LAPORAN PRAKTIKUM SISTEM KEAMANAN DATA



**Disusun Oleh :**

Ricky Suparman Saragih V3920051

Ridho Walidhayin Rifai V3920052

Rosa Auralia Adhani S V3920055

Zulfikar Ahmadi Rafsanjani V3920066

TI-E

TEKNIK INFORMATIKA – PSDKU

SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET

2021/2022

# JURNAL 1

IMPLEMENTASI KRIPTOGRAFI KUNCI PUBLIK DENGAN ALGORITMA RSA-CRT PADA APLIKASI INSTANT MESSAGING

## Latar Belakang Masalah

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. 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. 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. 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. 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.

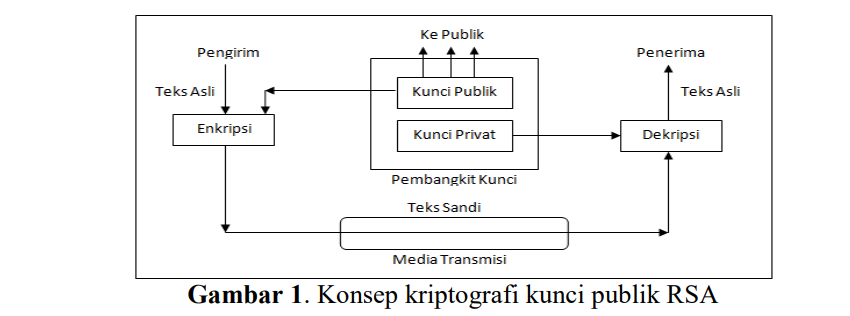
## Tujuan Penelitian

Tujuannya yaitu mengimplementasi algoritma kriptografi RSA-CRT pada aplikasi instant messaging pada panjang bit n mulai dari 56 bit sampai 88 bit, proses dekripsi RSA-CRT dua kali lebih cepat dibandingkan proses dekripsi RSA.

## Algoritma yang dipakai dan alur penelitiannya

### Kriptografi Kunci Public RSA

Algoritma RSA menggunakan 2 angka (e dan d) sebagai kunci publik dan kunci privat. Pada algoritma RSA e dan n diumumkan untuk umum sedangkan d dirahasiakan. Meskipun RSA dapat digunakan untuk mengenkripsi dan mendekripsi pesan, sangat lambat jika pesan tersebut panjang. Oleh karena itu, algoritma RSA berguna untuk pesan singkat. Sejak algoritma menggunakan 2 kunci untuk enkripsi dan dekripsi, algoritma RSA dianggap sebagai contoh kunci asimetrik kriptografi. Desain konseptual dari algoritma RSA dapat disajikan pada Gambar 1.



### CRT (Chinese Remainder Theorem)

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. Keuntungan dasar dengan menggunakan Chinese Remainder Theorem adalah memungkinkan untuk membagi modulo eksponensial yang besar ke dalam dua eksponensial yang jauh lebih kecil, satu di atas p dan satu di atas q. Dua modulo ini adalah faktor utama dari n yang dikenali.

### Algoritma RSA dan CRT dibagi menjadi 3 langkah :

#### Pembangkit Kunci RSA-CRT

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:

* Pilih 2 bilangan prima besar untuk nilai p dan q
* Hitung nilai modulus n = p x q
* Hitung menggunakan fungsi Euler
* Pilih nilai Integer *e* acak sebagai kunci public, dengan syarat memenuhi Greater Common Divisor (GCD)
* Hitung kunci privat d sehingga
* dP =
* dQ =
* qlnv =

#### Enkripsi RSA-CRT

Kunci public RSA-CRT sama dengan RSA yaitu (e, n) sehingga algoritma enkripsi tidak mengalami perubahan yaitu dengan menggunakan fungsi eksponensial modular yaitu Enkripsi 🡪

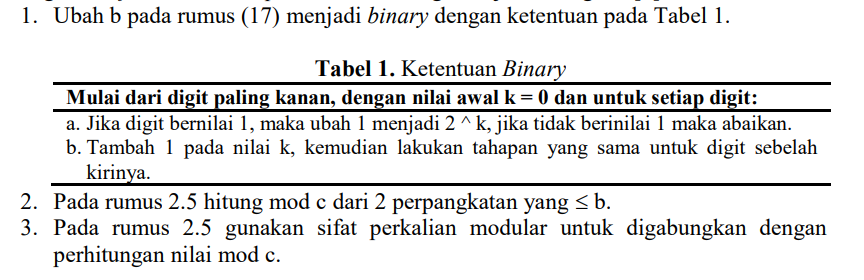
#### Deskripsi RSA-CRT

Diberikan teks sandi seperti rumus enkripsi dan kunci privat (dP, dQ, qlnv, p, v) deskripsi RSA-CRT seperti berikut :

M =

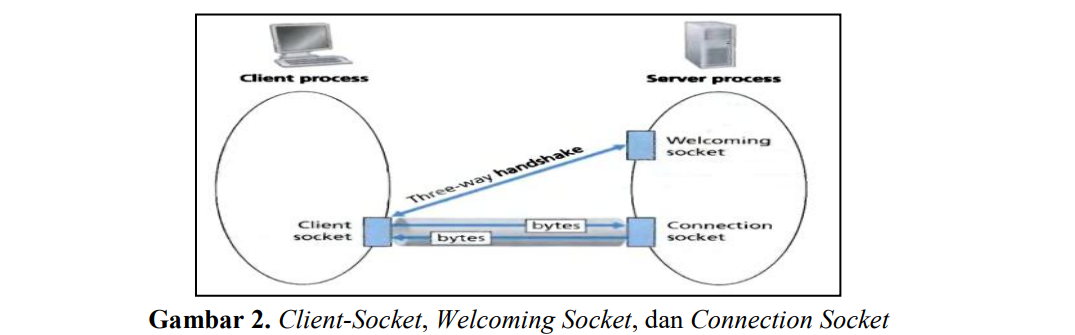
### Algoritma Fast Modular Exponentiation

Algoritma fast modular exponentiation merupakan algoritma untuk menghitung suatu modular exponentiation dengan cepat. Rumus modular exponentiation 🡪 ab mod c. dibagi menjadi 3 langkah yaitu :

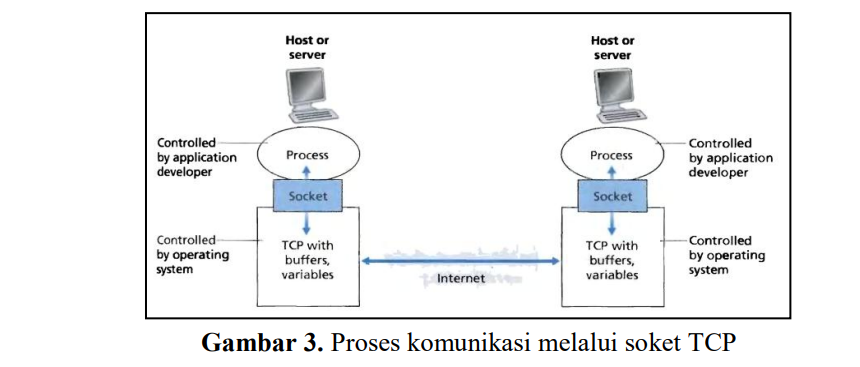


### Pemrogaman Soket dengan TCP (Transmission Control Protocol)

Aplikasi jaringan banyak terdiri dari sepasang program-program klien dan server program yang berada di dua sistem akhir yang berbeda. Ketika kedua program dijalankan, klien dan proses server dibuat, dan proses ini berkomunikasi satu sama lain dengan membaca dari dan menulis ke soket. Karena soket memainkan peran sentral dalam klien/server mengembangkan aplikasi klien/server juga disebut sebagai pemrograman soket, dapat dilihat pada Gambar 2.



Pemrograman soket dengan TCP adalah pemrograman soket yang berorientasi koneksi dan menyediakan reliable (handal) byte-stream yang menjamin bahwa proses server akan menerima (melalui koneksi soket) setiap byte dalam urutan yang dikirim. Selain itu proses klien tidak hanya mengirimkan byte tetapi juga menerima byte dari koneksi soket. Untuk proses komunikasi melalui soket TCP dapat dilihat pada Gambar 3.



## Hasil Penelitian

### Mengolah Server dan Client

Aplikasi instant messaging menggunakan algoritma kriptografi RSA-CRT dengan pemrogaman soket berbasis TCP, sehingga dibuatnya class TCPListener dengan port 8888 dan class TCPClient untuk server.

### Mengolah Kunci

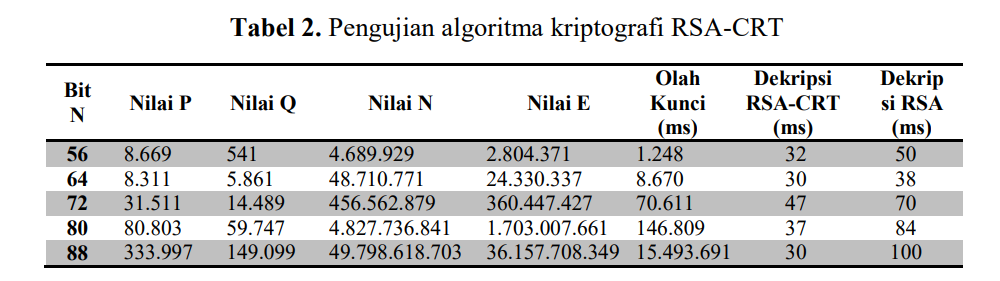
Pada alur mengolah kunci membangkitkan kunci satu dengan nilai P dan Q, sedangkan kunci dua menggunakan kunci acak lalu server akan menerima dua kunci public dari pengguna. Maka akan ditampilkan kunci satu dan dua dari pengolahan kunci selama beberapa milidetik. Kunci public satu digunakan untuk proses enkripsi ketika kunci dua mengirim pesan, dan begitu sebaliknya.

### Mengolah Pesan

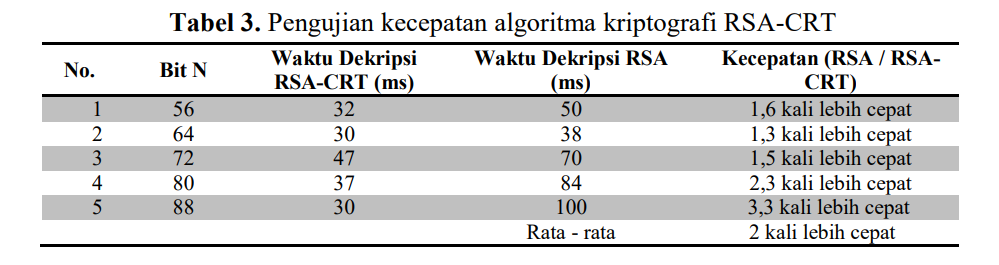
Pada proses olah pesan, kunci dua akan mengirim password dengan menggunakan kunci public satu kemudian akan disebarkan ke server kunci satu.

### Pengujian

Pengujian algoritma kriptografi RSA-CRT pada aplikasi instant messaging yang utama adalah membandingkan kecepatan dekripsi antara algoritma kriptografi RSA dengan algoritma kriptografi RSA-CRT. Waktu yang digunakan untuk melakukan proses dekripsi sebagai perbandingan antar kedua algoritma kriptografi.Pengujian dilakukan dengan menggunakan 1800 karakter dummy, jumlah bit n yangdigunakan mulai dari 56 bit sampai 88 bit, dikarenakan pesan yang digunakan untuk melakukan pengujian yaitu 1.800 karakter sehingga mempunyai syarat nilai n harus lebih besar atau sama dengan 1.000.000. Hasil pengujian dapat dilihat pada Tabel 2.



Berdasarkan hasil pengujian algoritma kriptografi RSA-CRT yang dapat dilihat pada Tabel 2 dapat diberi kesimpulan dengan rata-rata kecepatan yang dapat dilihat pada Tabel 3.



Dari pengujian kecepatan algoritma kriptografi RSA-CRT yang dapat dilihat pada Tabel 3, dapat diberi kesimpulan semakin besar jumlah bit n maka kemungkinan besar kecepatan waktu dekripsi RSA-CRT lebih cepat dan dari 5 pengujian yang dilakukan mulai bit n = 56 bit sampai bit n = 88 bit dapat disimpulkan kecepatan yang diperolah rata-rata yaitu dua kali lebih cepat ketika menggunakan dekripsi RSA-CRT dibandingkan menggunakan dekripsi RSA.

## Kesimpulan

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.

## Kelebihan dan Kekurangan

Pada penelitian ini sudah menjelaskan hampir secara rinci tentang RSA dan cara penggunaan rumus RSA sendiri, akan tetapi terdapat kekurangan pada penelitian ini yaitu kurangnya penjelasan pengerjaan alur progam RSA sendiri sehingga akan sedikit membingungkan orang-orang yang ingin implementasi jurnal ini.

# JURNAL 2

MODEL KEAMANAN INFORMASI BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA RSA

## Latar Belakang Masalah

Salah satu algoritma kriptografi untuk keamanan informasi adalah algoritma digital signature (DSA). DSA atau Digital Signature Algorithm merupakan salah satu algoritma kriptografi kunci publik yang paling banyak digunakan saat ini. Penerapan tanda tangan digital antara lain: sertifikat digital untuk keamanan e-commerce, untuk penandatanganan kontrak yang sah dan untuk mengamankan pembaruan perangkat lunak (Mollin, 2007).

DSA merupakan suatu tanda tangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim dari suatu pesan atau penandatangan dari suatu dokumen digital. Tanda tangan digital ini memastikan isi pesan atau dokumen digital yang dikirim tidak mengalami perubahan sampai ke tangan penerima. Dengan demikian penerima yakin bahwa pesan yang diterimanya benar-benar asli dari pihak pengirim. Selain kriptografi DSA juga membutuhkan fungsi hash, fungsi hash merupakan fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (fixed), umumnya berukuran jauh lebih kecil daripada ukuran string semula, hasil konversi pesan tersebut akan disamakan dengan hasil dekripsi dari proses kriptografi DSA untuk otentikasi dan integritas dari keaslian pesan.

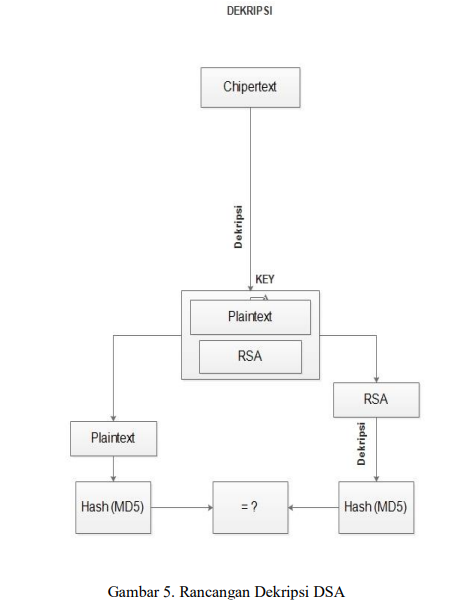
DSA banyak diaplikasikan untuk keamanan informasi berupa file digital, hal tersebut dilakukan untuk mencegah pemalsuan pengiriman suatu file atau pesan digital. Teknologi informasi yang semakin berkembang saat ini menuntut perusahaan untuk dapat menjaga keamanan dan kerahasiaan data perusahaan termasuk harus melakukan otentikasi pengirim dan kepercayaan pada file atau pesan digital yang akan dikirimkan.

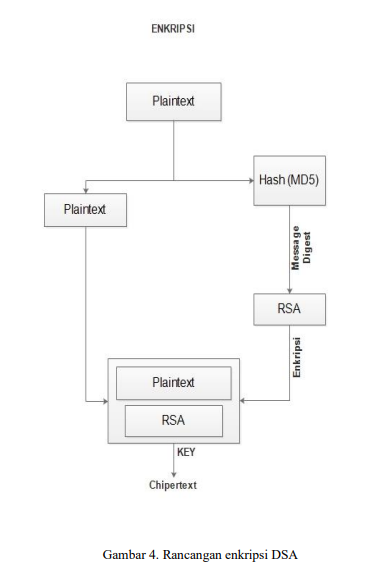
## Tujuan Penelitian

Tujuannya yaitu membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital, namun DSA dengan fungsi hash tidak mengenkripsi plainteks asli sehingga, dikombinasikan dengan RSA.

## Algoritma yang dipakai beserta alur penelitiannya

Teknik pengembangan pada penelitian ini adalah teknik pengamanan digital signature algorithm (DSA) dengan penambahan algoritma dan RSA. Adapun skema alur pengembangan teknik algortima Digital Signature dapat di lihat pada gambar dibawah ini:





Untuk memudahkan dalam hal pembahasan, gambar diatas dapat dibagi menjadi beberapa bagian, diantaranya adalah:

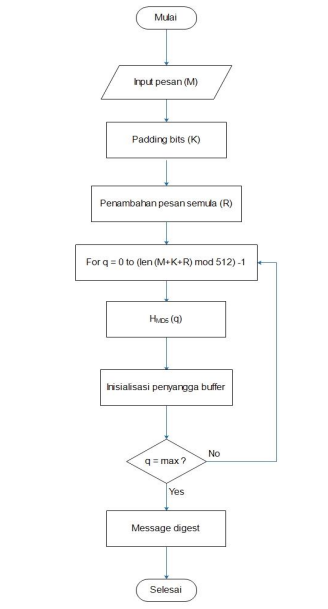
Proses enkripsi

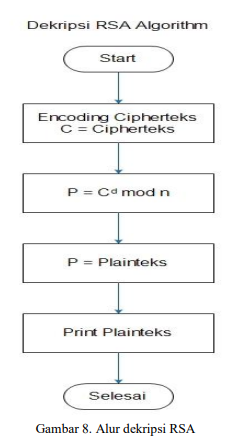
* Plainteks yang di bagi menjadi 2 bagian yaitu bagian plainteks asli dan bagian plainteks yang diubah menjadi message digest dengan menggunakan hashing MD5.
* Proses enkripsi message digest dengan menggunakan RSA.

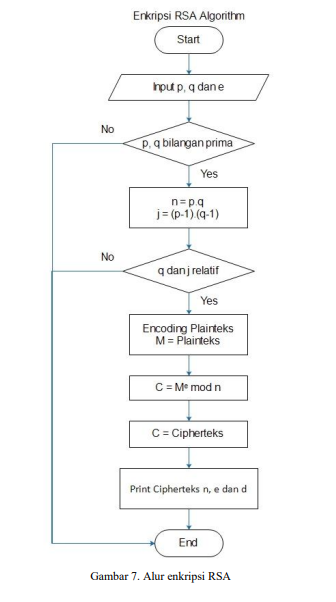
Proses dekripsi

* Cipherteks RSA didekripsikan sehingga menghasilkan message digest yang diperoleh dari hasil hashing MD5.
* Plainteks asli akan di jadikan message digest dengan MD5 dan akan dicocokkan dengan hasil message digest dari dekripsi RSA.

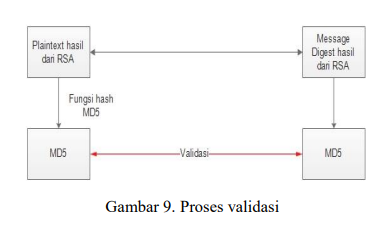
Fungsi merubah MD5



Alur enkripsi dan deskripsi RSA algoritma



Proses Validasi



Jika hasil ternyata cocok (sama) maka file/pesan terbukti keasliannya dan file dapat diunduh, namun jika terjadi ketidak cocokan, maka file/pesan tersebut sudah tidak asli dan file tidak dapat diunduh.

## Hasil Penelitian

Penelitian ini merupakan model dari digital signature algorithm dengan fungsi hash, yang mana ditambahkan kombinasi dari algortma RSA. Algoritma digital signature dengan fungsi hash yaitu tanda tangan digital yang dibangkitkan dari hash terhadap pesan. Nilai hash adalah kode ringkas dari pesan. Tanda tangan digital berlaku sepertu tanda tangan pada dokumen kertas. DSA model ini memiliki fungsi nir-penyangkalan, namun memiliki kelemahan dari sisi plainteks, algoritma DSA dengan fungsi hash akan tetap menampilkan plainteks yang dikirim tersebut , sehingga apabila teks tersebut dikirim ke penerima tetap akan menampilkan plainteks yang memungkinkan orang lain dapat melihatnya namun jika plainteks tersebut dirubah maka si penerima akan tau bahwa pesan tidak asli (nir-penyangkalan). Algoritma RSA merupakan sebuah algoritma simetris, dimana tingkat keamanannya tergantung dari perpangkatan bilangan prima yang menjadi kuncinya, algoritma RSA ini akan melakukan proses enkripsi pada hashing MD5 sehingga message digest terjaga dan terenkripsi, hal ini dilakukan untuk kemanan disisi MD5 yang akan dikirim bersamaan dengan plainteks.

## Kesimpulan

Berdasarkan pembahasan dan evaluasi, maka dapat ditarik kesimpulan sebagai berikut:

1. Model algoritma Digital Signature Algorithm (DSA) yang digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan sebagai nirpenyangkalan membutuhkan algoritma kriptografi RSA untuk menjaga keamanan dan kerahasiaan file dan pesan.
2. 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.
3. 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 Digital Signature Algorithm (DSA) sangat tepat digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan.

## Kelebihan dan Kekurangan

Pada jurnal dua ini lebih mengutamakan fungsi DSA nya saja sedangkan RSA hanya untuk fungsi penambahan, dan untuk penjelasannya juga kurang jelas.