). Kriptografi Audio Menggunakan Transposisi dan Affine Cipher yang Dikembangkan dengan Algoritma *Blum Blum Shub*. *Jurnal EurekaMatika*, *9*(1), 1-14. https://ejournal.upi.edu/index.php/JEM/article/view/32634/21764

Saputra, R. A., Windiarti, A., Sarita, I., & Sasilo, A. A. (2021). Implementasi Metode Blum Blum Shub (BBS) Untuk Pengacakan Soal Kuis Pada Aplikasi Media Pembelajaran Ipa Tingkat Sekolah Dasar Kelas 6 Berbasis Mobile. *Proceeding KONIK (Konferensi Nasional Ilmu Komputer)*, *5*, 428-433. https://doi.org/10.54209/jurnalkomputer.v13i02.27

Susanto, A., & Yusnaini, R. Peningkatan Deteksi Steganografi Algoritma Least Significant Bit pada Citra Grayscale. (Skripsi)

Stinson, D. R. & Rosen, K.H. (Penyunting). (2006). *Criptography: Theory and Practice.* 3rd Ed. Chapman & Hall/CRC: Ontario.

Vita, D. (2021). *Penerapan Metode Kriptografi RSA-CRT Dan Metode Steganografi LSB-LCG Pada Sistem Pengamanan Pesan Dengan Media Video*. (Skripsi)

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). Implementasi Caesar Cipher Pada Algoritma Kriptografi Klasik Dalam Penyandian Pesan. *Computer and Science Industrial Engineering (COMASIE), 7*(2),117-126. https://ejournal.upbatam.ac.id/index.php/comasiejournal/article/view/5978

Zuli, F., & Irawan, A. (2014). Penerapan Kombinasi Sandi Caesar Dan Vigenere Untuk Pengamanan Data Pesan Pada Surat Elektronik. *STUDIA INFORMATIKA: JURNAL SISTEM INFORMASI*, *7*(2). https://journal.uinjkt.ac.id/index.php/sisteminformasi/article/view/2173