**PENERAPAN SISTEM KRIPTOGRAFI HYBRID MENGGUNAKAN ALGORITMA RIVEST SHAMIR ADLEMAN DAN ADVANCED ENCRYPTION SYSTEM**

**SKRIPSI**

Diajukan untuk memenuhi salah satu persyaratan

kelulusan program Sarjana Strata Satu (S1)

Disusun oleh

**Afif Farakhan**

**NRP. 161014039**



**SEKOLAH TINGGI MANAJEMEN INFORMATIKA**

**D A N I L M U K O M P U T E R L P K I A**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**BANDUNG**

**2020**

# BAB I

# PENDAHULUAN

## Latar Belakang

Keamanan suatu pesan ataupun informasi merupakan hal yang sangat penting terlebih jika informasi tersebut merupakan informasi yang tidak boleh dilihat atau diakses oleh sembarang orang melainkan hanya boleh dilihat oleh orang-orang yang berhak mengakses nya saja.

Cara berkomunikasi di zaman sekarang semakin mengalami peningkatan dan perkembangan. Seiring semakin berkembangnya teknologi, banyak aspek di kehidupan kita yang terkena dampaknya termasuk dalam bertukar informasi.

Seiring meningkatnya perkembangan teknologi khususnya dalam berkomunikasi, orang-orang semakin sering bertukar pesan atau informasi melalui komunikasi secara digital. Namun bertukar informasi melalui cara digital pun tidak luput dari yang namanya masalah celah keamanan yang mungkin dimanfaatkan oleh orang-orang yang tidak bertanggung jawab.

Kriptografi merupakan ilmu yang digunakan untuk mengamankan kerahasiaan suatu pesan. Di zaman modern ini ilmu kriptografi sering sekali digunakan dan diimplementasikan ke dalam teknologi. Kriptografi pun terbagi ke dalam 2 jenis yaitu kriptografi simetris dan kriptografi asimetris.

Namun dari kedua jenis kriptografi ini pun masing-masing memiliki karakteristik, kelebihan dan kelemahan nya masing-masing. Seperti kriptografi simetris, karena memiliki kunci yang lebih kecil maka proses enkripsi dan dekripsi nya pun lebih cepat dan secara teori kriptografi ini kuat bila kunci nya aman di kedua belah pihak.

Namun masalah yang ada di kunci kriptografi ini yaitu kunci yang digunakan untuk menenkrip dan mendekrip merupakan kunci yang sama. Artinya bila ada pihak ketiga yang mengetahui kunci tersebut dengan cara penyerangan seperti MITM ataupun Snooping maka pihak tersebut pun dapat melakukan enkrpsi dan dekrpsi sama seperti pihak ke 1 dan ke 2 tersebut.

Lalu untuk kriptografi asimetris tidak perlu mengkhawatirkan soal pertukaran kunci dikarenakan terdapat 2 kunci yang digunakan yaitu kunci publik dan privat yang mana salah satu kunci digunakan untuk menenkrip pesan dan satu lagi digunakan untuk mendekrip pesan. Namun karena kunci yang digunakan lebih besar sehingga proses enkrip dekrip pun lebih lambat.

Bila hanya memanfaatkan salah satu sistem kriptografi saja maka mau tidak mau kita mendapatkan baik itu kelebihan maupun kekurangan sistem kriptografi tersebut. Maka digunakanlah sistem kriptografi hybrid yaitu dengan menggabungkan sistem kriptografi simetris dan asimetris sehingga menghasilkan kriptografi yang memiliki kelebihan-kelebihan dari kedua sistem kriptografi tersebut namun menambal kelemahan-kelemahan sistem kriptografi tersebut.

## Identifikasi Permasalahan

Berdasarkan latar belakang masalah yang telah tertulis diatas, maka berikut adalah identifikasi masalah yang akan dijadikan bahan penelitian yaitu:

1. Bagaimana mengatasi kelemahan Sistem Kriptografi Simetris dan Sistem Kriptografi Asimetris dengan penggunaan Sistem Kriptografi Hybrid.
2. Bagaimana proses Sistem Kriptografi Hybrid dengan menggunakan Sistem Kriptografi Rivest Shamir Adleman (RSA) dan Sistem Kriptografi Advanced Encryption System (AES).
3. Bagaimana proses pembangkitan kunci publik dan privat pada Sistem Kriptografi Rivest Shamir Adleman (RSA).
4. Bagaimana proses pembangkitan kunci pada Sistem Krptografi Advanced Encryption System (AES).

## Lingkup dan Batasan

Adapun ruang lingkup permasalahan dari penelitian ini yaitu:

1. Pesan yang akan dienkrip dan didekrip hanyalah pesan teks.
2. Karakter yang digunakan untuk enkrip dan dekrip hanya karakter ASCII.
3. Bilangan prima yang digunakan untuk Pembangkit kunci Sistem Kriptografi Rivest Shamir Adleman (RSA) minimal 257 dan maksimal 997.

## Tujuan Penelitian

Adapun tujuan dari penelitian ini yaitu:

1. Mengetahui proses pembangkitan kunci publik dan kunci privat pada Sistem Kriptografi Rivest Shamir Adleman (RSA).
2. Mengetahui proses pembangkitan kunci pada Sistem Kriptografi Advanced Encryption System (AES).
3. Mengetahui proses enkripsi dan dekripsi pada Sistem Kriptografi Rivest Shamir Adleman (RSA).
4. Mengetahui proses enkripsi dan dekripsi pada Sistem Kriptografi Advanced Encryption System (AES).
5. Mengetahui proses Kriptografi Hybrid menggunakan Sistem Kriptografi Simetris AES dan Sistem Kriptografi Asimetris RSA.
6. **Metodologi Penelitian**
7. Metodologi Penelitian

Dalam menyelesaikan masalah, penulis melakukan metode penelitian sebagai berikut :

1. Studi Literatur

Studi literatur adalah pencarian terhadap sumber tertulis yang sudah tersedia dan terverifikasi baik dari buku, arsip, artikel maupun jurnal yang relevan dengan permasalahan yang dibahas. Sehingga informasi yang didapat valid dan hasil dari skripsi ini dapat memperkual argumen – argument yang sudah ada.

1. Konsultasi

Konsultasi dilakukan untuk mengumpulkan saran-saran yang didapat dari beberapa pihak, seperti Dosen, Pebimbing dan Rekanan yang memahami tentang permasalahan yang diangkat.

1. Metode Pengumpulan Data
2. Observasi

Observasi merupakan salah satu metode pengumpulan data yang dilakukan dengan cara pengamatan sekaligus pencatatan secara urut yang terdiri dari unsur-unsur yang bermunculan dalam suatu fenomena-fenomena dalam objek penelitian. Hasil dari pengamatan akan dilaporkan dengan susunan yang sistematis dan sesuai kaidah yang berlaku.

1. Wawancara

Wawancara merupakah salah satu metode pengumpulan data yang dilakukan dengan melakukan suatu percakapan antara dua orang atau lebih dan berlangsung antara narasumber dan pewawancara. Tujuan dari wawancara ialah untuk memperoleh informasi yang tepat dari narasumber yang terpercaya. Wawancara dilakukan dengan cara penyampaian sejumlah pertanyaan dari pewawancara kepada narasumber. Wawancara terbagi menjadi dua kategori, yaitu wawancara terstruktur dan tidak terstruktur.

1. Metode Pengolahan Data

Apriori merupakan sebuah algoritma yang mengolah suatu database transaksi dengan setiap transaksi adalah suatu himpunan item-item. Kemudian mencari seluruh kaidah apriori yang memenuhi kendala minimum support dan minimum confidence yang diberikan user.

1. Metode Pengembangan Sistem

Metode untuk penelitian ini adalah Prototype. Prototype model ini merupakan metode siklus hidup pengembangan perangkat lunak yang bertujuan mendapatkan kebutuhan yang jelas. Metode ini memungkinkan untuk pengembangan piranti lunak yang jauh lebih cepat dibanding metode waterfall. Metode prototype digunakan karena cocok untuk sistem yang bersifat customize (Susanto, 2016).

1. Metode Pengembangan Perangkat Lunak

Perancangan dan pembangunan aplikasi dilakukan dengan menggunakan bahasa pemrograman Python dan database mySQL untuk sistem berbasis web dengan menerima masukan berupa file excel berformat .xls untuk data training dan data testing. Metode yang digunakan merupakan Object Oriented Programming (OOP).

1. Metode Pengujian Perangkat Lunak

Pengujian akan dilakukan dengan metode Black-box testing, karena black-box testing yang dibutuhkan untuk pengujian adalah fungsionalitas program tanpa alur kineja program.

## Sistematika Penulisan

Dalam penulisan skripsi ini dibagi dalam 5 bab, yaitu:

**BAB I : PENDAHULUAN**

Bab ini digunakan untuk mendefinisikan persoalan, ruang lingkup dan perencanaan kegiatan dilakukan. Bab ini berisi latar belakang, identifikasi permasalahan, ruang lingkup dan batasan permasalahan, tujuan perancangan, metodologi penelitian dan sistematika penulisan.

**BAB II : DASAR TEORI**

Bab ini berisi teori-teori pendukung tentang teori permasalahan, analisa penggalian data, pengembangan sistem, pengembangan perangkat lunak, yang meliputi: konsep dasar sistem, konsep dasar data mining, konsep dasar algoritma naive bayes, pengertian Prototype, pengertian OOP, pengertian web, pengertian UML, PHP, dan Framework CI, serta teori-teori lainnya yang digunakan untuk mendukung penganalisaan dan pengembangan sistem baru yang diusulkan.

**BAB III : ANALISIS DAN PERANCANGAN PERANGKAT LUNAK**

Bab ini berisi analisa penggalian data dalam memprediksi kelulusan mahasiswa berdasarkan IPK serta rancang bangun perangkat lunak yang akan di implementasikan.

**BAB IV : ANALISIS DAN PERANCANGAN PERANGKAT LUNAK**

Bab ini berisi uraian hasil rancangan sistem secara nyata, menggambarkan penggunaan perangkat lunak serta implementasi.

**BAB IV : KESIMPULAN DAN SARAN**

Bab ini berisi kesimpulan dan saran untuk kajian yang dapat dituliskan.