

# 1. PENDAHULUAN

## 1.1. Latar Belakang

Komunikasi merupakan sebuah interaksi yang sering kita temui pada aktifitas sehari-hari. Komunikasi merupakan suatu hal yang tidak dapat dihindari oleh setiap manusia. Sebagai makhluk sosial, manusia dikodratkan untuk hidup berinteraksi dengan manusia lainnya dengan berkomunikasi. [1] Beragam cara penyampaian informasi dari masa ke masa sudah melalui banyak perubahan. Komunikasi sederhana yang sering kita temui dapat berupa percakapan secara langsung antara dua orang atau lebih yang saling dapat bertatap muka. Komunikasi juga merupakan suatu media untuk menyampaikan sebuah informasi, baik informasi yang penting ataupun hanya sekedar ungkapan sapaan. Seiring perkembangan jaman, kini berkomunikasi dapat dilakukan dengan jarak jauh. Terdapat aplikasi berbasis *Chatting* yang kini dapat digunakan untuk melakukan komunikasi dalam jarak jauh. Namun pada aplikasi berbasis *Chatting* juga harus terdapat keamanan yang dapat menyimpan informasi percakapan antara dua belah pihak, baik dari pihak pengirim maupun pihak penerima pesan.

Penggunaan teknologi komputer dan teknologi telekomunikasi pada saat ini sudah dapat merubah cara pandang masyarakat dalam berkomunikasi. Kemajuan pesat yang terjadi pada bidang jaringan komunikasi seluler dengan *open system-nya*, yang sehingga dapat memudahkan orang lain untuk masuk kedalam jaringan tersebut. Hal tersebut dapat membuat proses pengiriman data menjadi terkendala, dan bahkan dapat terjadinya pencurian data di tengah tengah pengiriman data dan atau informasi tersebut. Masalah keamanan merupakan suatu aspek yang sangat penting dalam suatu proses pengiriman informasi yang memlalui suatu jaringan. Oleh karena itu dibutuhkan suatu system yang dapat dibangun suatu system keamanan data yang dapat menjaga kerahasiaan data maupun informasi tersebut.

Dalam membangun sebuah metode keamanan yang baik, diperlukan metode keamanan yang baik pula dalam menunjang efektifitas dan fungsionalitas. Terdapat beberapa metode keamanan yang dapat digunakan sebagai pilihan. Penerapan metode yang sudah ada akan memberikan keamanan yang baik, namun dengan adanya metode enkripsi berlapis, akan meminimalisasi kemungkinan

peretas data terhadap data yang sedang diolah. Dengan penerapan enkripsi berlapis, akan memberikan tingkat keamanan yang lebih optimal, dimana data olah sudah melalui lebih dari satu kali proses enkripsi, yang mana hasil dari enkripsi tersebut dienkripsi kembali yang menghasilkan data baru yang lebih sulit ditebak. Penggunaan tiga metode kombinasi yang menjadi pengujian berupa dua metode keamanan yang cukup kuno yaitu Reverse Cipher dan Vignere Cipher, dengan metode muda yaitu RSA.

Kriptografi adalah teknik untuk mencapai kerahasiaan pesan. Istilah ini memiliki arti khusus dalam Bahasa Yunani yang memiliki arti tulisan rahasia. Saat ini bagaimanapun, privasi individu dan organisasi disediakan melalui kriptografi pada tingkat tinggi, yang memastikan bahwa informasi yang dikirim aman dengan cara penerima yang berwenang dapat mengakses informasi tersebut [2] . Dalam Teknik pengamanan data, terdapat banyak metode keamanan yang dapat digunakan, berbagai macam metode metode kriptografi tersebut mempunyai cara dan steps tersendiri, dan langkah pengerjaan yang berbeda beda, baik dari segi panjangnya dan tingkat kerumitan yang digunakan. Salah satu metode kriptografi yang dapat digunakan dan akan digunakan pada kali ini adalah metode Reverse Cipher. Namun karena lemahnya tingkat keamanan jika hanya melakukan peninjauan keamana hanya dengan metode Reverse Cipher, maka akan dikombinasikan dengan metode RSA yang dapat digunakan sebagai kunci public dengan tingkat keamanan yang tinggi. Kemudian dilakukan penelitian mengenai kombinasi antara metode kriptografi Reverse Cipher yang dikombinasi dengan metode RSA yang akan diterapkan pada keamanan data teks dalam mencapai tujuan didapatkan tingkat keamanan yang tinggi.

Dari ketiga metode yang digunakan, dua diantaranya merupakan metode klasik, dan satu diantaranya merupakan metode yang baru ditemukan. Pada penelitian kali ini penulis mengevaluasi dari ketiga kombinasi metode tersebut. Metode reverse cipher dan vigenere cipher termasuk klasifikasi metode mudah dan kuno. Metode tersebut digunakan penulis supaya penulis dapat mengevaluasi apakah metode klasik atau kuno masih bisa bekerja sama dengan metode terkini dalam mengamankan data.

## 1.2. Perumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah yang akan diangkat pada masalah kali ini adalah sebagai berikut:

1. Bagaimana cara penerapan metode enkripsi dan deskripsi Reverse Cipher, Vigenere Cipher dan digabungkan dengan metode RSA untuk melakukan keamanan enkripsi data teks dan menentukan waktu proses eksekusi?
2. Bagaimana kerja efektifitas metode kriptografi kuno Reverse Cipher dan Vigenere Cipher jika dikombinasikan dengan metode yang ditemukan di era sekarang yaitu metode RSA?
3. Apakah hasil evaluasi terhadap metode kriptografi memiliki dampak terhadap pengamanan data teks.

## 1.3. Tujuan

1. Implementasikan enkripsi dan deskripsi pada setiap metode yang digunakan meliputi, Vigenere Cipher, Reverse Cipher, dan RSA.
2. Dapat mengetahui efektifitas hasil dari kombinasi metode di era lama dengan metode di era sekarang.
3. Dapat mengevaluasi hasil enkripsi untuk diterapkan dalam pengamanan data teks.

## 1.4. Batasan Masalah

Berikut ini adalah ruang lingkup yang ada pada penulisan tugas akhir ini adalah sebagai berikut:

1. Meningkatkan keamanan informasi pada pengiriman data.
2. Aplikasi yang digunakan menggunakan *operating system* berbasis android dengan minimal version *marshmallow*.
3. Data yang diolah berupa data berbasis string.

## 1.5. Sistematika Penulisan

Sistematika Penulisan Tugas Akhir disusun dengan sistematika penulisan sebagai berikut:

1. **BAB 1 Pendahuluan** pada bab ini akan dibahas mengenai latar belakang, rumusan masalah, dan tujuan.
2. **BAB 2 Kajian Pustaka** pada bab ini akan dibahas mengenai teori teori yang berkaitan dengan perancangan system yang akan dibangun. Dengan menggunakan metode yang sudah ada, dan melakukan analisis terkait kebutuhan yang menunjang jalannya pembangunan system yang akan dibangun
3. **BAB 3 Perancangan Sistem** pada bab ini akan dibahas mengenai metode yang digunakan dalam penelitian, dan rancangan system dengan metode yang ada dalam pengujian yang sedang dilakukan dalam penelitian
4. **BAB 4 Hasil dan Perancangan** pada bab ini akan dibahas mengenai hasil pengujian yang dilakukan oleh penulis dalam penelitian.
5. **BAB 5 Kesimpulan dan Saran** pada bab ini merupakan kesimpulan dan saran penulis terhadap pembaca.

## 1.6. Sistematika Penulisan

Sistematika Penulisan Tugas Akhir disusun dengan sistematika penulisan sebagai berikut:

6. **BAB 1 Pendahuluan** pada bab ini akan dibahas mengenai latar belakang, rumusan masalah, dan tujuan.
7. **BAB 2 Kajian Pustaka** pada bab ini akan dibahas mengenai teori teori yang berkaitan dengan perancangan system yang akan dibangun. Dengan menggunakan metode yang sudah ada, dan melakukan analisis terkait kebutuhan yang menunjang jalannya pembangunan system yang akan dibangun
8. **BAB 3 Perancangan Sistem** pada bab ini akan dibahas mengenai metode yang digunakan dalam penelitian, dan rancangan system dengan metode yang ada dalam pengujian yang sedang dilakukan dalam penelitian
9. **BAB 4 Hasil dan Perancangan** pada bab ini akan dibahas mengenai hasil pengujian yang dilakukan oleh penulis dalam penelitian.
10. **BAB 5 Kesimpulan dan Saran** pada bab ini merupakan kesimpulan dan saran penulis terhadap pembaca.