**TUGAS PRAKTIKUM**

**SISTEM KEAMANAN DATA**

**Resume**



**Disusun Oleh:**

(Andrean L N A) (V3920007)

(Andriyan Tatak W) (V3920008)

(Arin Dwi Padmasari) (V3920010)

( Dandy Dicky T ) (V3920016)

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**

**UNIVERSITAS SEBELAS MARET**

**SURAKARTA**

**2021**

## Jurnal 1

## Judul dan Latar Belakang Masalah

PENERAPAN ALGORITMA RSA UNTUK KEAMANAN PESAN INSTAN PADA PERANGKAT ANDROID> Android adalah suatu sistem yang di gunakan alat komunikasi telepon pintar yang perkembangannya cukup pesat. Android bisa di aplikasikan pada telepon pintar dengan segmen harga yang cukup luas, dari yang murah hingga yang mahal. Hal inilah yang menjadikan Android memiliki pasar yang luas. Pesan instan adalah suatu aplikasi pengirim pesan cepat dengan perantara jarinngan internet yang ada pada perangkat Android. Pesan instan dipilih kerena kecepatan pengiriman data dan murahnya biaya yang digunakan, dalam mengirim sebuah pesan, biaya dihitung berdasarkan besarnya data yang dikirim atau diterima. Karena menggunakan jaringan internet, menjaga kerahasiaan pesan dianggap penting.

* Salah satu cara untuk menjaga kerahasian data adalah menggunakan kriptografi. Prinsip dasar kriptografi adalah proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah plain text (text yang bisa dimengerti) menjadi chipher text (text yang sulit dimengerti), sedangkan dekripsi adalah kebalikan dari enkripsi. Salah satu algoritma kriptografi yang banyak digunakan adalah RSA. Algoritma RSA dibuat oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976. Menggunakan kunci pubik dan kunci privat untuk enkripsi dan dekripsi pesan. Salah satu keunggulan pada algortima RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima.

## Tujuan Penelitian

Peneliti ingin membangun sebuah aplikasi pesan instan pada perangkat Andrtoid yang menginplementasikan algoritma RSA dalam proses enkripsi dan dekripsi pesan teks.

## Algoritma yang dipakai beserta alur penelitiannya

Algoritma RSA digunakan untuk membangkitkan 2 kunci yaitu kunci publik dan kunci privat. Kunci publik adalah dua buah variable bilangan (e,n) yang di gunakan untuk mengenkripsi data. Sedangkan kunci privat adalah dua buah variabel bilangan (d,n) yang di gunakan untuk melakukan dekripsi data. Nilai e, d dan n adalah nilai bilangan bulat positif.

Keamanan algoritma RSA bergantung pada kesulitan memfaktorkan bilangan besar. “We have proposed a method for implementing a publik-key cryptosystem whose security rests in part on the difficulty of factoring large numbers”(R.L. Rivest, A. Shamir, and L. Adleman, 1977). Keamanan kunci privat dan kunci pulik pada algoritma RSA sangat bergantung pada dua variabel p dan q dimana variable ini di gunakan untuk menciptakan kedua kunci tersebut. Berikut adalah proses dimana kunci publik dan kunci privat diciptakan.

a) Tentukan dua nilai p dan q, dimana p dan q adalah bilangan prima contoh : 𝑝 = 3 𝑑𝑎𝑛 𝑞 = 11. b) Hitung nilai n dari hasil p . q, 𝑛 = 𝑝. 𝑞 = (3)(11) = 33 .Maka nilai n = 33.

c) Hitung nilai ∅(𝑛) = (𝑝 − 1)(𝑞 − 1) = (3 − 1)(11 − 1) = (2)(10) = 20.

d) Pilih nilai e dimana 1 < 𝑒 < ∅(𝑛) dan e adalah nilai prima, ditentukan nilai 𝑒 = 7.

) Hitung nilai d dimana (𝑑. 𝑒) 𝑚𝑜𝑑 ∅(𝑛) = 1, salah satu solusinya adalah 𝑑 = 3 perhitungannya ((3)(7)) 𝑚𝑜𝑑 20 = 1.

f) Karena nilai d, e, dan n telah diketahui maka kunci publik adalah (e,n) atau (7, 33) dan kunci privat adalah (d,n) atau (3,33).

g) Proses enkripsi bilangan 𝑚 = 2 => 𝑐 = 2 7 𝑚𝑜𝑑 33 = 29.

h) Proses dekripsi nilai 𝑐 = 29 => 𝑚 = 293 𝑚𝑜𝑑 33 = 2. Karena kunci privat d berisfat rahasia, maka semua element pembentuk nilai d juga harus rahasia, yaitu e dan ∅(𝑛). Namun nilai e bersifat publik yang di gunakan untuk enkripsi, ini menyisakan ∅(𝑛) harus bersifat rahasia maka dari itu bilangan pembentuk n juga harus rahasia (p dan q). Nilai p dan q tidak boleh sama karena jika p dan q sama maka nilai ini dapat ditentukan hanya dengan mencari pemfaktor nilai n yang digunakan untuk enkripsi √𝑛 = 𝑝 = 𝑞.

## Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

Hasil Pengujian :

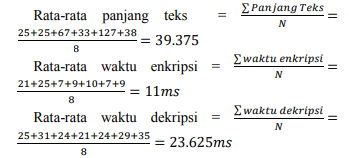
Perbandingan panjang teks dengan, waktu enkripsi serta waktu dekripsi :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| Panjang Teks | 2  5 | 2  5 | 6  7 | 3 | 5  4 | 2  7 | 3  8 | 0 |
| Waktu Enkripsi | 2  1m s | 2  5  ms | 7  ms | m s |  | 0  m s | 7  ms | m s |
| Waktu Enkripsi | 2  5  ms | 3  1  ms | 2  4 ms | 1  m s |  | 4  m s | 2  9  ms | 5  m s |

Rata-rata

Nilai rata-rata dihitung hanya pada sampel yang berhasil dilakukan enkripsi dan dekripsi :

N = 8



Maka akan disimpukan :

Berdasarkan pengujian dan pengolahan data maka dapat disimpulkan:

1. Algoritma RSA adalah algoritma asimetris yaitu algoritma yang mempunyai dua kunci berbeda untuk proses enkripsi dan dekripsi yaitu kunci publik dan kunci privat.

2. Kunci publik di gunakan untuk mendekripsi teks biasa menjadi teks yang terenkripsi atau disebut teks cipher.

3. Kunci privat digunakan untuk mengembalikan teks cipher menjadi teks biasa.

4. Penggunaan algoritma RSA untuk aplikasi pesan instan adalah untuk mengenkripsi pesan sebelum dikirim kepada penerima.

5. Untuk kebutuhan enkripsi, pengirim pesan meminta kunci publik dari penerima yang di distribusikan secara bebas.

6. Pesan yang diterima kemudian di dekripsi menggunkan kunci privat yang hanya dimiliki oleh penerima pesan.

## E. Kelebihan dan kekurangan masing-masing jurnal tersebut

Kekuragan : Dengan jumlah chipertext yang lebih panjang dari plaintext menyebabkan usaha untuk melakukan dekripsi dengan faktorisasi membutuhkan waktu yang lama.

Kelebihan : Salah satu keunggulan pada algortima RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima.

**Jurnal 2**

# A. Judul dan Latar Belakang Masalah

>**Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi *Instant Messaging***

>Kemajuan teknologi komputer dan telekomunikasi membantu dalam menyelesaikan banyak pekerjaan dengan cepat, akurat, dan efisien. Salah satu kemajuan teknologi komunikasi yaitu menghasilkan aplikasi instant messaging atau pesan instan. Instant messaging merupakan fasilitas komunikasi chatting untuk para pengguna internet sehingga user dapat berkomunikasi dengan cara mengirimkan pesan berupa teks dengan user lain [1]. Namun seiring dengan kemajuan teknologi, dengan semakin banyaknya pengguna yang menggunakan aplikasi instant messaging terdapat dampak negatif berupa penyadapan data khususnya saat terjadi komunikasi yang bersifat rahasia dan penting sehingga 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 [2]. Kriptografi bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau internet, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan.

RSA merupakan algoritma kriptografi kunci publik atau sering disebut kunci asimetrik (kunci enkripsi dan kunci dekripsi berbeda) sehingga tidak membutuhkan saluran yang aman untuk distribusi kunci. RSA ditemukan oleh tiga peneliti dari MIT (Massachussets Institute of Technology), yaitu Ronald Linn Rivest, Adi Shamir, dan Len Adleman pada tahun 1977 [3]. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

CRT (Chinese Remainder Theorem) merupakan suatu algoritma untuk mengurangi perhitungan aritmatika modular dengan modulus besar untuk perhitungan yang sama untuk masing-masing faktor dari modulus [4]. CRT dapat memperpendek ukuran bit eksponen dekripsi d (merupakan kunci publik RSA atau RSA-CRT) dengan cara menyembunyikan d pada sistem kongruen sehingga mempercepat waktu dekripsi serta dapat digunakan bersama algoritma RSA yang disebut RSA-CRT.

Untuk meningkatkan keamanan dari segi pengiriman pesan yang dibuat dalam saluran yang tidak aman serta modifikasi algoritma RSA dengan menggunakan teorema CRT agar dapat dibandingkan dengan algoritma RSA, perlu dibangun sebuah aplikasi instant messaging dengan mengimplementasikan algoritma kriptografi RSA-CRT.

# B. Tujuan Penelitian

Untuk meningkatkan keamanan dari segi pengiriman pesan yang dibuat dalam saluran yang tidak aman serta modifikasi algoritma RSA dengan menggunakan teorema CRT agar dapat dibandingkan dengan algoritma RSA, perlu dibangun sebuah aplikasi instant messaging dengan mengimplementasikan algoritma kriptografi RSA-CRT.

# C. Algoritma yang dipakai beserta alur penelitiannya

C. Algoritma RSA dan CRT (RSA-CRT)

Sistem kriptografi RSA dapat dimodifikasi dengan menggunakan teorema CRT disebut dengan RSA-CRT. Terbukti sistem kriptografi RSA-CRT memiliki waktu komputasi yang lebih singkat daripada sistem kriptografi RSA biasa, yaitu sekitar 4 kali lebih cepat [8].

Algoritma RSA-CRT dibagi menjadi 3 langkah:

1. Pembangkit Kunci RSA-CRT

Pada dasarnya RSA-CRT sama dengan RSA biasa tetapi memanfaatkan teorema CRT untuk memperpendek ukuran bit eksponen deksipsi d dengan cara menyembunyikan d pada sistem kongruen sehingga mempercepat waktu dekripsi. Berikut algoritma pembangkit kunci RSA-CRT:

a. Bangkitkan bilangan prima besar p dan q

b. Lihat rumus (1).

c. Lihat rumus (2).

d. Lihat rumus (3).

e. Lihat rumus (4).

f. dP = d mod (p – 1) (9)

g. dQ = d mod (q – 1) (10)

h. qInv = q-1 pada Zp (11)

i. Kpublik = (e, n), Kprivat = (dP, dQ, qInv, p, q) (12)

2. Enkripsi RSA-CRT

Kunci publik RSA-CRT sama dengan sistem RSA yaitu (e, n) sehingga algoritma enkripsi tidak mengalami perubahan yaitu dengan menggunakan fungsi eksponensial modular yaitu lihat pada rumus (5).

3. Dekripsi RSA-CRT

Diberikan teks sandi seperti rumus (5) dan kunci privat (dP, dQ, qInv, p, q) dekripsi RSA-CRT seperti berikut:

a. m1 = CdP mod p (13)

b. m2 = CdQ mod q (14)

c. h = qInv.(m1 – m2) mod p (15)

d. M = m2 + h.q (16)

# D. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

Implementasi algoritma kriptografi kunci publik dengan algoritma RSA-CRT pada aplikasi *instant messaging*, proses dekripsi menggunakan algoritma RSA-CRT untuk 1.800 karakter dengan bit n dari 56 bit sampai 88 bit memiliki kecapatan rata-rata dua kali lebih cepat dibandingkan menggunakan algoritma RSA. Semakin besar panjang *string,* nilai n kemungkinan besar semakin cepat waktu dekripsi menggunakan RSA-CRT.

# E. Kelebihan dan kekurangan masing-masing jurnal tersebut

>Kelebihan

Menjadi lebih aman karena algoritmanya menjadi lebih rumit

>Kekurangan

Karena algoritma menjadi lebih rumit maka akan lebih sulit juga untuk membuat programnya