

**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

© Widya Catur Utami Putri 2023

Universitas Pendidikan Indonesia

Agustus 2023

Hak cipta dilindungi undang-undang

Skripsi tidak boleh diperbanyak seluruhnya atau sebagian dengan dicetak ulang,
difotokopi, atau cara lainnya tanpa izin penulis

Widya Catur Utami Putri, 2023

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

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

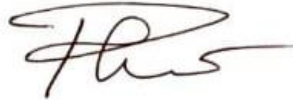
LEMBAR PENGESAHAN

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 dikonstruksi 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

LEMBAR PENGESAHAN	i
SURAT PERNYATAAN	ii
KATA PENGANTAR.....	iii
UCAPAN TERIMAKASIH	iv
ABSTRAK	v
<i>ABSTRACT</i>	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian	4
1.4 Batasan Penelitian.....	4
1.5 Manfaat Penelitian	4
BAB II LANDASAN TEORI	5
2.1 Teori Dasar Matematika.....	5
2.1.1 Relatif Prima	5
2.1.2 Algoritma Euclid.....	5
2.1.3 Fungsi Euler.....	6
2.1.4 Kekongruenan.....	6
2.2 Sistem ASCII	6
2.3 Operasi Biner XOR.....	8
2.4 Operasi Perkalian Heksadesimal	8
2.5 Kriptografi	9
2.5.1 Tujuan Kriptografi	9
2.5.2 Kriptosistem.....	10
2.5.3 Kriptografi Simetris	11
2.5.4 Kriptografi Asimetris	12
2.5.5 Kriptografi Modern.....	12
2.5.6 Kriptografi Hibrida	13

2.6	Algoritma Kriptografi RSA	13
2.7	Algoritma Kriptografi AES.....	16
2.7.1.	<i>Key Schedule</i>	18
2.7.2	<i>AddRoundKey</i>	19
2.7.3	<i>SubBytes</i>	19
2.7.4	<i>ShiftRows</i>	20
2.7.5	<i>MixColumns</i>	20
2.7.6	<i>InvShiftRows</i>	21
2.7.7	<i>InvSubBytes</i>	22
2.7.8	<i>InvMixColumns</i>	22
2.8	Program <i>Python</i>	23
BAB III METODE PENELITIAN.....		24
3.1	Identifikasi Masalah.....	24
3.2	Model Dasar.....	24
3.3	Pengembangan Model Dasar	26
3.4	Konstruksi Program Aplikasi.....	27
3.4.1	Input Output.....	28
3.4.2	Algoritma Deskriptif.....	29
3.4.3	Rancangan Tampilan Program	30
3.5	Penggunaan Program <i>Python</i>	32
3.6	Proses Validasi	33
3.7	Penarikan Kesimpulan	33
BAB IV HASIL DAN PEMBAHASAN.....		34
4.1	Skema Penggabungan Kriptografi RSA yang Ditingkatkan dan AES pada Aplikasi Pengiriman <i>Email</i>	34
4.2	Algoritma Program Penggabungan Kriptografi RSA yang Ditingkatkan dan AES pada Aplikasi Pengiriman <i>Email</i>	34
4.2.1	Algoritma Pembangkitan Kunci	35
4.2.2	Algoritma Enkripsi	36
4.2.3	Algoritma Dekripsi	37
4.2.4	Algoritma Aplikasi Pengirim <i>Email</i>	39
4.3	Program Penggabungan Kriptografi RSA yang Ditingkatkan dan AES pada Aplikasi Pengiriman <i>Email</i>	39

4.3.1	Tampilan Program Penggabungan Kriptografi RSA yang Ditingkatkan dan AES pada Aplikasi Pengiriman <i>Email</i>	39
4.4	Validasi Program Penggabungan Kriptografi RSA yang Ditingkatkan dan AES pada Aplikasi Pengiriman <i>Email</i>	44
4.4.1	Validasi Pembangkitan Kunci	44
4.4.2	Validasi Enkripsi Pesan.....	45
4.4.3	Validasi Dekripsi Pesan	50
BAB V KESIMPULAN DAN SARAN.....		55
5.1	Kesimpulan	55
5.2	Saran	55
DAFTAR PUSTAKA		57
LAMPIRAN		60

DAFTAR GAMBAR

Gambar 2.1 Skema Kriptosistem	11
Gambar 2.2 Proses Enkripsi dan Dekripsi pada AES	17
Gambar 2.3 Proses <i>AddRoundKey</i>	19
Gambar 2.4 Proses <i>SubBytes</i>	19
Gambar 2.5 Proses <i>ShiftRows</i>	20
Gambar 2.6 Proses <i>MixColumns</i>	21
Gambar 2.7 Proses <i>InvShiftRows</i>	21
Gambar 2.8 Proses <i>InvSubBytes</i>	22
Gambar 2.9 Operasi <i>InvMixColumns</i>	23
Gambar 3.1 Skema Algoritma Kriptografi RSA	25
Gambar 3.2 Skema Algoritma Kriptografi AES	26
Gambar 3.3 Skema Penggabungan Algoritma RSA yang Ditingkatkan dan AES	27
Gambar 3.4 Rancangan Tampilan Menu Utama	30
Gambar 3.5 Rancangan Tampilan Pembangkitan Kunci	30
Gambar 3.6 Rancangan Tampilan Enkripsi Pesan	31
Gambar 3.7 Rancangan Tampilan Dekripsi Pesan	31
Gambar 3.8 Rancangan Tampilan Pengiriman <i>Email</i>	32
Gambar 4.1 Skema Penggabungan Kriptografi RSA yang Ditingkatkan dan AES pada Aplikasi Pengiriman <i>Email</i>	34
Gambar 4.2 Tampilan Menu Utama	39
Gambar 4.3 Tampilan Tab Petunjuk Penggunaan Program	40
Gambar 4.4 Tampilan Tab Pembangkitan Kunci	40
Gambar 4.5 Tampilan Tab Enkripsi Pesan	41
Gambar 4.6 Tampilan Tab Dekripsi Pesan	42
Gambar 4.7 Tampilan Tab Pengiriman <i>Email</i>	42
Gambar 4.8 Cara Mendapatkan <i>App Password</i>	43
Gambar 4.9 Contoh <i>Email</i> yang Terkirim.....	44
Gambar 4.10 Proses Ekspansi Kunci Kolom Pertama	45
Gambar 4.11 Proses Ekspansi Kunci Kolom 2-4.....	46
Gambar 4.12 Proses XOR Plainteks dengan Kunci	47
Gambar 4.13 Proses <i>SubBytes</i> , <i>ShiftRow</i> , <i>MixColumns</i> , dan <i>AddRoundKey</i>	47
Gambar 4.14 Proses Ekspansi Kunci Kolom Pertama pada Dekripsi.....	51
Gambar 4.15 Ekspansi Kunci Kolom 2-4 pada Dekripsi.....	51
Gambar 4.16 Proses <i>AddRoundKey</i> , <i>ShiftRows</i> , dan <i>SubBytes</i> pada Dekripsi.....	52
Gambar 4.17 Proses Dekripsi pada Putaran 2-10.....	53

DAFTAR TABEL

Tabel 2.1 Operasi Biner XOR	8
Tabel 2.2 Kode ASCII	7
Tabel 2.3 Properti Algoritma AES	13
Tabel 2.4 Parameter AES	16
Tabel 2.5 Nilai <i>Rcon</i>	18
Tabel 2.6 <i>S-Box</i>	20
Tabel 2.7 <i>Inverse S-Box</i>	22
Tabel 3.1 Rancangan Input dan Output pada Program	28
Tabel 4.1 Perubahan Plainteks dan Kunci Menjadi Heksadesimal	45
Tabel 4.2 10 Kunci Hasil Ekspansi	46
Tabel 4.3 Hasil Proses Enkripsi AES	48
Tabel 4.4 Hasil Ekspansi Kunci pada Dekripsi	52
Tabel 4.5 Hasil Proses Dekripsi AES.....	53

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 Wiley & 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 Technology*, 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.

Widya Catur Utami Putri, 2023

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

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

- Schneier, B. (1996). *Applied Cryptography, Second Edition*. New York: John Wiley & 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.