IMPLEMENTASI KRIPTOGRAFI *HYBRID ADVANCED ENCRYPTION STANDARD* (AES) DAN *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) DENGAN *STEGANOGRAFI LEAST SIGNIFICANT BIT* (LSB) PADA PENGAMANAN PESAN KE DALAM GAMBAR

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika

Oleh:
Bahzar Fadhlal Fikry
1909550

PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2024

IMPLEMENTASI KRIPTOGRAFI HYBRID ADVANCED ENCRYPTION STANDARD (AES) DAN ELLIPTIC CURVE CRYPTOGRAPHY (ECC) DENGAN STEGANOGRAFI LEAST SIGNIFICANT BIT (LSB) PADA PENGAMANAN PESAN KE DALAM GAMBAR

Oleh
Bahzar Fadhlal Fikry

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

Bahzar Fadhlal Fikry
Universitas Pendidikan Indonesia
Januari 2024

LEMBAR PENGESAHAN

BAHZAR FADHLAL FIKRY

IMPLEMENTASI KOMBINASI KRIPTOGRAFI *ADVANCED ENCRYPTION SYSTEM* (AES) DAN *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) DENGAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB) PADA PENGAMANAN PESAN KE DALAM GAMBAR

Disetujui dan disahkan oleh pembimbing:

Pembimbing I

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

Pembimbing II

Dr. Sumanang Muhtar Gozali, M.Si.
NIP. 197411242005011001

Mengetahui,
Ketua Program Studi Matematika

Dr. Kartika Yulianti, S.Pd., M.Si.
NIP. 198207282005012001

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Implementasi Kriptografi *Hybrid Advanced Encryption Standard* (AES) dan *Elliptic Curve Cryptography* (ECC) dengan Steganografi *Least Significant Bit* (LSB) pada Pengamanan Pesan ke dalam Gambar" ini beserta seluruh isinya adalah benar-benar karya saya sendiri, kecuali kutipan-kutipan dari ringkasan yang semuanya telah saya jelaskan sumbernya. Apabila dikemudian hari ditemukan adanya pelanggaran, saya bersedia menanggung resiko atau sanksi yang dijatuhkan kepada saya.

Bandung, Desember 2023

Yang membuat pernyataan,

Bahzar Fadhlal Fikry

KATA PENGANTAR

Puji serta syukur kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Implementasi Kriptografi *Hybrid Advanced Encryption Standard* (AES) dan *Elliptic Curve Cryptography* (ECC) dengan Steganografi *Least Significant Bit* (LSB) pada Pengamanan Pesan ke dalam Gambar" sebagai salah satu syarat memperoleh gelar Sarjana Matematika di Universitas Pendidikan Indonesia (UPI). Harapannya skripsi ini dapat memberikan ilmu pengetahuan mengenai penelitian yang dilakukan oleh penulis.

Penulis menyadari bahwa masih terdapat kekurangan pada skripsi ini yang disebabkan oleh keterbatasan kemampuan penulis, Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun untuk menyempurnakan skripsi ini. Demikian skripsi ini penulis susun, semoga menjadi manfaat dan mohon maaf apabila ada kekurangan.

Bandung, Desember 2023

Penulis

UCAPAN TERIMA KASIH

Penulis menyadari bahwa penulisan skripsi ini tidak terlepas dari dukungan, bantuan, bimbingan dan do'a dari berbagai pihak. Oleh karena itu penulis menyampaikan rasa hormat dan terima kasih kepada:

1. Ibu Dra. Hj. Rini Marwati, M.Si. selaku Dosen Pembimbing I yang telah meluangkan waktunya untuk mengajarkan penulis dengan penuh kesabaran mengenai topik yang penulis bahas dalam skripsi ini.
2. Bapak Dr. Sumanang Muhtar Gozali, M.Si. selaku Dosen Pembimbing II yang telah meluangkan waktunya untuk memberikan arahan, masukan, dan motivasi yang banyak membantu penulis dalam penyusunan skripsi ini.
3. Ibu Dr. Entit Puspita, S.Pd., M.Si. selaku Dosen Pembimbing Akademik yang telah membantu penulis dalam pendampingan akademik selama menjalani perkuliahan di UPI.
4. Ibu Dr. Kartika Yulianti, S. Pd., M. Si. selaku Ketua Program Studi Matematika, Universitas Pendidikan Indonesia.
5. Seluruh dosen dan civitas akademika di lingkungan Prodi Matematika, Universitas Pendidikan Indonesia.
6. Kedua orang tua tercinta yang selalu memberikan dukungan moral, materil, kasih sayang, serta mendo'akan penulis setiap saat.
7. Rekan-rekan mahasiswa UPI yang senantiasa membantu, menemani, dan menghibur penulis selama perkuliahan dan saat penyusunan skripsi ini.
8. Pihak-pihak yang tidak dapat penulis cantumkan namanya, yang telah secara langsung dan/atau tidak langsung memberikan saran dan dukungan, memberi rasa senang, sedih, aman, selama proses penulisan skripsi ini sehingga memotivasi penulis untuk menyelesaikannya.

Semoga dukungan, do'a, bantuan, dan kebaikan yang telah diberikan mendapatkan balasan berkali-kali lipat dari Allah Subhanahu Wa Ta'ala. Aamiin.

ABSTRAK

Dalam era digital yang rentan terhadap risiko kebocoran dan peretasan, perlindungan data sensitif menjadi krusial. Kriptografi telah menjadi elemen kunci dalam melindungi informasi, dengan fokus pada pengembangan keamanan data. Penelitian ini mengusulkan pendekatan yang menggabungkan metode kriptografi *hybrid*, yaitu *Advanced Encryption Standard* (AES) dan *Elliptic Curve Cryptography* (ECC), dengan teknik steganografi *Least Significant Bit* (LSB). Proses implementasi mencakup pembangkitan kunci ECC, enkripsi pesan menggunakan AES, enkripsi kunci AES menggunakan ECC, dan penyisipan hasil enkripsi ke dalam gambar menggunakan metode LSB. Implementasi ini menunjukkan peningkatan keamanan data melalui serangkaian tahapan yang melibatkan teknik kriptografi simetris (AES), kriptografi asimetris (ECC), dan steganografi. Hasil penelitian menunjukkan bahwa pendekatan ini memberikan tingkat keamanan yang tinggi. Pesan terenkripsi yang disisipkan ke dalam gambar juga mengurangi kecurigaan pihak ketiga, menghasilkan perlindungan informasi secara komprehensif.

Kata Kunci: Kriptografi, Kriptografi *Hybrid, Advanced Encryption Standard, Elliptic Curve Cryptography*, Steganografi, *Least Significant Bit*

ABSTRACT

In a digital age vulnerable to the risk of leaks and hacking, the protection of sensitive data becomes crucial. Cryptography has become a key element in protecting information, with a focus on developing data security. The research proposes an approach that combines hybrid cryptography methods, namely Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), with the Least Significant Bit steganography technique (LSB). The implementation process includes generating ECC keys, encrypting messages using AES, encryption of AES keys using ECC, and inserting the result of encryptions into images using the LSB method. This implementation demonstrates improved data security through a series of stages involving symmetrical cryptography (AES), asymmetric cryptography (ECC), and steganography techniques. Research results show that this approach provides a high level of security. Encrypted messages inserted into images also reduce suspicion of third parties, resulting in comprehensive information protection.

Keywords: *Cryptography, Hybrid Cryptography, Advanced Encryption Standard, Elliptic Curve Cryptography, Steganography, Least Significant Bit*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

Abdelfatah, R. I. (2020). Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography. *IEEE Access*, *8*, 3875–3890. https://doi.org/10.1109/ACCESS.2019.2958336

Anwar, N., Munawwar, M., Abduh, M., & Santosa, N. B. (2018). Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(3), 783–791. https://doi.org/10.29207/resti.v2i3.606

Ariyus, D. (2006). *Kriptografi: Keamanan Data dan Komunikasi.* Yogyakarta: Andi.

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

Basri. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer*, *2*(2). http://ejournal.fikom-unasman.ac.id/index.php/jikom/article/view/82%0Ahttp://ejournal.fikom-unasman.ac.id/index.php/jikom/article/download/82/55

Bray, S. W. (2020). *Implementing Cryptography Using Python*. New York: John wiley & Sons Inc.

Dewi, N. P., Sembiring, D. J. ., Ginting, R. br., & Ginting, M. br. (2022). Pengamanan Data dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma Luc Serta Steganografi Chaotic Lsb. *Jurnal Syntax Admiration*, *3*(2). https://doi.org/10.46799/jsa.v3i2.389

Easttom, W. (2021). *Modern Cryptography*. Washington, DC: Springer Cham.

Fauji, S. A., Pradana, M. S., & Azhari, N. A. (2016). Penerapan Kode Huffman Pada Algoritma Rsa (Rivest-Shamir-Adleman) Untuk Menyandikan Password Email. *Jurnal UJMC*, *2*(1), 41–49.

Fikri, M. A., & Ferdinandus, F. X. (2022). Optimasi Teknik Steganografi Amelsbr Pada Empat Bit Terakhir Dengan Cover Image Berwarna. *Antivirus : Jurnal Ilmiah Teknik Informatika*, *16*(1), 25–38. https://doi.org/10.35457/antivirus.v16i1.1967

Gajcowski, N., & Jenkins, M. (2022). Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH). *RFC*, *9212*, 1–10. https://www.rfc-editor.org/rfc/rfc9212.txt

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge: Cambridge University Press.

Hamidah, S. N. (2009). *Konsep Matematis dan Proses Penyandian Kriptografi ElGamal* [Universitas Islam Negeri Maulana Malik Ibrahim]. https://api.semanticscholar.org/CorpusID:171569108

Herstein, I. N. (1975). *Topics in algebra* (2nd ed.). John Wiley and Sons Inc.

Hutahaean, J. (2015). *Konsep sistem informasi*. Deepublish.

Irmayanti, H. (2019). *Operasi Aritmatika Bilangan Biner, Octal Dan Heksadesimal*.

Kumar, D. S., Suneetha, C. H., & ChandrakeshAr, A. (2012). Encryption Of Data Using Elliptic Curve Over Finite Fields. *International Journal of Distributed and Parallel Systems*, *3*(1), 301–308. https://doi.org/10.5121/ijdps.2012.3125

Kuppuswamy, P., & Al-Khalidi, S. Q. Y. (2014). Hybrid encryption/decryption technique using new public key and symmetric key algorithm. *International Journal of Information and Computer Security*, *6*(4), 372–382. https://doi.org/10.1504/IJICS.2014.068103

Lewin, M. (2012). All About XOR. *Overload*, *20*(109), 14–19.

Listiani, I., Nasution, M. S., Sari, W. I., & Nasution, A. B. (2022). Perancangan Keamanan Data Pasien Di Klinik Kecantikan Ratu Beauty Studio Menggunakan Metode Kriptografi Rsa. *JINTEKS (Jurnal Informatika Teknologi Dan Sains)*, *4*(4), 437–443. https://doi.org/10.51401/jinteks.v4i4.2173

Lutfi, S., & Rosihan, R. (2018). Perbandingan Metode Steganografi LSB (Least Significant Bit) Dan MSB (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia Kedalam Citra Digital. *JIKO (Jurnal Informatika Dan Komputer)*, *1*(1), 34–42. https://doi.org/10.33387/jiko.v1i1.1169

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

Marsaid, Jan, R. H., Huda, M., Lydia, E. L., & Shankar, K. (2020). The Importance of Data Security in Business Management: Protection of the Company Against Security Threats. *Journal of Critical Reviews*, *7*(1), 251–256. https://doi.org/10.31838/jcr.07.01.45

Munir, R. (2019). *Kriptografi Edisi 2*. Bandung: Institut Teknologi Bandung.

Noviyanti, P., & Mira. (2022). Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – Study Literature. *Journal of Information Technology*, *2*(1), 23–30. https://doi.org/10.46229/jifotech.v2i1.387

Pratiwi, J. A., & Asmunin, A. (2022). Penggunaan QR code Berbasis Kriptografi

Menggunakan Algoritma Elliptic Curve Criptography. *Journal of Informatics and Computer Science (JINACS)*, *3*(04), 564–570. https://doi.org/10.26740/jinacs.v3n04.p564-570

Putra, W. A., Suyanto, & Zarlis, M. (2023). Performance Analysis Of The Combination Of Advanced Encryption Standard Cryptography Algorithms With Luc For Text Security. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, *8*(2), 890–897. https://doi.org/10.33395/sinkron.v8i2.12202

Putri, W. C. U. (2023). *Implementasi Penggabungan Kriptografi Rivest Shamir Adleman (RDA) yang Ditingkatkan dan Kriptografi Advanced Encryption Standard (AES) pada Aplikasi Pengirim Email*. Universitas Pendidikan Indonesia.

Rahmansyah, R. (2022). Penerapan Algoritma Friefalds Untuk Pembangkit Kunci Algoritma Knapsack Pada Pengamanan Record Database. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *2*(4), 132–137. https://doi.org/10.30865/klik.v2i4.317

Rothke, B. (2011). Advanced Encryption Standard (AES). *Encyclopedia of Information Assurance*. https://api.semanticscholar.org/CorpusID:63840360

Schneier, B. (1996). *Applied Cryptography* (2nd ed.). John Wiley And Sons.

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

Sibarani, E. B. H., Zarlis, M., & Sembiring, R. W. (2017). Analisis Kripto Sistem Algoritma AES Dan Elliptic Curve Cryptography (ECC) Untuk Keamanan Data. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *1*(2), 106–112. https://doi.org/10.30743/infotekjar.v1i2.71

Soleh, M. (2011). *Analisis dan implementasi watermarking dengan algoritma aes untuk pemberian data hak cipta pada file audio* [Skripsi Sarjana. Universitas Islam Negeri Syarif Hidayatullah Jakarta]. https://api.semanticscholar.org/CorpusID:59673018

Stinson, D. R. (2006). *Cryptography: theory and practice* (3rd ed.). Chapman and Hall/CRC.

Stinson, D. R., & Paterson, M. B. (2018). *Cryptography, Theory and Practice*. London: Chapman and Hall.

Suartana, I. M., Eka Putra, R., Bisma, R., & Prapanca, A. (2022). Pengenalan Pentingnya Cyber Security Awareness pada UMKM. *Jurnal Abadimas Adi Buana*, *5*(02), 197–204. https://doi.org/10.36456/abadimas.v5.i02.a4560

Supardi, Y., & Dede. (2020). *Semua Bisa Menjadi Programmer Python Case Study*. Jakarta: Elex Media Komputindo.

Surian, D. (2006). Algoritma Kriptografi Aes Rijndael. *Tesla*, *8*(2), 97–101.

Sutoyo, T., & Rini, W. B. (2009). *Teori Pengolahan Citra Digital*. Yogyakarta: Penerbit Andi.

Yonathan, F. D., Nasution, H., & Priyanto, H. (2021). Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan Algoritma Kompresi Huffman. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *7*(2), 181. https://doi.org/10.26418/jp.v7i2.47077

Yuniati, V., Gani, I., & Rachmat, A. (2009). Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File. *Jurnal Niformatika*, *5*(1), 22–31.