Implementasi Algoritma RSA untuk Pengamanan Transmisi Data Pada Jaringan *Wireless* Intranet

Diajukan Sebagai Syarat Untuk Menyelesaikan Pendidikan Program Strata-1 Pada
Jurusan Teknik Infotmatika Fakultas Ilmu Komputer UNSRI

Oleh:

CHRISTOFER YEREMIA

NIM: 09021181621024

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN TUGAS AKHIR

IMPLEMENTASI ALGORITMA RSA UNTUK PENGAMANAN TRANSMISI DATA PADA JARINGAN *WIRELESS* INTRANET

Oleh:

CHRISTOFER YEREMIA
NIM : 09021181621024

Palembang, Juni 2020

Pembimbing I,

Drs. Megah Mulya, M.T.
NIP. 196602202006041001

Pembimbing II,

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika,

Rifkie Primartha, M.T
NIP. 197706012009121004

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Selasa tanggal 12 Mei 2020 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Christofer Yeremia
Nim : 09021181621024
Judul : Implementasi Algoritma RSA untuk Pengamanan Transmisi Data Pada Jaringan Wireless Intranet

1. Pembimbing I

   Drs. Megah Mulya, M.T ……
   NIP. 196602202006041001

2. Pembimbing II

   Mastura Diana Marieska, M.T. ……
   NIP. 198603212018032001

3. Penguji I

   Dian Palupi Rini, M.Kom., Ph.D. ……
   NIP. 197802232006042002

4. Penguji II

   Desty Rodiah, M.T. ……
   NIP. 1671016112890005

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, MT
NIP. 197706012009121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Christofer Yeremia
NIM	: 09021181621024
Program Studi	: Teknik Informatika
Judul Skripsi	: Implementasi Algoritma RSA untuk Pengamanan Transmisi Data Pada Jaringan Wireless Intranet

Hasil Pengecekan Software *iThenticate/Turnitin* : 8%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Juni 2020

Christofer Yeremia
NIM. 09021181621024

MOTTO DAN PERSEMBAHAN

"I can do all things through Christ who strengthens me"

Philippians 4:13

Kupersembahkan karya tulis ini kepada :

- *Orangtuaku tercinta dan adikku tercinta*
- *Keluarga besarku*
- *Sahabat-sahabat Tersayangku*
- *Fakultas Ilmu Komputer*
- *Universitas Sriwijaya*

ABSTRACT

Securing data that will be transmitted on a wireless network is important. It is because many unauthorized parties can steal the data from the network. Therefore a strong method needed to secure the transmitted data so it cannot be read. One of the data security technique is asymmetric cryptography, where the encryption key and the decryption key are different. In this research, the asymmetry algorithm used is the RSA algorithm. The RSA algorithm is known to have a robust level of security, this is due to the difficulty of factoring large prime numbers. The data that will be secured using the RSA algorithm in this study is a string data type. The data encryption process is executed before the data transmitted into a wireless network. The decryption process is executed when the data has been received. Based on the results of tests that have been done, it is known that the speed of the RSA algorithm in performing encryption and decryption is influenced by the size of the public and private keys. After several experiments using public keys (16381, 11663) and private keys (3061, 11663) in securing 1152-bits data, the encryption time is 19,043 ms and the decryption time is 10.451 ms. The encryption time is greater than the decryption time because the public key is greater than the private key, so the encryption time is slightly longer than the decryption time.

Keywords : Cryptography, RSA (R'ivest - S'hamir - A’dleman), wireless

ABSTRAK

Pengamanan terhadap data yang akan ditransmisikan pada suatu jaringan *wireless* merupakan hal yang sangat penting. Hal ini dikarenakan banyak pihak yang tidak bertanggung jawab dapat melakukan pencurian data apapun yang ditransmisikan pada suatu jaringan *wireless*. Oleh sebab itu, dibutuhkan suatu metode yang sangat kuat untuk mengamankan suatu data yang akan ditransmisikan ke dalam jaringan. Salah satu teknik pengamanan data adalah menggunakan teknik kriptografi kunci asimetri, dimana kunci enkripsi dan kunci dekripsinya berbeda. Pada penelitian ini, algoritma asimetri yang digunakan adalah algoritma RSA. Algoritma RSA dikenal memiliki tingkat keamanan yang sangat kuat, hal ini dikarenakan sulitnya untuk melakukan pemfaktoran bilangan prima yang sangat besar. Data yang akan diamankan menggunakan algoritma RSA dalam penelitian ini merupakan data yang bertipe *string*. Proses enkripsi terhadap data dilakukan sebelum data ditransmisikan kedalam suatu jaringan *wireless*. Sedangkan untuk proses dekripsi dilakukan ketika data telah diterima. Berdasarkan hasil pengujian yang telah dilakukan, diketahui bahwa kecepatan algoritma RSA dalam melakukan enkripsi dan dekripsi dipengaruhi oleh besarnya kunci *public* dan kunci *private*. Setelah dilakukan beberapa percobaan algoritma RSA dengan menggunakan kunci public (16381,11663) dan kunci private (3061, 11663) dalam mengamankan data berukuran 1152 *bit*, didapat waktu enkripsi sebesar 19,043 *ms* dan waktu dekripsi sebesar 10,451 *ms*. Waktu enkripsi lebih besar dari pada waktu dekripsi dikarenkan kunci *public* lebih besar dari pada kunci *private*, sehingga waktu enkripsi sedikit lebih lama dari waktu dekripsi.

Kata Kunci : Kriptografi, RSA (R'ivest – S'hamir – A'dleman), *wireless*

KATA PENGANTAR

Penulis ucapkan puji syukur kepada Tuhan Yesus Kristus atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir dengan judul "**Implementasi Algoritma RSA untuk Pengamanan Transmisi Data Pada Jaringan Wireless Intranet**" dengan baik untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin mengucapkan terimakasih kepada pihak-pihak yang telah berperan memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung dalam menyelesaikan tugas akhir ini. Penulis ingin menyampaikan rasa terima kasih kepada:

1. Orang tuaku, Herry Sunyoto dan Reni Tinde Setia Ningsih, saudariku, Ajeng Geina Hasian dan seluruh keluarga besarku, khususnya Opung (ALM) dan Budet serta Oom dan Tante yang selalu mendokan serta memberikan dukungan baik moril maupun materil.
2. Bapak Jaidan Jauhari, M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya. Bapak Rifkie Primartha selaku Ketua Jurusan Teknik Informatika beserta jajarannya, dan Ibu Alvi Syahrini Utami, M.Kom selaku Sekretaris Jurusan Teknik Informatika.
3. Bapak Drs. Megah Mulya, M.T selaku dosen pembimbing I dan Ibu Mastura Diana Marieska, S.T., M.T selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
4. Bapak M. Fachrurrozi, S.Si., M.T selaku dosen pembimbing akademik, yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
5. Ibu Dian Palupi Rini, M.Kom., Ph.D selaku dosen penguji I, dan Ibu Desty Rodiah, M.T selaku dosen penguji II yang telah memberikan masukan dan dorongan dalam proses pengerjaan Tugas Akhir.

6. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Pak Tony, Mbak Anna dan Mbak Wiwin beserta seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
8. Sahabat-sahabat terbaik dalam hidupku yang selalu memberikan *support*. Maaf, tidak dapat disebutkan satu persatu.
9. Teman-teman jurusan Teknik Informatika yang telah berbagi keluh kesah, motivasi, semangat, dan canda tawa selama masa perkuliahan.
10. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu persatu.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, Juni 2020

Christofer Yeremia

DAFTAR ISI

Halaman

DAFTAR TABEL

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini akan menjelaskan mengenai latar belakang pengambilan topik "Implementasi Algoritma RSA untuk Pengamanan Transmisi Data Pada Jaringan *Wireless* Intranet" sebagai bahan penelitian. Pada bab ini juga akan menjelaskan rumusan masalah, tujuan dan manfaat penelitian, batasan masalah dan sistematika penulisan.

1.2 Latar Belakang

Perkembangan teknologi pada saat ini mengalami peningkatan yang sangat pesat khususnya pada bidang komunikasi. Hal tersebut dapat dilihat dengan semakin meningkatnya pengiriman dan pertukaran data melalui jaringan internet. Tetapi seiring dengan berkembangnya teknologi pada bidang komunikasi, menimbulkan beberapa permasalahan baru seperti, privasi dan keamanan terhadap suatu data yang ditransmisikan. Permasalahan – permasalahan inilah yang sering dimanfaatkan oleh pihak – pihak yang tidak bertanggung jawab untuk melakukan suatu tindak kejahatan. Terdapat berbagai macam kasus tindak kejahatan seperti, penyebaran informasi palsu, pembobolan akun, pencurian data dan masih banyak lagi.

Pada saat ini tindak kejahatan yang sering terjadi adalah pencurian data khususnya adalah data - data pelanggan pada suatu perusahaan. Terdapat banyak kasus pencurian dan penyalahgunaan data yang cukup meresahkan masyarakat.

Pada tahun 2013 hingga tahun 2018 terdapat pencurian data sebanyak 14,6 miliar data yang telah dicuri[1)], sedangkan pada tahun 2019 terdapat 945.800 data pelanggan yang dijual[2)]. Pencurian dan penjualan data pelanggan tersebut dapat disalahgunakan oleh pihak – pihak yang tidak berwenang untuk melakukan tindak kriminal seperti penipuan yang dapat mengakibatkan kerugian yang sangat besar pada pelanggan.

Terjadinya pencurian data – data pelanggan tersebut bisa disebabkan oleh dua faktor yaitu, pertama pencurian data dilakukan oleh karyawan perusahaan itu sendiri melalui jaringan *wireless* intranet perusahaan tersebut, ketika data pelanggan sedang di transmisikan atau dengan langsung melakukan pengaksesan ke dalam basis data perusahaan tersebut. Akan tetapi pencurian data dengan melakukan pengaksesan ke dalam suatu basis data cukup susah, hal ini dikarenakan keamanan dan pembatasan akses ke dalam basis data tersebut. Kemungkinan yang paling tinggi dalam pencurian data oleh karyawan dilakukan pada saat data tersebut ditransmisikan. Sedangkan faktor kedua dilakukan oleh pihak luar yang menerobos masuk ke dalam suatu jaringan *wireless* Intranet suatu perusahaan untuk mengambil data – data yang ditransmisikan.

Oleh sebab itu di perlukan suatu pengamanan terhadap data – data yang ditransmisikan melalui jaringan *wireless* intranet. Salah satu cara melakukan pengamanan tersebut dengan menggunakan metode kriptografi. Kriptografi adalah

---

1). Artikel berita “Liputan 6”,12 Oktober 2018

2). Artikel berita “CNN Indonesia”,21 Mei 2019

suatu ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat huruf atau tulisan tersebut tidak dapat dibaca (M. Arief, Fitriyani, & Ikhsan, 2015).

Metode kriptografi terbagi menjadi dua tipe algoritma kunci yaitu, simetris dan asimetris. Pada Algoritma kunci simetris, kunci enkripsi dan dekripsinya menggunakan kunci yang sama, sehingga apabila terjadi penyerangan akan lebih mudah untuk mendapatkan data yang telah diamankan. Sedangkan pada algoritma kunci asimetri, kunci enkripsi dan dekripsinya berbeda dan akan menyulitkan penyerang untuk mendapatkan data yang telah diamankan. Dikarenakan hal itulah banyak perusahaan – perusahaan yang menggunakan metode kriptografi dengan algoritma kunci asimetri dikarena ketahanannya terhadap serangan. Salah satu algoritma kunci asimetri yang banyak digunakan adalah algoritma RSA (R'ivest - S'hamir - A'dleman).

Pada Penelitian sebelumnya penerapkan pengamanan menggunakan algoritma RSA telah diterapkan untuk mengamankan aplikasi *file transfer client – server base* (M. Arief et al., 2015), Pengamanan data pada *Cloud computing* (S & Prabha, 2015), dan Pengamanan *Wireless Text Message Transmission* (Islam & Islam, 2014). Berdasarkan penelitian - penelitian yang telah dilakukan sebelumnya, pada penelitian ini algoritma yang akan digunakan untuk mengamankan data pada saat ditransmisikan di jaringan *wireless* intranet adalah algoritma RSA. Algoritma RSA merupakan algoritma yang mempunyai tingkat keamanan yang cukup tinggi, hal ini didasarkan pada sulitnya memfaktorkan bilangan besar menjadi faktor – faktor prima. Selain itu setelah dilakukan penelitian oleh (Muttaqin, Sajati, & Dewi, n.d.)

yang menggunakan algoritma RSA untuk mengamankan pesan pada aplikasi *chatting* ditemukan bahwa algoritma RSA juga memiliki juga mempunyai waktu enkripsi dan dekripsi yang dinilai cukup cepat untuk digunakan dalam pengamanan data yang *real-time*. Dikarenakan hal itu algoritma RSA menjadi pilihan yang tepat dalam mengamankan suatu data ketika di transmisikan pada jaringan *wireless* intranet untuk mencegah pencurian data – data pelanggan dan data suatu perusahaan.

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, pengamanan terhadap suatu data pada saat akan dikirimkan melalui jaringan *wireless* intranet merupakan suatu hal yang sangat penting. Hal ini dikarenakan banyaknya kasus pencurian dan penyalahgunaan data dilakukan oleh pihak yang tidak bertanggung jawab. Oleh sebab itu dibutuhkan suatu pengamanan yang kuat untuk melakukan pengaman terhadap data yang akan dikirimkan. Salah satu algoritma yang cukup kuat adalah algoritma kriptografi RSA dikarenakan memiliki tingkat keamanan yang tinggi, sebab sulitnya dalam melakukan pemfaktoran bilangan yang besar menjadi faktor prima yang berguna untuk memperoleh kunci *private*. Berdasarkan rumusan masalah tersebut maka pertanyaan penelitian yang akan diselesaikan adalah sebagai berikut :

1. Bagaimana mengamankan data pada saat ditransmisikan pada jaringan *wireless* Intranet dengan menggunakan algoritma RSA (R’ivest - S’hamir - A’dleman).
2. Apakah data *chiphertext* yang telah dienkripsi menggunakan algoritma RSA dapat dikembalikan kembali menjadi *plaintext*.

3. Apakah terdapat kenaikan ukuran data setelah dilakukan enkripsi dengan data yang tidak dilakukan enkripsi.
4. Berapa lama waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi pada suatu data.

1.4 Tujuan Penelitian

Tujuan dari penelitian tugas akhir ini adalah sebagai berikut :

1. Mengembangkan skema pengamanan transmisi data pada jaringan *wireless* Intranet.
2. Mengembangkan suatu aplikasi yang dapat melakukan pengamanan data pada saat ditransmisikan dengan menggunakan algoritma RSA.
3. Membuktikan data yang ditransmisikan adalah benar, dalam bentuk *chiphertext* dan dapat dikembalikan menjadi bentuk *plaintext* dengan menggunakan *software* ettercap.
4. Mengukur perbedaan ukuran data tanpa menggunakan enkripsi dengan data yang telah dilakukan enkripsi pada saat ditransmisikan.
5. Mengukur berapa lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi pada suatu data.

1.5 Manfaat Penelitian

Penelitian ini bermanfaat untuk menjaga data saat ditrasmisikan pada jaringan *wireless* intranet, agar tidak terjadi pencurian data yang dapat disalahgunakan untuk tindak kejahatan. kemudian untuk mengetahui kenaikan ukuran data pada saat dilakukan enkripsi, serta mengetahui waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi terhadap suatu data.

1.6 Batasan Masalah

Batasan masalah yang didefinisikan dalam pelaksanaan tugas akhir ini adalah sebagai berikut :

1. Aplikasi hanya melakukan enkripsi pada data - data pada jaringan *wireless* Intranet.
2. Enkripsi data dilakukan pada aplikasi *client* dan komputer *gateway*, dimana aplikasi *client* dan komputer *gateway* akan mempunyai kunci *public* masing-masing.
3. Dekripsi data dilakukan pada aplikasi *client* dan komputer gatewaiy, dimana aplikasi *client* dan komputer *gateway* dan akan mempunyai kunci *private* masing - masing.

1.7 Sistematika Penulisan

Sistematika Penulisan penelitian ini akan disusun dengan rangkaian sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini diuraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah/ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan berisikan penjelasan mengenai landasan teori yang akan dipakai dalam penelitian ini, penjelasan mengenai skema enkripsi dan dekripsi pada algoritma kriptografi RSA dan penelitian yang relevan.

BAB III. METODOLOGI PENELITIAN

Pada bab ini akan dibahas mengenai tahapan yang akan dilaksanakan pada penelitian ini. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci dengan mengacu pada suatu kerangka kerja. Di akhir bab ini berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini diuraikan tahapan yang dilakukan dalam proses pengembangan perangkat lunak untuk melakukan pengamanan data yang akan ditransmisikan dengan menggunakan algoritma RSA berdasarkan metode *Rational Unified Process* (RUP) yang mencakup fase insepsi, elaboras I, elaborasi II, konstruksi, dan insepsi.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini menguraikan tentang hasil pengujian dan analisis hasil pengujian dari pengembangan perangkat lunak yang telah diuraikan pada bab IV.

BAB VI. KESIMPULAN DAN SARAN

Akan dipaparkan mengenai kesimpulan dan saran dari hasil dan analisis penelitian yang telah dilakukan pada bab V

1.8 Kesimpulan

Pada bab ini telah dijelaskan mengenai latar belakang permasalahan yang akan diselesaikan yaitu, mengenai keamanan data pada saat ditransmisikan. Oleh karena itu akan dikembangkan sebuah perangkat lunak yang dapat melakukan pengamanan terhadap data yang akan ditransmisikan pada jarigan *wireless* intranet dengan menggunakan algoritma RSA sehingga data yang ditransmisikan tidak dapat dicuri oleh pihak yang tidak berwenang.

DAFTAR PUSTAKA

Apdillah, D., Siregar, H. F., & Swanda, H. (2018). *Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP*. *2*(1), 45–52.

Arief, A., & Saputra, R. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. *Scientific Journal of Informatics*, *3*(1), 46–54. https://doi.org/10.15294/sji.v3i1.6115

Arief, M., Fitriyani, & Ikhsan, N. (2015). Kriptografi Rsa Pada Aplikasi File Transfer Client- Server Based. *Jurnal Ilmiah Teknologi Informasi Terapan*, *1*(3).

Arifin, Z. (2009). Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman. *Informatika Mulawarman*, *4*(3), 7–14.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2017). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi Dan Sistem Komputer*, *3*(2), 253. https://doi.org/10.14710/jtsiskom.3.2.2015.253-258

Ginting, N. F., & Ginting, M. (2017). Perbandingan Kriptografi RSA dengan Base64. *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)*, *02*(02), 47–52.

Islam, M. A., & Islam, A. Z. M. T. (2014). Secure Wireless Text Message Transmission with the Implementation of RSA Cryptographic Algorithm. *International Journal of Computer Networks and Communications Security*,

2(5), 146–151.

Muchlis, B. S., & Rachmawati, D. (2019). *Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik*. *2*, 49–64.

Muttaqin, Sajati, H., & Dewi, N. (n.d.). *PENERAPAN SISTEM KEAMANAN MENGGUNAKAN CRYPTOGRAPHY PADA APLIKASI CHATTING DENGAN MEMODIFIKASI ALGORITMA RIVEST SHAMIR ADELEMAN (RSA)*. 61–74.

Raju, D. G., & Kiran, K. (n.d.). *Analysis of Avalanche Effect in Asymmetric Cryptosystem Using NTRU & RSA*. *7884*.

S, M. S. N., & Prabha, R. (2015). *Cloud Computing : Data Security Using RSA*. *IV*(X), 57–59.