SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK III - Surabaya, 11 Maret 2023
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2023.4093

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Implementasi Kriptografi dengan Algoritma RSA pada Aplikasi Transfer File

Wahyu Widodo, Rachmad Ardiyanto, Rinci Kembang Hapsari

Jurusan Teknik Informatika, Fakultas Teknik Elektro dan Teknologi Informasi,
Institut Teknologi Adhi Tama Surabaya
e-mail: rincikembang@itats.ac.id

ABSTRACT

Currently, the security of information on data has become an important role in the world of technology, especially in exchanging information. One of them is file transfer. Transferring files here requires an internet connection, which will likely spread the news to irresponsible parties. Therefore, cryptography is used to secure information using the RSA algorithm. From the implementation of cryptography with the RS algorithm, there are three processes: key generation, encryption, and decryption. The results of this study from the RSA algorithm computation time for encryption for testing files with different numbers of characters have an average of 825 ms. In comparison, decryption is 781.2 ms with Throughput, which averages 221,470 Kbps.

Keywords: *Cryptography, Steganography, RSA, File Transfer.*

ABSTRAK

Saat ini, keamanan informasi pada data menjadi peranan penting dalam dunia teknologi khususnya kegiatan saling bertukar informasi. Salah satu diantaranya yaitu transfer file. Transfer file disini membutuhkan koneksi internet yang berkemungkinan besar informasi tersebut akan tersebar kepada pihak yang tidak bertanggung jawab. Maka dari itu digunakan kriptografi untuk mengamankan suatu informasi yang menggunakan algoritma RSA. Dari implementasi kriptografi dengan algoritma RSA, terdapat 3 proses yaitu pembangkitan kunci, proses enkripsi, dan proses dekripsi. Hasil penelitian ini dari algoritma RSA waktu

komputasi enkripsi untuk pengujian file dengan jumlah karakter yang berbeda memiliki rata-rata sebesar 825 ms sedangkan dekripsi sebesar 781.2 ms dengan Throughput yang memiliki rata-rata 221.470 Kbps.

Kata kunci: Kriptografi, Steganografi, RSA, File Transfer.

PENDAHULUAN

Dalam perkembangan dewasa ini, keamanan informasi terkait data menjadi penting dalam dunia teknologi. Khususnya dalam kegiatan saling bertukar informasi antar dua user atau lebih. Dibutuhkannya keamanan informasi guna mewaspadai adanya pihak ketiga yang tidak bertanggung jawab yang bisa saja mengambil dan memanipulasi informasi yang akan dikirim antar user tersebut. Untuk itu, kriptografi sangat diperlukan pada keamanan informasi data dalam pengiriman informasi tersebut [1]. Sebagai ilmu yang sudah diterapkan dalam pengamanan informasi, kriptografi dapat digunakan untuk mengamankan informasi penting yang terkandung dalam file. Dimana informasi asli (plaintext) tersebut akan diubah ke dalam bentuk informasi acak(ciphertext)yang disebut dengan proses enkripsi. Sedangkan proses pengembalian informasi acak (ciphertext) ke dalam bentuk informasi asli (plaintext) disebut dengan proses dekripsi [2].

Aplikasi Transfer File merupakan aplikasi dalam jaringan yang mengizinkan penggunanya untuk dapat mengkopi file dari satu komputer ke komputer yang lain. Aplikasi Transfer File juga membutuhkan koneksi internet [3]. Dengan pertukaran file berisi informasi penting yang melalui koneksi internet ini dapat menyebabkan rentannya informasi tersebut akan tersebar yang kemungkinan besar isi file tersebut akan bocor ditangan pihak yang tidak bertanggung jawab. Hal ini menjadi kekurangan dalam aplikasi Transfer File, karena informasi yang terkandung dalam file tersebut tidak dienkripsi terlebih dahulu sehingga pihak ketiga dapat dengan mudah membaca informasi tersebut. Maka dari itu digunakannya kriptografi guna mengacak informasi yang dikirimkan menjadi bentuk lain yang tidak bermakna.

Pengamanan file dengan kriptografi telah digunakan dalam file pdf, dengan menggunakan algoritma RSA [4], pada penelitian lain algoritma kriptografi RSA dapat digunakan untuk melakukan enkripsi dan dekripsi untuk mengirim maupun menerima email [5]. Metode kriptografi dengan algoritma juga dapat digunakan untuk mengamankan data rekam medic pasien yang berisikan catatan dan dokumen tentang identitas pasien, diagnosa penyakit, pengobatan dan pelayanan lain [6].

Pada penelitian sebelumnya menurut Himawan [7] menyatakan bahwa perbandingan waktu proses enkripsi dan dekripsi pada algoritma RSA adalah 5,8-6,16 kali lebih cepat dibandingkan dengan algoritma ElGamal yang membutuhkan waktu 7,37-7,38 kali lebih cepat dari jumlah pesan. Sehingga algoritma RSA lebih unggul dalam kecepatan waktu proses enkripsi dan dekripsi yang jauh lebih cepat. Sehingga dalam penelitian ini melakukan pengamanan data menggunakan metode RSA.

METODE

Di dalam penelitian ini, dirancang dan dikembangkan sebuah sistem keamanan data dalam bertukar informasi proses pengacakan informasi. Penelitian ini dimulai dari proses input file yang sudah berisi sebuah informasi, yang kemudian isi dari file tersebut akan dienkripsi terlebih dahulu dengan algoritma RSA. Dalam penelitian ini, terdapat 3 proses untuk mengenkripsi informasi dengan menggunakan algoritma RSA yaitu proses pembangkitan kunci, enkripsi file, dekripsi file.

Kriptografi

Kriptografi merupakan ilmu sekaligus seni dalam menjaga keamanan pesan [1]. Selain itu pengertian kriptografi yaitu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan,integritas data, serta otentikasi [8].

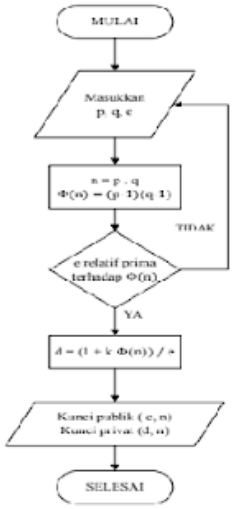
Keamanan data sangatlah penting pada saat ini karena canggihnya teknologi, seseorang bisa saling tukar menukar informasi dengan sangat mudah dan cepat tanpa melalui perantara kantor pos. Dalam menjaga kerahasiaan data, kriptografi merupakan salah satu teknik yang digunakan untuk mengamankan suatu informasi dengan cara mengubah pesan asli tersebut ke dalam bentuk pesan yang tidak memiliki makna. Dengan kata lain, informasi hanya dapat dibaca oleh orang yang berhak terhadap informasi tersebut. Terdapat empat tujuan umum dari sistem kriptografi [9][10]:

1. *Confidentiality,* Maksud dari kerahasiaan ini adalah layanan yang bertujuan untuk menjaga isi dari suatu pesan yang tidak dapat diakses oleh siapapun kecuali orang yang memiliki otoritas terhadap pesan tersebut.
2. *Data Integrity* (Data Integritas), Maksud dari data integritas yaitu layanan yang bertujuan untuk mencegah terjadinya perubahan data dan mengecek data yang sampai di penerima adalah data asli yang telah dikirim oleh pengirim
3. *Authentication* (Keaslian), Maksud dari keaslian ini adalah layanan yang terkait dengan proses identifikasi, dimana data akan dicek apakah mengalami manipulasi dalam isinya seperti penyisipan, penghapusan, dan penggantian data.
4. *Non-Repudiation* (Tidaknya Penyangkalan), Maksud dari *non-repudiation* yaitu jika seseorang sudah mengirimkan pesan, maka orang tersebut tidak dapat membantah atau menyangkal pengiriman pesan tersebut.

Algoritma RSA (*Rivest-Shamir-Adleman)*

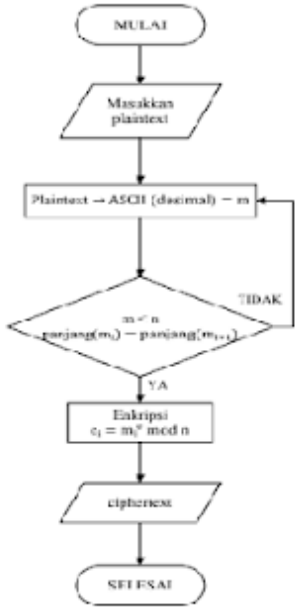
RSA adalah suatu algoritma yang termasuk algoritma kriptografi kunci public atau kriptografi kunci asimetris. Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (*Massachusetts Institute of Technology*) pada tahun 1976, yaitu Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan pada algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci pribadi[7].

Algoritma RSA terdiri dari tiga tahap yaitu tahap pembangkitan kunci, tahap enkripsi dan dekripsi pesan. Tahap pembagkitan kunci ditunjukkan pada Gambar 1.



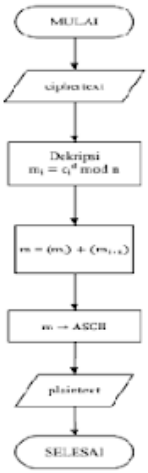
Gambar 1. *Flowchart* Pembangkitan Kunci Algoritma *RSA*

Dimana proses pembangkitan kunci dimana p dan q adalah inputan bilangan prima secara acak dengan syarat $p \neq q$. Kemudian dilakukan proses perhitungan nilai n, yang mana pada RSA bilangan n disebut dengan modulus. Setelah itu masukkan bilangan e dengan syarat $1 < e < \Phi(n)$ dan $PBB(e, \Phi(n)) = 1$, yang mana e nanti akan diuji apakah e relatif prima terhadap $\Phi(n)$ dan akan menjadi kunci publik. Kemudian dilakukan proses perhitungan terhadap d. Setelah proses ini selesai nanti akan dihasilkan kunci publik yang berupa bilangan dari (e, n) dan kunci privatenya berupa (d, n).



Gambar 2. *Flowchart* Enkripsi Algoritma RSA

Gambar 2 adalah *flowchart* enkripsi dari algoritma RSA, dimana pada saat pengirim akan mengirimkan informasi kepada penerima maka harus dilakukan proses enkripsi terlebih dahulu agar informasi tersebut tidak diketahui oleh penyusup. Dimulai dari menulis informasi yang akan dienkripsi, kemudian mengubah informasi tersebut ke dalam bentuk desimal yang sesuai dengan tabel ASCII. Setelah itu membagi *file* informasi tersebut menjadi beberapa blok (m_i), dengan syarat $m_i < n$ dan panjang(m_i) = panjang(m_{i+1}). Setelah itu setiap blok dienkripsi menggunakan pasangan kunci publik, yang nantinya akan menghasilkan *ciphertext*.



Gambar 3. Flowchart Dekripsi Algoritma RSA

Gambar 3 adalah proses terakhir yaitu proses dekripsi informasi. Ciphertext yang telah didapat akan didekripsi untuk mendapatkan plaintext (informasi semula) dengan menggunakan kunci private. Kunci private didapatkan pada tahap pembangkitan pasangan kunci.

HASIL DAN PEMBAHASAN

Dalam mengetahui performa implementasi kriptografi, dalam penelitian ini dilakukan pengujian terhadap waktu komputasi dan throughput. Waktu komputasi untuk proses enkripsi dan dekripsi ditunjukkan pada Tabel 1.

Tabel 1. Waktu komputasi enkripsi dan dekripsi

Jumlah Char	Enkripsi (ms)	Dekripsi (ms)
160	592	499
162	619	609
170	648	612
172	684	613
174	728	646
175	785	734
177	820	771
179	1010	984
181	1028	1018
186	1332	1326
Rata-rata	825	781.2

Pada pengujian *throughput* dilakukan perhitungan dan perbandingan ukuran informasi sebelum dienkripsi. Pengujian sistem menggunakan *throughput*, yaitu menghitung jumlah karakter dalam file yang akan dibagi dengan waktu komputasi dari proses enkripsi. Hasil perhitungan *throughput*, ditunjukkan pada Tabel 2.

Tabel 2. Hasil dari *throughput*

Jumlah Char	Enkripsi (s)	*Throughput* (Kbps)
160	0.592	268.456
162	0.619	261.712

170	0.648	262.345
172	0.684	251.461
174	0.728	239.010
175	0.785	222.929
177	0.820	215.853
179	1.010	177.227
181	1.028	176.639
186	1.332	139.639
Rata-rata	0.825	221.470

KESIMPULAN

Setelah melakukan implementasi algoritma RSA untuk kriptografi file, dihasilkan kesimpulan yaitu:

1. Dari hasil pengujian 10 file berukuran 1 kb dengan jumlah karakter yang berbeda, didapatkan hasil bahwa semakin banyak jumlah karakter dalam file maka akan semakin lama waktu komputasinya. Sehingga dihasilkan rata-rata waktu dekripsi sebesar 781.2 ms lebih singkat dari proses enkripsi yang menghasilkan rata-rata sebesar 825 ms.
2. Sedangkan dari hasil waktu komputasi enkripsi 10 file berukuran 1 kb dengan jumlah karakter yang berbeda, didapatkan Throughput dengan rata-rata 221.470 Kbps. Karena semakin besar waktu komputasi enkripsinya maka akan semakin kecil Throughputnya, begitu pula sebaliknya.

DAFTAR PUSTAKA

[1] A. R. Taqwa and D. Haryo Sulaksono, "IMPLEMENTASI KRIPTOGRAFI DENGAN METODE ELLIPTIC CURVE CRYPTOGRAPHY (ECC) UNTUK APLIKASI CHATTING BERBASIS ANDROID Article History ABSTRAK," *J. Ris. Inov. Bid. Inform. dan Pendidik. Inform.*, vol. 1, no. 1, pp. 42–48, 2020.

[2] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[3] B. P. S. Hutomo, H. K. Wardana, and B. W. Yohanes, "Pendeteksi Error dengan CRC32 dan Cek Integritas dengan SHA256 pada Aplikasi Pengunduh dan Transfer File," *Techné J. Ilm. Elektrotek.*, vol. 17, no. 02, pp. 109–114, 2018, doi: 10.31358/techne.v17i02.178.

[4] J. K. Azhar and S. Yuliany, "Implementasi Algoritma RSA (Rivest , Shamir dan Adleman) untuk Enkripsi dan Dekripsi File.pdf," 2019.

[5] A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 253, 2015, doi: 10.14710/jtsiskom.3.2.2015.253-258.

[6] S. Sutejo, "Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien," *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 4, no. 1, pp. 104–114, 2021, doi: 10.31539/intecoms.v4i1.2437.

[7] C. Himawan, T. Wibowo, B. Sulityo, R. Roestam, Y. Wahyu, and R. B. Wahyu, "Studi Perbandingan Algoritma RSA dan Algoritma El-Gamal," *Semin. Nas. APTIKOM*, vol. 6, no. 1, pp. 28–29, 2016.

[8] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

[9] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[10] W. R. Maya, A. Azanuddin, and E. Elfitriani, "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 1, p. 1, 2022, doi: 10.53513/jis.v21i1.4764.