**LAPORAN PRAKTIKUM**

**PRAKTIK SISTEM KEAMANAN DATA**

REVIEW JURNAL RSA



**Disusun oleh :**

Muhammad Farhan (V3922033)

**Dosen :**

Yusuf Fadila Rachman, S. Kom, M. Kom

**PSDKU D-III TEKNIK INFORMATIKA**

**SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**2023**

1. **Review Jurnal 1**
2. Judul dan Latar Belakang Masalah :

* Judul : Implementasi Kriptografi Kunci Publik pada Aplikasi Instant Messaging dengan Algoritma RSA-CRT.
* Latar belakang masalah :

Kemajuan teknologi komputer dan telekomunikasi telah membantu dalam menyelesaikan banyak pekerjaan dengan cepat, akurat, dan efisien. Salah satu kemajuan teknologi komunikasi adalah aplikasi instant messaging atau pesan instan. Namun, semakin banyaknya pengguna aplikasi instant messaging berakibat pada dampak negatif berupa penyadapan data khususnya saat terjadi komunikasi yang bersifat rahasia. Oleh karena itu, aspek keamanan dalam pertukaran informasi dianggap penting. Kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data. RSA merupakan algoritma kriptografi kunci publik yang tidak membutuhkan saluran yang aman untuk distribusi kunci. Namun, proses dekripsi algoritma RSA sering terjadi kendala karena ukuran kunci dekripsi yang relatif besar dapat memperlambat proses. Oleh karena itu, algoritma RSA dapat dimodifikasi dengan algoritma CRT (Chinese Remainder Theorem), sering disebut dengan Algoritma RSA-CRT untuk mempercepat proses dekripsi.

1. Tujuan Penelitian :

Untuk mengimplementasikan algoritma kriptografi RSA-CRT pada aplikasi instant messaging dengan panjang bit n mulai dari 56 bit sampai 88 bit. Penelitian ini bertujuan untuk mempercepat proses dekripsi pada aplikasi messaging dengan menggunakan algoritma RSA-CRT.

1. Algoritma yang dipakai beserta alur penelitiannya :

Algoritma yang digunakan dalam penelitian ini adalah algoritma kriptografi kunci publik RSA-CRT. Alur penelitiannya mencakup langkah-langkah sebagai berikut:

1. Pembangkit Kunci RSA-CRT

a. Bangkitkan bilangan prima besar p dan q

b. Hitung nilai modulus n = p x q

c. Hitung menggunakan fungsi Euler(n) = (p-1) x (q-1)

d. Pilih nilai integer e acak sebagai kunci publik, dengan syarat memenuhi Greater Common Divisor (GCD) (e,(n)) = 1, 1 < e <(n)

e. Hitung kunci privat d sehingga d x e = 1 (mod(n))

f. Hitung dP = d mod (p – 1)

g. Hitung dQ = d mod (q – 1)

h. Hitung qInv = q^(-1) pada Zp

i. Kunci publik = (e, n), Kunci privat = (dP, dQ, qInv, p, q)

2. Enkripsi RSA-CRT

- Kunci publik RSA-CRT sama dengan sistem RSA yaitu (e, n), sehingga algoritma enkripsi tidak mengalami perubahan.

3. Dekripsi RSA-CRT

- Proses dekripsi RSA-CRT menggunakan nilai dP, dQ, qInv, p, q untuk mempercepat waktu dekripsi.

Algoritma ini diimplementasikan pada aplikasi instant messaging dengan panjang bit n mulai dari 56 bit sampai 88 bit

1. Hasil penelitian dan kesimpulan :

Penelitian ini mengimplementasikan algoritma kriptografi RSA-CRT pada aplikasi instant messaging dengan panjang bit n mulai dari 56 bit sampai 88 bit. Hasil penelitian menunjukkan bahwa menggunakan dekripsi RSA-CRT memiliki kecepatan rata-rata dua kali lebih cepat dibandingkan dengan menggunakan dekripsi RSA. Kesimpulan dari penelitian ini adalah bahwa implementasi algoritma RSA-CRT pada aplikasi instant messaging dapat mempercepat proses dekripsi, terutama saat menggunakan panjang bit n yang lebih besar.

1. Kelebihan dan kekurangan :

**Kelebihan :**

Kelebihan dari implementasi algoritma RSA-CRT pada aplikasi instant messaging adalah kemampuannya untuk mempercepat proses dekripsi, terutama saat menggunakan panjang bit n yang lebih besar. Hal ini dapat meningkatkan keamanan pesan yang dikirim melalui saluran yang tidak aman.

**Kekurangan :**

Kekurangan dari implementasi ini mungkin terletak pada kompleksitas algoritma RSA-CRT yang memerlukan perhitungan tambahan untuk menghasilkan kunci privat tambahan seperti dP, dQ, dan qInv. Selain itu, implementasi yang kurang tepat dapat menyebabkan kerentanan keamanan pada aplikasi.

1. **Review Jurnal 2**
2. Judul dan Latar Belakang Masalah :

* Judul : Model Keamanan Informasi Berbasis Digital Signature dengan Algoritma RSA
* Latar Belakang Masalah :

Latar belakang masalah dari penelitian ini adalah kebutuhan akan keamanan dan kerahasiaan data yang sangat penting dalam lingkungan perusahaan. Untuk menjaga kerahasiaan dan keamanan data, teknik kriptografi seperti Digital Signature Algorithm (DSA) digunakan. DSA merupakan suatu tanda tangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital. Namun, DSA dengan fungsi hash tidak mengenkripsi plainteks asli, sehingga dikombinasikan dengan algoritma RSA untuk meningkatkan keamanan informasi digital

1. Tujuan Penelitian :

Tujuan dari penelitian ini adalah untuk mengembangkan model keamanan informasi berbasis digital signature dengan menggabungkan algoritma Digital Signature Algorithm (DSA) dan RSA. Dengan demikian, diharapkan dapat meningkatkan keamanan dan kerahasiaan data perusahaan serta memberikan mekanisme nirpenyangkalan yang handal

1. Algoritma yang dipakai beserta alur penelitiannya :

Penelitian ini menggunakan algoritma Digital Signature Algorithm (DSA) dengan fungsi hash dan RSA. Algoritma DSA digunakan untuk membuat tanda tangan digital yang dibangkitkan dari hash terhadap pesan, sedangkan algoritma RSA digunakan untuk mengenkripsi message digest yang dihasilkan dari proses hashing MD5.

Alur penelitian dimulai dengan melakukan proses enkripsi pada pesan atau teks yang akan dikirimkan. Plainteks dibagi menjadi dua bagian, yaitu bagian plainteks asli dan bagian plainteks yang diubah menjadi message digest dengan menggunakan hashing MD5. Kemudian, message digest dienkripsi menggunakan algoritma RSA. Setelah itu, cipherteks RSA dikirimkan ke penerima.

Pada sisi penerima, cipherteks RSA didekripsi sehingga menghasilkan message digest yang diperoleh dari hasil hashing MD5. Plainteks asli akan dijadikan message digest dengan MD5 dan akan dicocokkan dengan hasil message digest dari dekripsi RSA. Jika hasilnya sama, maka pesan dianggap asli dan tidak mengalami perubahan.

Dengan menggunakan kombinasi algoritma DSA dan RSA, diharapkan dapat meningkatkan keamanan dan kerahasiaan data perusahaan serta memberikan mekanisme nirpenyangkalan yang handal

1. Hasil penelitian dan kesimpulan :

Hasil penelitian menunjukkan bahwa model keamanan informasi berbasis digital signature dengan menggabungkan algoritma DSA dan RSA dapat meningkatkan keamanan dan kerahasiaan data perusahaan serta memberikan mekanisme nirpenyangkalan yang handal. Proses validasi pesan yang dikirimkan perusahaan menggunakan model algoritma DSA dengan fungsi hash dari proses dekripsi RSA dan fungsi hash dari plainteks, apabila hash tidak sesuai maka file tidak akan bisa diunduh. Waktu yang dibutuhkan dalam proses hash dan enkripsi serta dekripsi beberapa file dengan kapasitas dan ekstensi yang berbeda-beda memiliki rata-rata kurang dari 1 detik, menunjukkan bahwa model algoritma DSA sangat tepat digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan

Kesimpulan dari penelitian ini adalah bahwa penggunaan kombinasi algoritma DSA dan RSA dapat meningkatkan keamanan dan kerahasiaan data perusahaan serta memberikan mekanisme nirpenyangkalan yang handal. Model keamanan informasi berbasis digital signature dengan menggabungkan algoritma DSA dan RSA dapat digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan

1. Kelebihan dan kekurangan :

Kelebihan dari penggunaan kombinasi algoritma DSA dan RSA adalah dapat meningkatkan keamanan dan kerahasiaan data perusahaan serta memberikan mekanisme nirpenyangkalan yang handal. Model keamanan informasi berbasis digital signature dengan menggabungkan algoritma DSA dan RSA juga dapat digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan. Selain itu, waktu yang dibutuhkan dalam proses hash dan enkripsi serta dekripsi beberapa file dengan kapasitas dan ekstensi yang berbeda-beda memiliki rata-rata kurang dari 1 detik, menunjukkan bahwa model algoritma DSA sangat tepat digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan

Namun, kekurangan dari penggunaan kombinasi algoritma DSA dan RSA adalah kompleksitas algoritma yang digunakan. Selain itu, penggunaan algoritma RSA untuk mengenkripsi message digest yang dihasilkan dari proses hashing MD5 juga dapat memperlambat proses enkripsi dan dekripsi. Selain itu, model algoritma lain yang dapat melakukan proses pengiriman dan pengamanan file yang berukuran lebih besar (kapasitas Giga Byte) perlu diteliti untuk pengembangan lebih lanjut

Sumber 1

<https://journal.unnes.ac.id/nju/index.php/sji/article/view/6115/4910>

Sumber 2

<https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/4037/3591>