

IMPLEMENTASI ALGORITMA RSA (RIVEST-SHAMIR-ADLEMAN) PADA LAYANAN *CHATTING* BERBASIS LAN (*LOCAL AREA NETWORK*)

¹Dony Catur Dermawan. ²Ari Eko W.,S.T.,M.Kom., ³Triawan Adi C.,M.Kom.
Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember
Email : donycad2212@gmail.com

ABSTRAK

Pertukaran pesan (*chatting*) sudah luas digunakan oleh berbagai kalangan. Pesan yang dikirimkan sering berisi informasi yang penting. Masalah keamanan informasi pesan (*chatting*) seringkali kurang mendapat perhatian dari perancang dan pengelola informasi. Dalam pencegahannya dapat digunakan algoritma kriptografi kunci publik sehingga pesan (*chatting*) yang akan dikirimkan diamankan dan dirahasiakan. Salah satu metode kriptografi kunci publik yang paling aman dalam jaringan digunakan algoritma RSA (Rivest-Shamir-Adleman). Tujuan penelitian ini adalah mengimplementasikan algoritma RSA (Rivest-Shamir-Adleman) pada layanan *chatting* berbasis LAN (*Local Area Network*) sebagai solusi untuk mengamankan pesan yang dikirimkan. Selanjutnya pesan (*chatting*) yang terenkripsi dikirimkan melalui jaringan untuk dideskripsi menjadi pesan plainteks. Jika hasilnya dapat dideskripsikan oleh penerima maka pesan yang dikirimkan terjamin keasliannya. Pesan yang dikirimkan melalui jaringan, pesan tersebut sangat sulit dideskripsi tanpa mengetahui kunci privat.

Kata kunci : *chatting*, RSA (Rivest-Shamir-Adleman), Kriptografi

ABSTRACT

Exchange of messages (*chatting*) has been widely used by many. Messages sent often contain important information. Information security issues messages (*chatting*) is often less attention from designers and managers of information. Can be used in the prevention of public key cryptography algorithm so that messages (*chatting*) that will be sent secured and confidential. One method of public key cryptography safest in the network use the RSA algorithm (Rivest-Shamir-Adleman). The purpose of this study adalah implementing RSA algorithm (Rivest-Shamir-Adleman) on the chat service-based LAN (Local Area Network) as a solution for securing messages sent. Further messages (*chatting*) sent encrypted over the network to be described into a plaintext message. If the results can be described by the recipient that the message is sent guarantee its authenticity. Messages sent via the network, the message is very difficult to be described without knowing the private key.

Keywords : Chatting, RSA (Rivest-Shamir-Adleman), Cryptography

I. PENDAHULUAN

Pertukaran pesan (*chatting*) sudah luas digunakan oleh berbagai kalangan. Pesan yang dikirimkan sering berisi informasi yang penting. Masalah keamanan informasi pesan (*chatting*) seringkali kurang mendapat perhatian dari perancang dan pengelola informasi. Pesan (*chatting*) tidak akan menjadi rahasia lagi apabila ditengah jalan informasi itu diakses oleh orang yang tidak berhak atau tidak berkepentingan.

Pada proses pengiriman pesan (*chatting*) terdapat beberapa hal yang harus diperhatikan, yaitu : kerahasiaan, integritas data, autentikasi dan *non repudiasi*. Oleh karenanya dibutuhkan suatu proses penyandian atau pengkodean data sebelum dilakukan proses pengiriman. Sehingga pesan (*chatting*) yang dikirim terjaga kerahasiaannya dan tidak dapat dengan mudah diubah untuk menjaga integritas data tersebut.

Untuk menjaga kerahasiaan, salah satunya dengan enkripsi data informasi yang akan dikirimkan dengan kriptografi. Enkripsi data yang bisa dilakukan menggunakan algoritma RSA (Rivest-Shamir-Adleman). Algoritma RSA (Rivest-Shamir-Adleman) digunakan untuk membangkitkan sebuah kunci rahasia antara dua komputer yang saling terhubung. RSA (Rivest-Shamir-Adleman) digunakan dengan alasan tingkat keamanan sangat tinggi.

Dalam tugas akhir ini akan dilakukan implementasi algoritma RSA (Rivest-Shamir-Adleman) dalam pertukaran pesan antara dua komputer yang terhubung jaringan. Sehingga komunikasi antara komputer yang terhubung jaringan bisa terjamin keamanannya.

II. DASAR TEORI

2.1 Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan perangkat jaringan lainnya yang terhubung dalam satu kesatuan yang bekerja bersama - sama untuk mencapai suatu tujuan yang sama. Pertukaran Informasi dan data melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data atau mencetak pada printer yang sama dan bersama-sama menggunakan *hardware/software* yang terhubung dengan jaringan. Setiap komputer, printer atau periperal yang terhubung dengan jaringan disebut *node*. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan *node*.

Secara umum jaringan komputer dibagi atas lima jenis, yaitu;

1. *Local Area Network* (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama

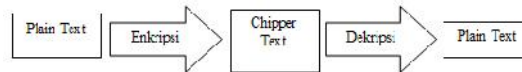
2. sumberdaya (misalnya printer) dan saling bertukar informasi.
3. *Metropolitan Area Network* (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.
4. *Wide Area Network* (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program atau aplikasi pemakai.
5. Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak compatible dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet. (Budi Sutedjo Dharma Oetomo,2003)
6. Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel.

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta layanan disebut klien (*client*) dan yang memberi layanan disebut pelayan (*server*). Arsitektur ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer.(Budi Sutedjo Dharma Oetomo,2003)

2.2 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan Kriptografi adalah sebuah ilmu menyandikan dan mengacak suatu pesan untuk menjaga keamanan dari isi pesan tersebut.(Kurniawan, 2004).Kriptografi diperlukan untuk menghindari pihak yang tidak berhak mengetahui isi dari pesan yang dikirimkan tersebut. Dengan adanya kriptografi, isi dari pesan akan diacak sedemikian rupa menggunakan algoritma kriptografi tertentu sehingga akan menghasilkan sebuah pesan yang acak yang tidak dapat dibaca sebelum isi pesan yang sebenarnya kembali dimunculkan menggunakan algoritma kriptografi tersebut. (Schneier, 1996).

Pesan asli sebelum dienkripsi disebut plain text. Sedangkan pesan yang sudah diacak disebut chipper text. Proses perubahan plain text menjadi chipper text disebut dengan enkripsi, sedangkan proses perubahan chipper text kembali menjadi plain text disebut dengan deskripsi.



Gambar 2.1 Proses Enkripsi Dekripsi

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan deskripsi. Enkripsi adalah proses mengubah suatu pesan asli (plaintext) menjadi suatu pesan dalam bahasa sandi (cipherteks), $C = E(M)$ dimana:

M = pesan asli

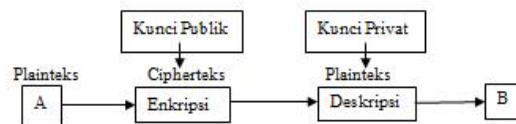
E = proses enkripsi

C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi)

Sedangkan deskripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali, yaitu $M = D(C)$ dimana D = proses dekripsi. Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci yang dibagi menjadi kunci simetris dan asimetris. (Munir, 2006)

2.3 Algoritma RSA (Rivest-Shamir-Adleman)

Algoritma RSA (Rivest-Shamir-Adleman) merupakan algoritma kriptografi kunci publik (asimetris). Ditemukan pertama kali pada tahun 1977 oleh R. Rivest, A. Shamir, dan L. Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci privat. Kunci publik boleh diketahui oleh siapa saja dan digunakan untuk proses enkripsi. Sedangkan kunci privat hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses deskripsi. Keamanan sandi RSA (Rivest-Shamir-Adleman) terletak pada sulitnya memfaktorkan bilangan yang besar. Sampai saat ini RSA (Rivest-Shamir-Adleman) masih dipercaya dan digunakan secara luas di internet.



Gambar 2.2 Skema Algoritma Kunci Publik

Besaran-besaran yang digunakan pada algoritma RSA (Rivest-Shamir-Adleman) antara lain:

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

3. $db(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci deskripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Secara garis besar, proses kriptografi pada algoritma RSA (Rivest-Shamir-Adleman) terdiri dari 3 tahapan yaitu :

1. Pembangkitan Kunci

Untuk membangkitkan kedua kunci, dipilih dua buah bilangan prima yang sangat besar, p dan q . Untuk mendapatkan keamanan yang maksimum, dipilih dua bilangan p dan q yang besar. Kemudian dihitung :

$$n = p * q$$

Kemudian dihitung:

$$\Phi(n) = (p-1)(q-1)$$

Lalu dipilih kunci enkripsi secara acak, sedemikian sehingga e dan $(p-1)(q-1)$ relative prima. Artinya e dan ϕ tidak memiliki faktor persekutuan bersama. Kemudian dengan algoritma Euclidean yang diperluas, dihitung kunci dekripsi d , sedemikian sehingga:

$$ed = 1 \pmod{(p-1)(q-1)}$$

atau

$$ed - 1 = k(p-1)(q-1)$$

di mana k merupakan konstanta integer. Perhatikan bahwa d dan n juga relative prima. Bilangan e dan n merupakan kunci publik, sedangkan d kunci privat. Dua bilangan prima p dan q tidak diperlukan lagi. Namun p dan q kadang diperlukan untuk mempercepat perhitungan deskripsi.

2. Proses Enkripsi

Untuk mengenkripsi pesan m , terlebih dahulu pesan dibagi kedalam blok-blok numeric yang lebih kecil dari n (dengan data biner, dipilih pangkat terbesar dari 2 yang kurang dari n). Jadi jika p dan q bilangan prima 100 digit, maka n akan memiliki sekitar 200 buah digit dari setiap blok pesan m , seharusnya kurang dari 200 digit panjangnya. Pesan yang terenkripsi (c), akan tersusun dari blok-blok (c) yang hampir sama panjangnya. Rumus enkripsinya adalah:

$$c = m^e \pmod n$$

dimana:

m = pesan asli

e = proses enkripsi

c = pesan dalam bahasa sandi

n = modulus

3. Proses Deskripsi

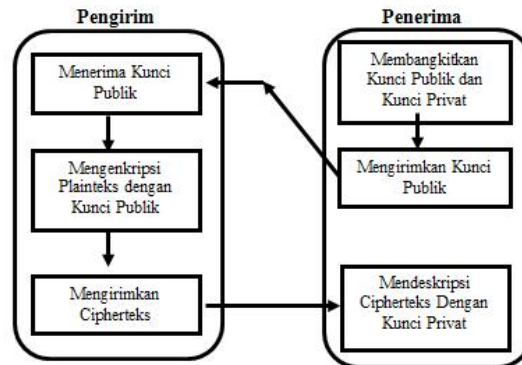
Setelah menerima pesan yang sudah terenkripsi maka penerima pesan akan melakukan proses dekripsi pesan dengan cara:

$$m = cd \pmod n$$

dimana:

m = pesan asli

e = proses enkripsi
 c = pesan dalam bahasa sandi
 n = modulus



Gambar 2.3 Proses Algoritma RSA (Rivest-Shamir-Adleman)

Gambar 2.3 diatas menjelaskan tentang proses pembentukan algoritma RSA (Rivest-Shamir-Adleman). Algoritma RSA (Rivest-Shamir-Adleman) dijalankan dengan membangkitkan kunci publik dan kunci privat. Penerima kemudian mengirimkan kunci publik kepada pengirim untuk mengenkripsi pesan atau plaintext. Setelah pesan terenkripsi dalam bentuk ciphertext maka dapat dikirimkan kembali ke penerima. Setelah penerima mendapatkan pesan tersebut maka dapat dideskripsi dengan kunci privatnya.

Contoh proses Algoritma RSA (Rivest-Shamir-Adleman) dapat dijalankan pada tahapan-tahapan yaitu sebagai berikut:

Plaintext = M= CINTA MATI

M diubah ke dalam ASCII = 67737884653277658473

Pembentukan kunci :

1. Misalkan $p = 47$ dan $q = 71$ (p dan q harus bilangan prima) dimana p dan q dipilih secara acak.
2. Hitung: $n = p \cdot q = 47 \cdot 71 = 3337$
3. Maka $\Phi(n) = (p-1)(q-1) = 3220$
4. Pilih kunci publik $e = 79$ (relative prima terhadap 3220 karena pembagi terbesar bersamanya adalah 1).
5. Didapat kunci private sebagai berikut :
 $e \cdot d = 1 \pmod{\phi(n)}$
 $d = 1 \pmod{\phi(n)} = 1019$
6. Maka kunci publik dan kunci privat adalah
 Kunci publik = $(e, n) = (79, 3337)$
 Kunci privat = $(d, n) = (1019, 3337)$

Ubah Plainteks menjadi Cipherteks dengan kunci publik:

$$c_1 = m_1^e \pmod n = 67779 \pmod{3337} = 231$$

$$c_2 = m_2^e \pmod n = 37879 \pmod{3337} = 3092$$

$$c_3 = m_3^e \pmod n = 84679 \pmod{3337} = 470$$

$$c_4 = m_4^e \pmod n = 53279 \pmod{3337} = 407$$

$$c_5 = m_5^e \text{ mod } n = 77679 \text{ mod } 3337 = 14$$

$$c_6 = m_6^e \text{ mod } n = 58479 \text{ mod } 3337 = 2842$$

$$c_7 = m_7^e \text{ mod } n = 07379 \text{ mod } 3337 = 725$$

Jadi cipherteks yang dihasilkan adalah

231 3092 470 407 14 2842 725

Ubahlah cipherteks dengan menggunakan kunci privat

$$m_1 = c_1^d \text{ mod } n = 2311019 \text{ mod } 3337 = 677$$

$$m_2 = c_2^d \text{ mod } n = 30921019 \text{ mod } 3337 = 378$$

$$m_3 = c_3^d \text{ mod } n = 4701019 \text{ mod } 3337 = 846$$

$$m_4 = c_4^d \text{ mod } n = 4071019 \text{ mod } 3337 = 532$$

$$m_5 = c_5^d \text{ mod } n = 141019 \text{ mod } 3337 = 776$$

$$m_6 = c_6^d \text{ mod } n = 28421019 \text{ mod } 3337 = 584$$

$$m_7 = c_7^d \text{ mod } n = 28421019 \text{ mod } 3337 = 73$$

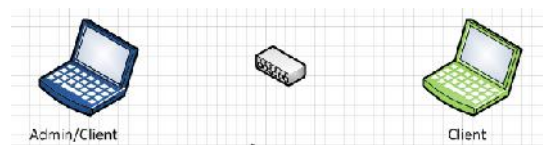
Jadi plaintext yang dihasilkan :

677 378 846 532 776 584 73=CINTA MATI

III. RANCANGAN SISTEM

3.1 Gambaran Sistem

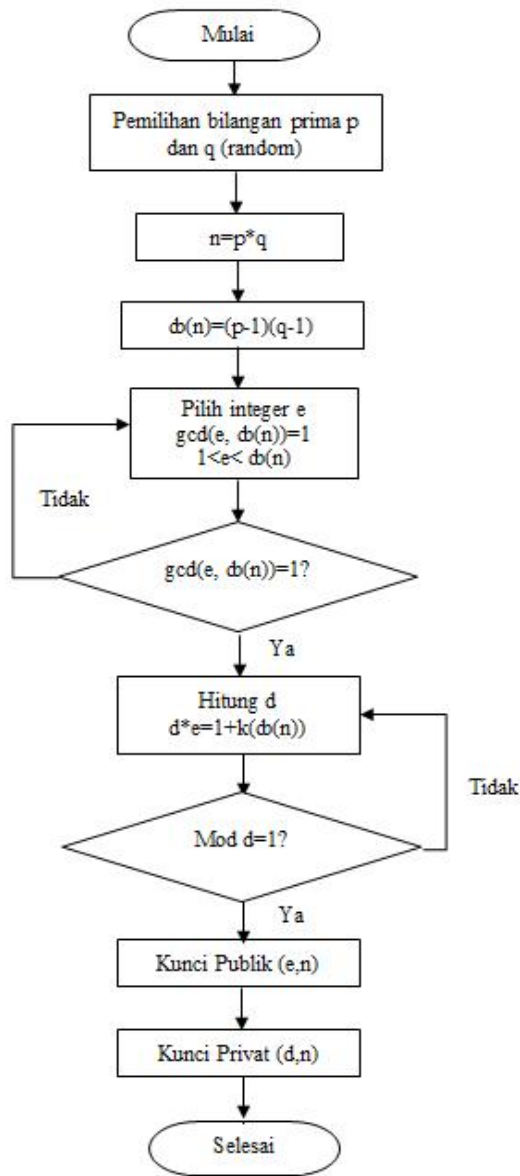
Gambaran sistem merupakan gambaran lengkap tentang sistem yang akan dibangun. Sistem menggunakan 1 admin dan 2 client yang dibangun dalam jaringan localhost dan kemudian akan diberikan sistem keamanan algoritma RSA dalam enkripsi dan deskripsi pesan.



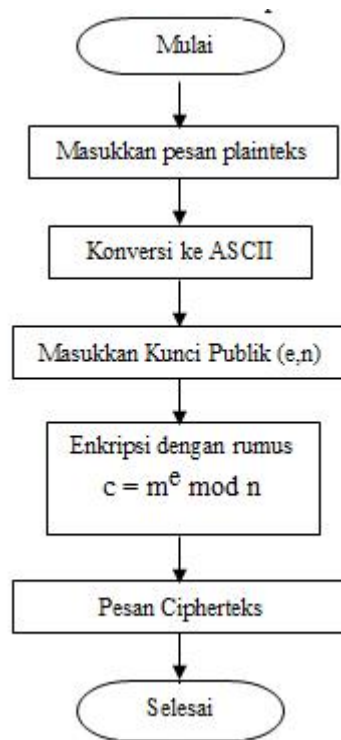
Gambar 3.1 Jaringan Localhost

3.2.1 Flowchart

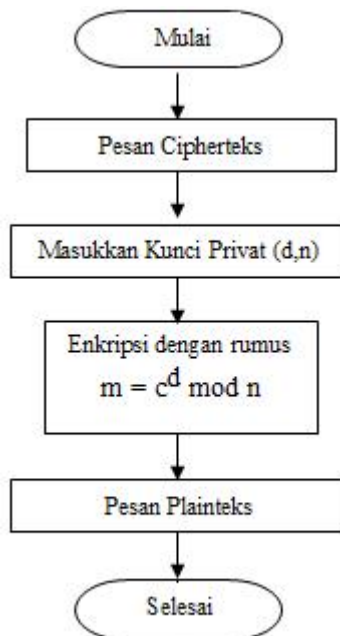
Flow Chart pada Algoritma RSA (Rivest-Shamir-Adleman) disusun sesuai tahapan proses yaitu terdiri dari Setup Key, Proses Enkripsi, dan Proses Deskripsi



Gambar 3.2 Flowchart Setup Key



Gambar 3.3 *Flowchart Proses Enkripsi*



Gambar 3.4 *Flowchart Proses Deskripsi*

IV. IMPLEMENTASI DAN UJICOBA

Penelitian ini adalah perangkat lunak enkripsi dan deskripsi pesan sebagai implementasi Algoritma RSA (Rivest-Shamir-Adleman).

Dalam proses pengiriman pesan dimasukkan dalam database mysql yang ditampilkan dalam ERD (*Entity Relationship Diagram*) dibawah ini.



Gambar 4.1ERD Pengiriman Pesan

Perangkat lunak yang dihasilkan terdiri dari 5 halaman yaitu halaman utama, halaman admin, halaman penerima, halaman pengirim, dan halaman penyerang yang masing – masing halaman dapat dilihat pada gambar dibawah ini.

4.1 Halaman Utama



Gambar 4.2Halaman Utama

Gambar 4.2 halaman utama yang terdapat form untuk login dengan mempunyai 3 hak akses user yaitu admin, pengirim, dan penerima. Ketika masuk ke halaman admin maka username-nya adalah admin dan password adalah admin. Bisa juga ke halaman penerima maka username yang dimasukkan adalah galih dan password yaitu galih, maka akan masuk ke halaman penerima.php .Jika ingin masuk ke halaman pengirim yaitu pengirim.php maka username-nya ratna dan password juga ratna.

4.2 Halaman Admin

Halaman admin adalah halaman yang digunakan untuk melakukan semua proses dalam aplikasi ini. Termasuk untuk mencoba jalannya aplikasi yang akan disimulasikan. Halaman ini dapat dilihat pada gambar 4.3

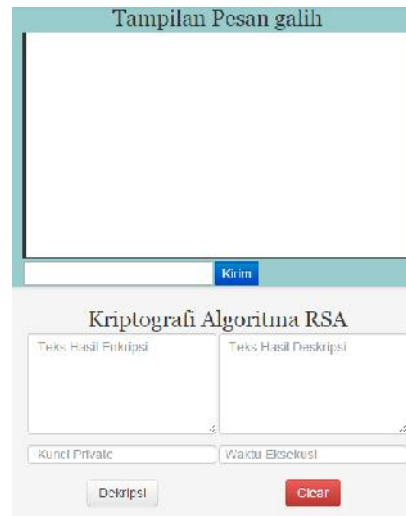


The screenshot shows a web interface titled "Tampilan Pesan admin". It features a large white text area for input, a blue "Kirim" button below it, and three text boxes for "Teks Sebelum Enkripsi", "Teks Hasil Enkripsi", and "Teks Hasil Deskripsi". Below these are input fields for "Kunci Public" and "Kunci Private", and buttons for "Enkripsi", "Deskripsi", and "Clear".

Gambar 4.3Halaman Admin

4.3 Halaman Penerima

Pada halaman ini terdapat tampilan pesan, dan hasil pesan yang diterima yang akan di deskripsi menjadi pesan yang asli atau plainteks. Penerima juga bisa mengirimkan pesan plainteks sehingga dapat diketahui oleh pengirim dan penyerang. Halaman penerima ini juga dilengkapi waktu eksekusi untuk mendeskripsikan karakter. Halaman ini dapat dilihat pada gambar 4.4



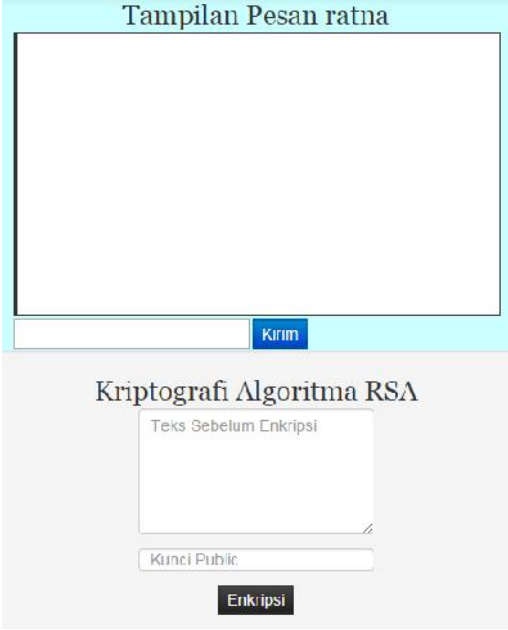
The screenshot shows a web interface titled "Tampilan Pesan galih". It features a large white text area for input, a blue "Kirim" button below it, and two text boxes for "Teks Hasil Enkripsi" and "Teks Hasil Deskripsi". Below these are input fields for "Kunci Private" and "Waktu Eksekusi", and buttons for "Deskripsi" and "Clear".

Gambar 4.4Halaman Penerima

4.4 Halaman Pengirim

Halaman ini dapat mengirimkan pesan asli atau plainteks dan pesan yang telah di enkripsi atau cipherteks. Pengirim merupakan pengirim pesan yang ditujukan pada

penerima, oleh karena itu pengirim hanya bisa mengenkripsi data menjadi cipherteks dan hanya penerima yang akan mendeskripsikannya menjadi plainteks kembali. Halaman ini dapat dilihat pada gambar 4.5.

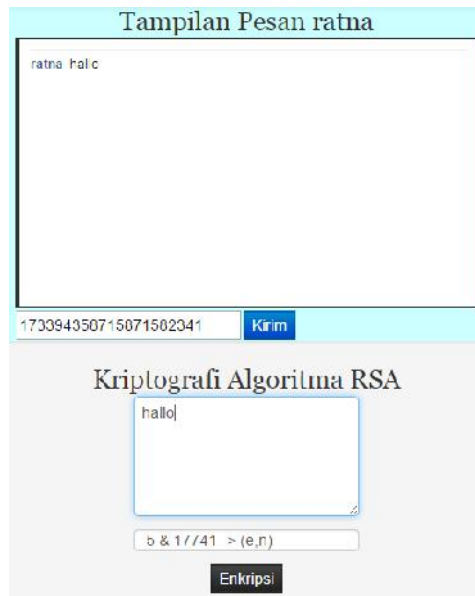


The image shows a web application interface for RSA encryption. It is divided into two main sections. The top section, titled "Tampilan Pesan ratna", features a large empty text area for input and a blue "Kirim" button. The bottom section, titled "Kriptografi Algoritma RSA", contains a text input field labeled "Teks Sebelum Enkripsi", a text input field labeled "Kunci Public", and a black "Enkripsi" button.

Gambar 4.5 *Halaman Pengirim*

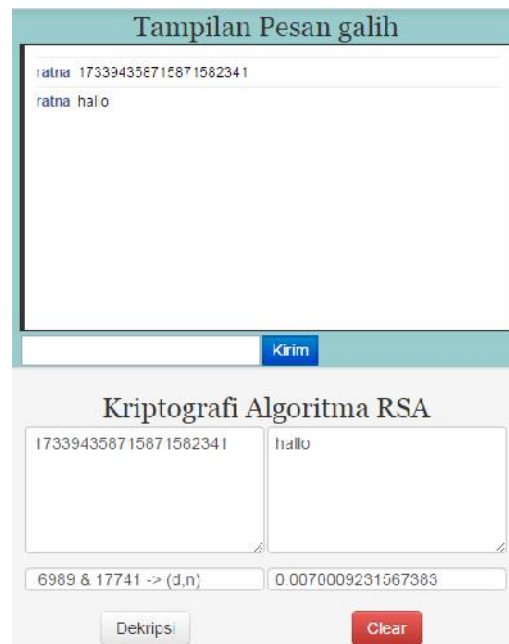
4.5 Pengiriman Pesan Terenkripsi

Setelah melakukan proses pengiriman pesan yang dapat disadap oleh attacker kemudian dibuat pengiriman pesan yang terenkripsi. Simulasi pesan ini akan dijalankan pada proses enkripsi pesan yang akan dikirimkan kemudian saat pesan diterima pihak dapat mendeskripsikan pesan tersebut sehingga pesan yang dijalankan terjamin keasliannya. Dalam aplikasi ini juga diasumsikan bahwa attacker juga dapat menyerang aplikasi tetapi hal tersebut dapat diatasi setelah proses deskripsi sehingga pesan yang dikirimkan attacker tidak akan terbaca. Pada gambar 4.9 dibawah ini terjadi proses enkripsi pesan oleh ratna kemudian dikirimkan kepada galih. Pesan yang terenkripsi akan berupa angka yang telah dibentuk menggunakan algoritma RSA (Rivest-Shamir-Adleman).



Gambar 4.6 Pengiriman Pesan Terenkripsi

Pesan yang dikirimkan melalui jaringan sudah dalam bentuk terenkripsi. Pada gambar 4.6 ditampilkan bahwa pesan sudah terkirim dalam bentuk enkripsi. Setelah itu galih dapat mendeskripsikan dengan kunci privatnya.



Gambar 4.7 Mendeskripsikan Pesan Yang Terkirim

Gambar 4.7 menunjukkan pesan yang terenkripsi dapat dideskripsikan dengan kunci privat sehingga pesan cipherteks dapat didefinisikan dan pesan asli tidak dapat. Jika pesan itu dienkripsi dengan kriptografi algoritma RSA (Rivest-Shamir-Adleman) maka pesan dapat di deskripsikan.

Pada saat pengiriman pesan ada proses verifikasi pesan cipherteks dan pesan plainteks sehingga pesan yang dikirimkan kepada galih benar-benar asli dari ratna. Saat attacker menyerang dengan data asli pada pesan galih maka hal tersebut tidak dapat dideskripsikan

V. KESIMPULAN

1. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus. Selain itu, bahwa ternyata pada proses spoofing yaitu man the middle attack sangat mungkin untuk menjebol informasi pesan yang dikirimkan lewat jaringan.
2. Sistem enkripsi kunci publik-privat, yang memegang peranan dalam menjebol kunci privat adalah kesulitan mencari faktor prima bilangan yang sangat besar. Beberapa kunci yang dipergunakan 10 tahun lalu saja kini sama sekali tidak laik pakai seiring dengan perkembangan ilmu pengetahuan dan teknologi. Kunci publik dari RSA (Rivest-Shamir-Adleman) adalah teknologi kunci publik 40-bit, yang ternyata dapat dijebol dalam waktu 1,3 hari dengan 100 komputer menggunakan brute-force attack. Ronald Rivest, salah seorang penemu RSA (Rivest-Shamir-Adleman), juga pernah menghitung bahwa untuk menemukan kunci RSA 512-bit dengan cara brute-force attack membutuhkan biaya 8,2 juta dollar AS . Untuk kasus tertentu, ini pun tidak aman. Kini perusahaan-perusahaan disarankan menggunakan kunci 2048 bit agar data aman sampai tahun 2015.
3. Pesan yang dikirimkan melalui jaringan, pesan tersebut sangat sulit dideskripsi tanpa mengetahui kunci privat. Dan untuk proses enkripsi meskipun kunci publik sudah diketahui orang lain tetapi tetap pihak attacker tidak bisa mengenkripsi pesan aslinya.

DAFTAR PUSTAKA

- Kurniawan, J. 2004. Kriptografi, Keamanan Internet, dan Jaringan Komunikasi. Bandung: Informatika.
- Rizkianto Agung, 2011, Implementasi Algoritma Diffie-Hellman Untuk menangani Ip Spoofing Pada Jaringan .Skripsi Sarjana ITS. Surabaya: tidak diterbitkan.
- Mahardika Primaditya Surya, 2013, Aplikasi Chatroom Berbasis Web .Skripsi Sarjana Universitas STIKUBANK Semarang: tidak diterbitkan

Sadikin, Rifki. 2006. Kriptografi untuk Keamanan Jaringan. Yogyakarta: Andi Publisher.

Susilo, Anton Rifco. 2007. “Analisis dan Implementasi Penerapan Enkripsi Algoritma Kunci Publik RSA Dalam Pengiriman Data Web – Form”. Makalah Jurusan Teknik Informatika ITB, Bandung.

Arifin, Zainal. 2009. “Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman”. Jurnal Prodi Ilmu Komputer Universitas Mulawarman , Samarinda

Harahap Rahmat Hidayat, 2009, Instalasi Jaringan Wireless LAN (Hotspot Area) Sebagai Sarana Komersil .Tugas Akhir Universitas Sumatera Utara: tidak diterbitkan

Hakim, Lukmanul. 2010. Bikin Website Super Keren dengan PHP dan JQuery. Yogyakarta: Lokomedia.

Yuana, Rosihan Ari. 2010. 67 Trik dan Ide Brilian Master PHP. Yogyakarta: Lokomedia.

Hakim, Lukmanul. 2010. Jalan Pintas Menjadi Master PHP. Yogyakarta: Lokomedia.