IMPLEMENTASI PENGGABUNGAN KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) YANG DITINGKATKAN DAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) PADA APLIKASI PENGIRIM *EMAIL*

SKRIPSI

Diajukan untuk memenuhi sebagian dari syarat untuk memperoleh gelar
Sarjana Matematika

Oleh:
Widya Catur Utami Putri
1905700

PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2023

LEMBAR HAK CIPTA

IMPLEMENTASI PENGGABUNGAN KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) YANG DITINGKATKAN DAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) PADA APLIKASI PENGIRIM *EMAIL*

Oleh:

Widya Catur Utami Putri

NIM 1905700

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Agustus 2023

LEMBAR PENGESAHAN

WIDYA CATUR UTAMI PUTRI

IMPLEMENTASI PENGGABUNGAN KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) YANG DITINGKATKAN DAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) PADA APLIKASI PENGIRIM *EMAIL*

Disetujui dan disahkan oleh pembimbing :

Pembimbing I

Dra. Rini Marwati, M.S.

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

ABSTRAK

Email merupakan salah satu sarana komunikasi yang umum digunakan. Pesan yang dikirim melalui *email* dapat berisi informasi rahasia. Telah tercatat sejumlah serangan *cyber* menargetkan *email*, dalam penggunaannya pun terkadang pengguna kurang bijak dan berhati-hati. Oleh karena itu, diperlukan tindakan pengamanan untuk pesan rahasia yang dikirimkan melalui *email*. Kriptografi adalah salah satu tindakan pengamanan yang dapat dilakukan untuk mengirim pesan rahasia melalui *email*. Terdapat dua jenis kriptografi berdasarkan jumlah kuncinya yaitu kriptografi simetris dan asimetris. Kriptografi simetris menggunakan kunci yang sama dalam proses enkripsi dan dekripsinya, sedangkan kriptografi asimetris menggunakan kunci yang berbeda dalam proses enkripsi dan dekripsi. Dalam penerapannya terdapat kekurangan dalam beberapa algoritma kriptografi. Permasalahan transmisi kunci rahasia adalah salah satu masalah yang ada pada kriptografi simetris. Kriptografi *hybrid* dapat menjadi salah satu solusi untuk mengatasinya, kunci simetris dapat dienkripsi oleh kunci asimetris agar transmisi kunci rahasia lebih aman. Kriptografi simetris dan asimetris yang dipilih adalah AES (*Advanced Encryption Standard*) dan RSA (Rivest Shamir Adleman) yang ditingkatkan. Kriptografi RSA terkenal akan keamanannya yang kuat didasarkan pada sulitnya operasi eksponensial dan faktorisasi, sedangkan kriptografi AES merupakan standar kriptografi aman yang memiliki waktu komputasi relatif cepat. Aplikasi pengirim *email* untuk mengirimkan pesan rahasia menggunakan algoritma kriptografi penggabungan akan dikontruksi menggunakan bahasa pemrograman *python*.

Kata Kunci: Kriptografi, Algoritma RSA, RSA yang ditingkatkan, *Advanced Encryption Standard*, *Email*

ABSTRACT

Email is one of the most commonly used tools of communication. Messages sent via email can contain confidential information. There have been a number of cyber attacks targeting email, and sometimes users are not wise and careful in their use. Therefore, security measures are needed for confidential messages sent via email. Cryptography is one of the security measures that can be taken to send confidential messages via email. There are two types of cryptography based on the number of keys, namely symmetric and asymmetric cryptography. Symmetric cryptography uses the same key in the encryption and decryption process, while asymmetric cryptography uses different keys in the encryption and decryption process. In its application, there are shortcomings in some cryptographic algorithms. The problem of secret key transmission is one of the problems in symmetric cryptography. Hybrid cryptography can be one of the solutions to overcome this, symmetric keys can be encrypted by asymmetric keys to make the transmission of secret keys more secure. The symmetric and asymmetric cryptography chosen are AES (Advanced Encryption Standard) and enhanced RSA (Rivest Shamir Adleman). RSA cryptography is known for its strong security based on the difficulty of exponential and factorization operations, while AES cryptography is a secure cryptography standard that has a relatively fast computation time. An email application to send secret messages using merged cryptography algorithm will be constructed using python programming language.

***Keywords**: Cryptography, RSA Algorithm, Enhanced RSA, Advanced Encryption Standard, Email*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Anonim. (2015). ASCII Table. [Online]. Diakses dari: http://www.gcsecs.com/ascii1.html.

Anwar, N., Munawwar, 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. doi: https://doi.org/10.29207/resti.v2i3.606

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

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

Bash, Ajax. (2022, 23 Agustus). "New Iranian APT Data Extraction Tool" [Forum daring]. Diakses dari https://blog.google/threat-analysis-group/new-iranian-apt-data-extraction-tool/.

Basri. (2016). Kriptografi Simetris dan Asimetris Dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer, 2*(2), 16-23.

Bimantoro, Y., & Sari, R. T. (2021). Enkripsi Data Menggunakan RSA & AES Pada Aplikasi Instant Messaging Berbasis Mobile. *Jurnal Teknik Informatika, 14*(2), 135-144. doi: https://doi.org/10.15408/jti.v14i2.23469

Buchmann, J. A. (2004). *Introduction to Cryptography.* New York: Springer.

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

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

Easttom, W. (2021). *Modern Cryptography.* Washington, DC: Springer Cham. doi: https://doi.org/10.1007/978-3-030-63115-4

Enriquez, M., Garcia, D. W., & Arboleda, E. (2017). Enhanced Hybrid Algorithm of Secure and Fast Chaos-based, AES, RSA and ElGamal Cryptosystems. *Indian Journal of Science and Technologi, 10*(27), 1-14. doi: http://dx.doi.org/10.17485/ijst/2017/v10i27/105001.

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), 41-49. doi: https://doi.org/10.52166/ujmc.v2i1.448

Ferdinan, M. A. (2021). Aplikasi Pengiriman *Email* Menggunakan Enkripsi Elliptic Curve Diffie Hellman. (Skripsi). Bandung: Universitas Pendidikan Indonesia.

Firdaus, J., Marwati, R., & Gozali, S. M. (2018). Penyandian Pesan Menggunakan Kombinasi Algoritma RSA yang Ditingkatkan dan Algoritma ElGamal. *Jurnal EurekaMatika, 6*(1), 23-32. doi: https://doi.org/10.17509/jem.v6i1.11653

Fitzpatrick, M. (2020). *Create GUI Applications with Python & Qt5 (PyQt5 Edition).* New York.

Galbraith, S. D. (2012). *Mathematics of Public Key Cryptography.* Cambridge: Cambridge University Press.

Hermawan, A., & Ujianto, E. I. (2021). Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 5*(2). doi: https://doi.org/10.30743/infotekjar.v5i2.3585

Hutahaean, J. (2014). *Konsep Sistem Informasi.* Yogyakarta: Deepublish.

Hutasuhut, D. I., Aldizar, M. R., & Nasution, I. F. (2023). Perbandingan Algoritma Kriptografi Simetris dan Asimetris. *UNES Journal of Information System, 8*(1), 042-047.

Ireland, K., & Rosen, M. (1990). *A Classical Introduction to Modern Number Theory.* New York: Springer.

Irmayanti, H. (2019). *Operasi Aritmatika Bilangan Biner, Octal, dan Heksadesimal*. [*Online*]. Diakses dari http://repository.unikom.ac.id/id/eprint/61599.

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

Mufadilah, A. T. (2019). Implementasi Kriptografi Rivest Shamir Adleman (RSA) yang Ditingkatkan dan Steganografi Least Significant Bit (LSB). (Skripsi). Bandung: Universitas Pendidikan Indonesia.

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

Munir, R. (2016). *Algoritma dan Pemrograman dalam Bahasa Pascal, C, dan C++*. Bandung: Penerbit Informatika.

Munir, R. (2019). *Kriptografi: Edisi Kedua*. Bandung: Penerbit Informatika.

Kuppuswamy, P., & Khalidi, S.Q.Y.A. (2014). Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm. *International Journal of Information and Computer Security, 6*(4), 372-382. doi: http://dx.doi.org/10.1504/IJICS.2014.068103

Rosen, K. H. (1984). *Elementary Number Theory and Its Applications.* Boston: Addison-Wesley.

Schneier, B. (1996). *Applied Cryptography, Second Edition*. New York: John Wliey & Sons Inc.

Soliman, M. I. (2010). FastCrypto: Parallel AES Pipelines Extension for General-Purpose Processors. *Neural, Parallel, and Scientific Computations*, 18, 47-58. doi: http://dx.doi.org/10.1115/1.802977.paper114

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

Suhardi. (2016). Aplikasi Kriptografi Data Sederhana dengan Metode Exclusive-OR (XOR). *Jurnal Teknovasi, 03*(2), 23-31.

Surian, D. (2006). Algoritma Kriptografi AES Rijndael. *Tesla: Jurnal Teknik Elektro, 8*(2), 97-101.

Ulfah, N. (2020). Penyandian Pesan Teks dengan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Least Significant Bit (LSB). (Skripsi). Bandung: Universitas Pendidikan Indonesia.

Yuniati, V., Indriyanta, G., & Rachmat, A. (2009). Enkripsi dan Dekripsi dengan Algoritma AES 256. *Jurnal Informatika, 5*(1), 22-31.