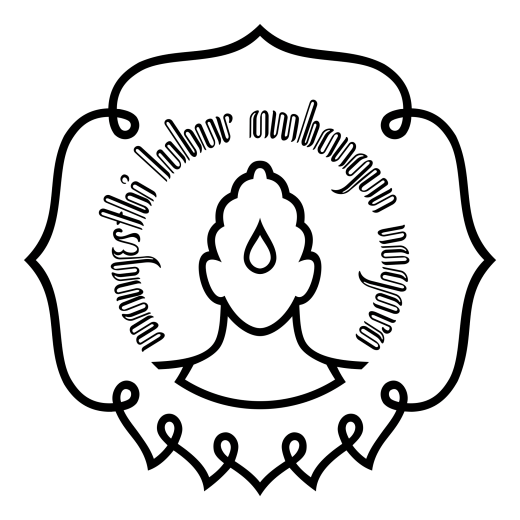
**ALGORITMA RSA**



**Disusun Oleh:**

Agnar Briantama R V3920003

Bancar Anggono F V3920013

Catur Edi Prasetyo V3920014

Dwi Ayuni Rohana V3920019

Intan Naumi V3920028

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**2021**

**ANALISIS DAN IMPLEMENTASI ALGORITMA ASIMETRIS DUAL MODULUS RSA (DM-RSA) PADA APLIKASI CHAT**

1. **LATAR BELAKANG**

Algoritme RSA merupakan salah satu algoritme kriptografi asimetris yang memiliki sepasang kunci di mana prosesnya didasarkan atas model pemfaktoran dengan membangkitkan bilangan prima. Jadi, untuk memecahkan kunci di dalam algoritma RSA harus mengetahui faktor dari perkalian di dalam bilangan prima. Keamanan pada algoritme RSA terletak pada bilangan prima yang dibangkitkan pada proses pembangkitan kunci. Bilangan prima yang dibangkitkan diharapkan memiliki nilai yang besar sehingga algoritme tidak mudah ditembus. Sebaliknya apabila bilangan prima yang digunakan kecil maka semakin kecil pula keamanan dan mengakibatkan algoritme ini condong untuk mudah ditembus. Algoritme RSA memiliki keamanan yang sulit ditembus apabila menggunakan bilangan prima yang besar, tetapi apabila kecil keamanan algoritme tersebut juga menjadi semakin kecil dan rentan. Algoritme DM-RSA memiliki empat buah bilangan prima dan apabila bilangan prima yang digunakan kecil tidak mempengaruhi karena menggunakan 4 buah bilangan prima sekaligus yang artinya 2 kali lipat dari RSA. Diharapkan algoritme yang akan dibahas mampu memiliki ketahanan yang lebih kuat jika dibandingkan dengan algoritme RSA, dikarenakan jika ada attacker yang mendapatkan 1 kunci pribadi tidak akan bisa untuk mendapatkan hasil dekripsi (pesan asli) karena masih ada 1 buah kunci pasangan untuk dekripsi pesan tersebut. Maka dari itu, beberapa kajian keilmuan yang membahas tentang modifikasi algoritme RSA.

1. **TUJUAN PENELITIAN**

Mengimplementasikan RSA dan DM-RSA dalam aplikasi chatting dengan Memodifikasi algoritme RSA pada pembangkitan kunci dengan menggunakan banyaknya bilangan prima.

1. **ALGORITMA YANG DIPAKAI BESERTA ALUR PENELITIAN**

Menggunakan Algoritme kriptografi Dual Modulus RSA atau yang disebut dengan DM-RSA. Algoritme ini disebut Dual Modulus karena memiliki 2 buah modulus yang digunakan untuk proses pembangkitan kunci, proses enkripsi dan proses dekripsi, sehingga algoritma ini memiliki 4 buah bilangan prima 𝑝1, 𝑝2, 𝑞1, 𝑞2. Teknik semacam ini diharapkan dapat meningkatkan keamanan algoritme RSA dikarenakan menggunakan dual modulus atau 2 buah modulus dan dalam proses enkripsi dan dekripsi menggunakan kunci dobel (2 kunci publik dan 2 kunci pribadi). Alur penelitian tersebut yang pertama membuat arsitektur aplikasi chatting, kedua membuat rancangan algoritme RSA, dan terakhir membuat rancangan algoritme DM-RSA

1. **CERITAKAN HASIL PENELITIAN PADA JURNAL TERSEBUT DAN KESIMPULAN**

Tahap pertama yang dilakukan peneliti adalah dengan melakukan perbandingan pengujian waktu pembangkitan kunci RSA dan DM-RSA, dimana hasil analisa yang dapat diperoleh diantaranya adalah panjang bit 8 dan 16 pada algoritme RSA dan DM-RSA tidak terlalu berbeda pada proses pembangkitan kunci, yaitu rata rata dari bit 8 dan 16 memiliki nilai yang hampir sama atau memiliki selisih sedikit tidak naik atau turun secara drastis tetapi selalu mengalami kenaikan. Lalu Panjang bit 24 dan 32 pada algoritme RSA terbukti lebih cepat dalam proses pembangkitan kunci, algoritme Dual Modulus RSA lebih lambat hal ini terjadi karena pada proses pembangkitan kunci pada algoritme DM-RSA membangkitkan 4 buah bilangan prima (𝑝1, 𝑝2, 𝑞1, 𝑞1) sedangkan RSA 2 buah bilangan prima (𝑝 dan 𝑞). Kemudian tahap kedua melakukan perbandingan pengujian waktu proses enkripsi RSA dan DM-RSA dimana didapat hasil kecepatan algoritma RSA lebih cepat disbanding DM-RSA. Lalu tahap ketiga dilakukan perbandingan pengujian waktu deskripsi RSAA dan DM-RSA dan didapa hasil Algoritme RSA terbukti lebih cepat terlihat bahwa algoritme RSA memiliki waktu lebih cepat hingga 50% atau bahkan 2 kali lipat dari algoritme DM-RSA. Dan yang terakir Pengujian metode Keamanan Menggunakan Pengujian Faktorisasi Kraitchik lalu didapat hasil Algoritme DM-RSA terbukti lebih tahan dibandingkan algoritme RSA dalam serangan ini. Algoritme Dual Modulus RSA ini terbukti lebih tahan hingga 2 kali lipat bahkan lebih dibandingkan algoritme RSA

Dari hasil pengujian yang telah dilakukan dapat diambil kesimpulan diantaranya adalah berkaitan dengan kecepatan pemrosesan algoritme RSA maupun DM-RSA sangat dipengaruhi oleh jumlah bit dan jumlah karakter yang diinputkan. Kemudian dari pengujian ketahanan algoritme dengan menggunakan metode faktorisasi kraitchik bahwa algoritme DM-RSA terbukti memiliki ketahanan yang lebih baik dibandingkan algoritme RSA karena algoritme DM-RSA memiliki waktu yang lebih lama hingga dua kali jika dibandingkan algoritme RSA standar seperti yang telah disajikan pada Tabel 7. Hal ini disebabkan karena modulus yang digunakan pada algoritme DM-RSA memiliki 2 modulus yang memberikan efek lebih tahan terhadap serangan faktorisasi.

1. **KELEBIHAN DAN KEKURANGAN MASING MASING JURNAL**

Kelebihannya adalah memaparkan secara jelas dan lengkap mulai dari pendahuluan atau latar belakang dari permasalahan, penulisan jurnal teratur dan sesuai dengan kaidah pembuatan penulisan jurnal. Kekurangannya adalah space penulisan yang kurang teratur.

**PERANCANGAN APLIKASI PENGAMANAN FILE TEKS DENGAN SKEMA**

**HYBRID MENGGUNAKAN ALGORITMA ENIGMA DAN ALGORITMA RSA**

1. **LATAR BELAKANG**

Pengiriman atau pertukaran data adalah hal yang sering terjadi dalam dunia teknologi informasi. Data yang dikirim kadang sering berisi data informasi yang penting bahkan sangat rahasia dan harus dijaga keamanannya. Apalagi pengiriman data dilakukan melalui layanan komunikasi dunia maya, ancaman kejahatan sangat banyak terjadi didalamnya. Dengan adanya ancaman kejahatan seperti interception (penyadapan), Salah satunya adalah kriptografi dimana pesan disamarkan menjadi pesan tersandi. Dalam proses penyandian, penyandian yang digunakan adalah Enigma dan RSA (Rivest Shamir Adleman) .

1. **TUJUAN PENELITIAN**

Menerapkan perancangan aplikasi pengamanan file teks dengan skema hybrid menggunakan algoritma enigma dan algoritma RSA

1. **ALGORITMA YANG DIPAKAI BESERTA ALUR PENELITIAN**

Menggunakan algoritma enigma dan algoritma RSA, Dimana Enigma sebagai algoritma simetris yang mengamankan suatu pesan asli (plaintext) menjadi pesan tersandi (chipertext). Selanjutnya key pada enigma akan digunakan untuk enkripsi chiperkey dengan menggunakan algoritma RSA, RSA sebagai algoritma Asimetris yang mengamankan suatu kunci. Sehingga pesan atau file teks yang dikirim tidak memiliki arti apapun bagi siapapun termasuk operator, jika tidak memiliki kunci pembuka dari pesan tersebut, jadi pesan atau file teks dapat dijaga kerahasiannya.

1. **CERITAKAN HASIL PENELITIAN PADA JURNAL TERSEBUT DAN KESIMPULAN**

Tahap pertama yang dilakukan peneliti adalah menerapkan algoritma pada aplikasi dengan menggunakan 3 komponen utama yang nanti akan berperan dalam enkripsi / deskripsi pada enigma tersebut yakni keyboard,rotor, dan reflector. Kemudian peneliti melakukan perhitungan manual menggunakan algoritma enigma tersebut. Kemudian peneliti melakukan penerapan pada aplikasi menggunakan algoritma RSA dan melakukan perhitungan manual menggunakan algoritma RSA. Selanjutnya dari perhitungan yang sudah dilakukan peneliti menggunakan 2 algoritma tersebut, didapatkan tampilan form menu utama,tampilan form bangkit kunci, tampilan form enkripsi, tampilan form setting rotor, tampilan form deskripsi, tampilan form tentang, dan tampilan form bantuan.

Kesimpulan yang didapat peneliti adalah Sistem pada aplikasi yang mudah dimengerti karena memiliki tampilan yang menarik dan sederhana, dengan menggunakan algoritma enigma dan algoritma RSA yang merupakan salah satu algoritma yang sulit dipecahkan, pada pembuatan aplikasi menggunakan algoritma enigma yang berfungsi untuk mengamankan informasi pesan yang akan di enkripsi lalu sedangkan algoritma RSA berfungsi untuk mengamankan kunci dari pesan yang telah di enkripsi, dari penelitian ini mempermudah pengguna dalam memilih rotor enigma yang akan digunakan.

1. **KELEBIHAN DAN KEKURANGAN MASING MASING JURNAL**

Kelebihannya adalah materi yang disajikan cukup lengkap dan mendetail, penulisan isi jurnal sudah benar namun hanya kurang rapi pada penulisannya.