E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333

IMPLEMENTASI VERIFIKASI TEKS MENGGUNAKANMETODE RIVEST SHAMIR ADLEMAN (RSA)

Harin Noor Octafiani[1], Ai Rosita[2]
Universitas Widyatama, Universitas Widyatama
Universitas Widyatama
Jl. Cikutra No.204A, Sukapada, Cibeunying Kidul, Kota
Bandungharinnoor@gmail.com[1], ai.rosita@widyatama.ac.id[2]

Abstrak

Perkembangan teknologi dan sistem jaringan saat ini mengalami peningkatan secara signifikan, terutama dalam aspek keamanan. Keamanan jaringan setidaknya memiliki dua syarat, yaitu authenticity dan nonrepudiation. Kriptografi dapat dimanfaatkan terkait dengan keamanan informasi berupa kerahasiaan, keutuhan data, nir penyangkalan, serta otentikasi. Untuk menjaga keamanan pesan berupa teks atau kata, biasanya digunakan teknik enkripsi agar kerahasiaan data tersebut terjamin. Salah satu algoritma enkripsi yang sering digunakan yaitu algoritma kriptografi Rivest Shamir Adleman (RSA). Pada penelitian ini, algoritma RSA digunakan sebagaipelindung data, dan menggunakan mekanisme berupa teks sebagai alat verifikasi. Penelitian ini bertujuan untuk membuat interface pengiriman pesan terautentikasi dengan menerapkan algoritma kriptografi Rivest Shamir Adleman (RSA) pada sebuah teks. RSA merupakan algoritma asimetrik yang mempunyai dua kunci yang berbeda, yaitu kuncipublik dan kunci privat. Kedua pasangan kunci (key pair) tersebut digunakan untuk proses enkripsi dan dekripsi. Tingkat keamanan algoritma RSA sangat bergantung pada ukuran kunci tersebut, karena makin kecil ukuran kunci, maka makin besar juga kemungkinan kombinasi kunci yang bisa dijebol dengan metode memeriksa kombinasi satu persatu kunci atau lebih dikenal dengan istilah Brute Force Attack. Bilangan prima yang dihasilkan dalam algoritma RSA mempengaruhi ukuran kunci sandi.

Kata kunci :

Teks, metode Rivest Shamir Adleman (RSA), Autentikasi, Keamanan Data, Jaringan.

Abstract

The development of technology and network systems experience a significant increase, especially in the security aspect. Network security has at least two features, specifically authentication and nonrepudiation. Cryptography can be used for information security in the form of confidentiality, data integrity, non-denial, and authentication. To maintain the security of messages in the form of text or words, encryption techniques are usually employed to guarantee the confidentiality of the data. One of the encryption algorithms that is frequently used is the Rivest Shamir Adleman (RSA) cryptographic algorithm. In this study, the RSA algorithm is used as a data protector and uses a texting mechanism as a verification tool. This study aims to create an authenticated message delivery interface by applying the Rivest Shamir Adleman (RSA) cryptographic algorithm to a text. RSA is an asymmetric algorithm that has two dissimilar keys, explicitly the public key and the private key. The two key pairs are used for the encryption and decryption process. The security level of the RSA algorithm is very dependent on the size of the key, because the smaller the key size, the greater the possibility of key combinations that can be broken by checking the combination of keys one by one or better known as Brute Force Attack. The prime numbers generated in the RSA algorithm affect the size of the cipher key.

Keywords :

Text, Rivest Shamir Adleman (RSA) method, Authentication, Data Security, Network

I. PENDAHULUAN

Kemajuan perkembangan teknologi telah berpengaruh pada seluruh kehidupan manusia. Salah satunya dalam hal berkomunikasi. Dengan adanya internet komunikasi dapat dilakukan tanpa adanya batasan jarak. Sehingga informasi – informasi yang dikirimkan sangatlah penting. Sangat pentingnya sebuah informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang – orang tertentu saja. Untuk itu keamanan dari sistem informasi yang digunakan haruslah terjamin. Permasalahan akan informasi tersebut dipertanyakan dan dapat dijawab salah satunya dengan proses kriptografi.

Kriptografi dapat dimanfaatkan terkait dengan keamanan informasi berupa kerahasiaan, keutuhan data, nir penyangkalan, serta otentikasi. Pengamanan menggunakan kriptografi memerlukan banyak pertimbangan dan strategi. Perlindungan terhadap kerahasiaan informasi dengan menggunakan kriptografi sekarang ini semakin meningkat, salah satu caranya dengan penyandian atau enkripsi. Ada beberapa algoritma enkripsi yang dapat digunakan, salah satu algoritma yang sering digunakan yaitu algoritma kriptografi Rivest Shamir Adleman (RSA).

Mekanisme kerja RSA cukup sederhana dan mudah dimengerti, tetapi kokoh. Sampai saat ini satu - satunya cara untuk mendobraknya adalah dengan cara mencoba satu persatu kombinasi kunci yang mungkin atau yang biasa 2 disebut brute force attack. Sehingga penentuan tingkat keamanan suatu sandi dari kemungkinan dibongkar adalah seberapa panjang dari sandi (ukuran kunci) tersebut. Karena jika semakin panjang suatu kode, maka semakin banyak pula kombinasi kunci yang mungkin ada.

Algoritma ini tidak berdasarkan pada proses enkripsi dan dekripsi, melainkan lebih kepada proses matematika yang dilakukan untuk menghasilkan kunci rahasia yang dapat disebarkan secara bebas tanpa harus khawatir karena kunci rahasia tersebut hanya dapat didekripsi hanya oleh pengirim dan penerima pesan. Dasar dari algoritma ini memfaktorkan bilangan yang besar menjadi faktor - faktor prima.

Pada penelitian sebelumnya yang membahas tentang perangkat lunak yang dapat melakukan proses enkripsi dan dekripsi pesan sehingga dapat mengamankan data “chat” antar pengguna. Program ditulis menggunakan bahasa pemrograman PHP. Bertujuan untuk kirim pesan di jaringan lokal yang rentan terhadap serangan Man In The Middle seperti sniffing (Dermawan et al., 2014).

Pada penelitian yang lain mengenai bagaimana pengamanan dokumen khususnya untuk dokumen teks. Dalam penelitian ini, metode yang digunakan adalah metode RSA, sistem dibangun dengan perangkat lunak Borland Delphi 7 (Supriyono, 2008). Penelitian selanjutnya membahas menggabungkan metode RSA yang dihasilkan secara acak oleh modul pada IDE Android Studio bahasa pemprograman Java, sedangkan untuk perekaman kunci biometriknya menggunakan aplikasi yang dikembangkan menggunakan library OpenCV dengan cara pembelajaran atau pengenalan node objek yang akan direkam (PERMANA, 2019).

Penelitian lainnya yang membahas bagaimana kriptografi menjaga kerahasiaan informasi yang terkandung dalam pesan sehingga informasi tersebut tidak dapat diketahui oleh pihak yan tidak sah (Maharani & Agus, 2009). Serta pada penelitian yang membahas tentang menggunakan metode RSA dan LSB sebagai cara untuk menjaga keamanan pesan menggunakan teknik steganografi. Algoritma kriptografi yang digunakan adalah algoritma RSA (Arifin & Oktoviana, 2013).

II. KAJIAN LITERATUR

II.1 Teks

Istilah teks sebenarnya berasal dari kata text yang berarti ‘tenunan’. Teks dalam filologi diartikan sebagai ‘tenunan kata-kata’, yakni serangkaian kata-kata yang berinteraksi membentuk satu kesatuan makna yang utuh (Herti Gustina, Meri Asparina, 2013). Dari pengertian diatas diartikan bahwa teks adalah suatu kesatuan bahasa yang memiliki isi dan bentuk, baik lisan maupun tulisan yang disampaikan oleh pengirim kepada penerima untuk menyampaikan pesan tertentu.

II.2 Rivest Shamir Adleman (RSA)

Algoritma RSA merupakan penerapan dari kriptografi asimetri, yaitu jenis kriptografi yang menggunakan dua kunci yang berbeda: kunci publik (public key) dan kunci pribadi (private key). Adapun tingkat kerahasian dari besaran besaran pada algoritma RSA diantaranya adalah besaranbesaran yang digunakan pada algoritma RSA menurut (Dony.2008):

1. p dan q bilangan prima (rahasia)
2. N = p . q (tidak rahasia)

3. Φ(n) = (p – 1)(q – 1) (rahasia)
4. e = (kunci enkripsi) (tidak rahasia)
5. d = (kunci dekripsi) (rahasia)
6. X (plainteks) (rahasia)
7. Y (cipherteks) (tidak rahasia)

II.3 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Yusfrizal, 2019). Disimpulkan bahwa kriptografi yaitu suatu ilmu atau seni merahasiakan sebuah informasi penting dengan fungsi dan algoritma – algoritma matematika sehingga informasi yang dikirimkan tidak diketahui oleh orang yang tidak berhak.

II.4 *Enskripsi*

Enkripsi berasal dari bahasa Yunani "kryptos" yang berarti tersembunyi atau rahasia. Enkripsi adalah sebuah proses penyandian yang mengubah teks-asli atau pesan yang dapat dimengerti (*plaintext*) menjadi teks-kode atau pesan yang tidak bisa dimengerti (*ciphertext*) (Munir, 2006).

Berikut ini adalah proses enkripsi RSA. Dilakukan oleh pihak pengirim, dalam hal ini adalah seluruh perhitungan pemangkatan bilangan modulo dilakukan menggunakan metode fast exponentiation.

(1) Ambil kunci publik (n,b).
(2) Pilih plaintext m, dengan $0 \leq m \leq n-1$.
(3) Hitung c = me mod n.
(4) Diperoleh ciphertext c, dan kirimkan kepadaB.

II. 5 *Deskripsi*

Dekripsi adalah sebuah proses pembalikan yang mengubah teks-kode atau pesan yang tidak bisa dimengerti (*ciphertext*) menjadi sebuah teks-asli atau pesan yang dapat dimengerti (*plaintext*) (Munir, 2006).

Berikut ini adalah proses deskripsi RSA. Dilakukan oleh pihak pengirim, penerima ciphertext, yaitu B.

(1) Ambil kunci publik (n,b) dan kunci rahasia a.
(2) Hitung m = c d mod n.

III. ANALISIS DAN PERANCANGAN

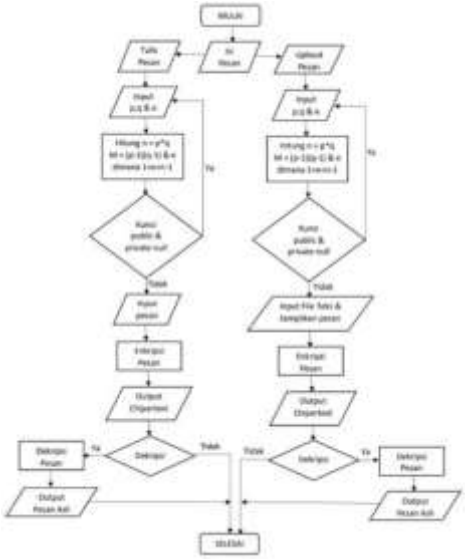
III.1 Analisis Masalah

Verifikasi teks dilakukan untuk mendeteksi apakah isi pesan yang diterima merupakan pesan yang dikirimkan oleh pengirim tanpa ada modifikasi secara illegal oleh pihak yang tidak bertanggung jawab. Maka dalam penulisan ini, penulis akan mengimplementasikan verifikasi teks menggunakan metode Rivest Shamir Adleman (RSA). Dengan demikian implementasi ini dapat digunakan untuk memenuhi setidaknya dua syarat keamanan jaringan, yaitu *Authenticity* dan *Nonrepudiation*.

III.2 Analisis Sistem

Cara kerja sistem ini memiliki tahapantahapan yang dilakukan saat sistem mengubah teks menjadi enkripsi dan dekripsi adalah sebagai berikut :

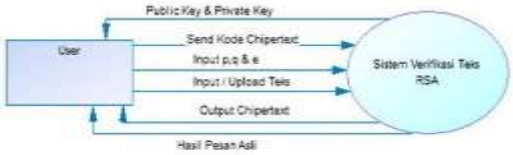
1. Mendeteksi pesan yang dimasukkan.
2. Melakukan serangkaian proses algoritma menggunakan metode Rivest Shamir Adleman (RSA).
3. Hasil keluaran dari sistem yaitu berupa enkripsi dari pesan yang dimasukkan.
4. Melakukan pengujian teks enkripsi yang sesuai dengan pesan yang dikirimkan.



Gambar 1. Flowchart Alur Kerja Sistem

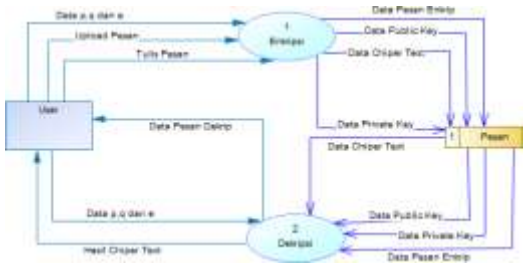
III.3 Perancangan Sistem

Berikut merupakan Konteks Diagram dan Data Flow Diagram (DFD) yang digunakan dalam penelitian ini.



Gambar 2. Flowchart Alur Kerja Sistem

Berdasarkan gambar 2 diatas yang memperlihatkan keseluruhan sistem secara umum melalui diagram konteks.



Gambar 3. DFD Level 1

Gambar 3 merupakan hasil turunan dari diagram konteks. DFD level 1 akan menjelaskan tentang aliran data deteksi objek yang melewati berbagai proses. Proses enkripsi yang menghasilkan pesan tersembunyi berupa kode yang tidak dapat dimengerti oleh orang awam karena tidak dapat membaca kode tersebut. Selanjutnya proses dekripsi yang menghasilkan pesan asli sehinga penerima dapat membaca pesan yang telah dikirim pengirim. Sistem melakukan enkripsi dan dekripsi dengan menggunakan metode Rivest Shamir Adleman (RSA).

IV. IMPLEMENTASI DAN PENGUJIAN

IV.I Implementasi

Dalam implementasinya, aplikasi sistem verifikasi teks menggunakan metode Rivest Shamir Adleman (RSA) ini membutuhkan sarana-sarana pendukung berupa perangkat keras (*hardware*) dan perangkat lunak (*software*).

Gambar 4. Tampilan Halaman Utama

Gambar 5. Tampilan Halaman Upload File

Pada gambar 4 dan 5 merupakan tampilan implementasi perancangan sistem yang akan dibuat. Implementasi sistem ini menggunakan Netbeans dengan Bahasa pemrograman Java. Berikut hasil aplikasi yang telah dibuat.

Gambar 6. Halaman Utama

E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333

Gambar 7. Halaman Upload File

IV. II Pengujian

Bagian ini akan menjelaskan pengujian sistem yang dilakukan dengan metode black box atau yang biasa juga disebut pengujian fungsional. Hasil dari pengujian menunjukan bahwa kelebihan menggunakan metode Rivest Shamir Adleman (RSA) yaitu pada kekuatan algoritma RSA dimana tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor primanya. Namun, terdapat kekurangan dimana karena ukuran kunci privat tersebut besar mengakibatkan proses dalam sistem menjadi lambat terutama pada pesan yang besar. Semakin banyak kata dalam isi pesan, maka proses enkripsi dan dekripsi juga semakin besar melakukan perhitungannya.

Tabel 1. Pengujian Black Box

No	Skenario Pengujian	Keluaran yang Diharapkan	Hasil Uji
1.	Mengisi p,q dan e pada sistem	Sistem menerima p,q dan e	Berhasil
			
2.	Klik tombol *generate keys*	Sistem akan menghasilkan kunci publik (*public key*) dan kunci private (*private key*)	Berhasil
			
3.	Klik tombol *generate keys*	Sistem akan menghasilkan kunci publik (*public key*) dan kunci private (*private key*)	Berhasil
			
4.	Masukkan bahasa untuk mengirim pesan misal a – z	Sistem akan menampilkan pemberitahuan untuk diisi bahasa	Berhasil
			
5.	Masukkan pesan berupa teks/kata Misal "aku"	Sistem akan menampilkan pesan	Berhasil
			
6.	Klik tombol *Encryption*	Sistem akan menampilkan *chipher text*	Berhasil
			
7.	Klik tombol *Send To Receiver* untuk mengirim *cipher text*	Sistem akan menampilkan *chipher text* untuk di *decrypt*	Berhasil
			
8.	Klik tombol *Decryption*	Sistem akan menampilkan	Berhasil

		pesan asli atau yang telah di dekripsi 	
9.	Klik tombol *Clear*	Sistem akan kembali pada tampilan awal 	Berhasil
10.	Klik tombol ke Upload File	Sistem akan berpindah ke form upload file 	Berhasil

V. KESIMPULAN DAN SARAN

V.1 Kesimpulan

Berdasarkan hasil yang didapat dalam menyusun tugas akhir ini, maka dapat ditarik kesimpulan sebagai berikut :

1. Sistem yang dibuat menjelaskan cara kerja dari verifikasi teks dengan metode Rivest Shamir Adleman (RSA).
2. Sistem yang dikembangkan menggunakan metode kriptografi Rivest Shamir Adleman (RSA).
3. Sistem akan menampilkan hasil pesan yang telah diverifikasi menjadi pesan tersembunyi / enkripsi dan pesan asli / dekripsi agar dapat dibaca kembali.

V.2 Saran

Adapun dibawah ini merupakan saran penulis yang dapat digunakan untuk pengembangan sistem kedepannya agar lebih baik lagi, sebagai berikut :

1. Disarankan untuk menambah atau membandingkan antara metode Rivest Shamir Adleman (RSA) dengan metode lain dalam pembuatan sistem.
2. Disarankan untuk mengembangkan sistem dengan metode selain RSA agar dapat mengirim pesan dengan jumlah isi pesan yang banyak.
3. Disarankan untuk memberikan pilihan bilangan yang dimasukkan agar perhitungan sesuai.

REFERENSI

Arifin, R., & Oktoviana, L. T. (2013). Implementasi Kriptografi dan Steganografi menggunakan Algoritma RSA dan metode LSB. *Universitas Malang*

Dermawan, D. C., Cahyanto, T. A., Informatika, J. T., Teknik, F., Jember, U. M., & Network, L. A. (2014). *Aplikasi Kirim Pesan Berbasis Jaringan Lokal Dengan Menerapkan Algoritma RSA Sebagai Teknik Dalam Menjaga Kerahasiaan Pesan*. 1-6.

Herti Gustina, Meri Asparina, H. O. S. (2013). Makalah Penelitian Filologi. *Ilmu Pengetahuan Wawasan*, 1–6. http://hertigustin.blogspot.com/2015/01/metode-penelitian-filologi.html

Maharani, S., & Agus, F. (2009). Implementasi Perangkat Lunak Penyandian Pesan Menggunakan Algoritma RSA. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, *4*(1), 13–20.

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

PERMANA, A. A. (2019). Pengamanan Teks Menggunakan Metode Algoritma Rsa Dengan Verifikasi Realtime Biometrik Menggunakan Opencv. *Jurnal Teknik*, *7*(2). https://doi.org/10.31000/jt.v7i2.1352

Supriyono, S. (2008). PENGUJIAN SISTEM ENKRIPSI-DEKRIPSI DENGAN METODE RSA UNTUK PENGAMANAN DOKUMEN. *Jurnal Forum Nuklir*, *2*(2), 179–194.

Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *JTIK (Jurnal Teknik Informatika Kaputama)*, *3*(2), 29–37.