BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Meningkatnya pengguna internet yang disebabkan oleh pandemi *COVID-19* belakangan ini ternyata mempengaruhi tingkat kejahatan siber yang terjadi di dunia. Menurut data dari salah satu perusahaan keamanan siber *Trend Micro*, tipe kejahatan siber yang banyak dijumpai adalah *phising* dan *ransomeware*. Kedua tipe kejahatan tersebut mendapatkan peningkatan kasus hingga dua kali lipat sejak pandemi pada tahun 2020 hingga 2021 kemarin. Kedua tipe kejahatan siber tersebut mempunyai satu kesamaan yaitu mencuri informasi pribadi dari korban seperti pencurian identitas, data rekening, password dan informasi berharga lainnya. Untuk meminimalisir dampak dari kasus-kasus di atas, ada beberapa cara untuk mengamankan informasi dalam dunia teknologi, diantaranya yaitu dengan menggunakan teknik kriptografi dan steganografi.

Secara universal, kriptografi menggambarkan suatu prosedur dengan suatu kunci tertentu yang mengolah data awal (*plaintext*) menjadi data baru yang tidak dapat dibaca oleh bahasa manusia(*cipher text*) dan sebaliknya. Adapun penamaan proses tersebut adalah proses enkripsi sedangkan proses kebalikannya adalah proses dekripsi. Pada umumnya terdapat dua jenis kriptografi yaitu simetris dan asimetris. Perbedaan keduanya yaitu terdapat pada kunci yang digunakan untuk proses enkripsi dan dekripsi dimana kriptografi simetris menggunakan satu kunci sedangkan kriptografi asimetris menggunakan dua kunci yang berbeda. Contoh kriptografi asimetris yaitu *RSA.*

Steganografi adalah seni penyembunyian informasi ke dalam informasi lainnya yang telah ada sejak sebelum masehi dan saat ini di tengah pertumbuhan dan kemajuan teknologi jaringan, steganografi banyak dimanfaatkan untuk mengirim informasi melalui jaringan internet tanpa terlihat orang lain [3]. Terdapat tiga bagian penting yang ada dalam steganografi yaitu *secret-data*, *cover-object* dan *stego-object*. Penjelasan dari secret-data adalah informasi rahasia yang akan disembunyikan. *Cover-object* merupakan media atau wadah dimana secret-data akan disembunyikan sedangkan *stego-object* adalah hasil proses penggabungan *secret-data* dengan *cover-object* melalui proses steganografi. Jenis

media yang umum digunakan pada steganografi yaitu video, gambar, audio dan teks. Steganografi pada media teks dipercaya lebih sulit dikarenakan sedikitnya redundansi pada struktur data media teks. Media teks memiliki struktur yang identik seperti yang terlihat sedangkan media selain teks memiliki struktur yang berbeda dengan yang terlihat. Sulit dilakukan penyembunyian informasi pada media teks jika harus mengubah struktur datanya karena jika ada perubahan makna atau penambahan simbol, maka akan mudah dicurigai. Kelebihan dari penggunaan media teks dalam steganografi yaitu sedikitnya penggunaan memori dan proses sorting yang lebih cepat dibandingkan media lainnya [4].

Pada penelitian sebelumnya, banyak digunakan kombinasi antara kriptografi dengan steganografi untuk mengamankan informasi diantaranya kriptografi biner ke *ASCII* digabungkan dengan steganografi yang menggunakan *cover-object* kodingan *website*[22], kriptografi *twofish+3DES* digabungkan dengan steganografi *LSB* menggunakan *cover-object* gambar iris mata[23], kriptografi *Hill Cipher* digabungkan dengan steganografi *LSB* menggunakan *cover-object* gambar[7], kriptografi *Caesar Cipher* untuk mengenkripsi nama *file* dan *folder* digabungkan dengan steganografi dengan *cover-object* fungsi *OS Windows*[10] dan kriptografi *AES+ECC* digabungkan dengan steganografi LSB menggunakan *cover-object* foto profil user pada suatu *website cloud*[26]. Melihat jarangnya penelitian yang menggunakan metode penggabungan kriptografi asimetris dengan steganografi dengan *cover-object* teks, penulis tertarik untuk mencoba membuat suatu aplikasi yang menggunakan gabungan kriptografi asimetris *RSA* dengan steganografi teks dengan metode *LSB Matching*.

Dalam kriptografi, *RSA* merupakan algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini merupakan algoritma paling awal yang diketahui sangat cocok untuk menandai (*signing*) dan untuk enkripsi (*encryption*) serta salah satu penemuan besar pertama dalam kriptografi kunci publik[1]. *RSA* pertama kali dipublikasikan pada tahun 1978 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman[5]. Ada dua kunci yang digunakan pada kriptografi RSA yaitu kunci publik yang dapat dibagikan ke umum dan kunci privat yang hanya boleh diketahui pihak tertentu. Fungsi kunci publik adalah untuk proses enkripsi sedangkan fungsi kunci privat adalah untuk proses dekripsi.

Least Significant Bit (LSB) merupakan sebutan untuk suatu bit dari data biner yang letaknya paling kanan dan mempunyai nilai paling tidak berarti. Maksud dari tidak berarti disini artinya adalah jika dilakukan perubahan pada nilai bit tersebut, tidak terjadi perubahan yang signifikan pada data. Steganografi metode *Least Significant Bit* (*LSB*) merupakan metode yang sering digunakan untuk media selain teks. Secara umum, cara kerjanya yaitu melihat setiap angka biner *LSB* dari suatu data yang dijadikan *cover-object* kemudian dicocokkan dengan setiap angka biner data pesan rahasia agar data tersebut dapat disisipkan jika terdapat kemiripan pada angka biner *LSB* data *cover-object*.

Berdasarkan uraian di atas, untuk mengamankan informasi, bisa digunakan dua jenis algoritma yaitu kriptografi dan steganografi. Lalu, melihat belum adanya penelitian yang menggabungkan kriptografi asimetris dengan steganografi dengan *cover-object* teks maka dalam penelitian ini, penulis mencoba untuk menggabungkan kedua algoritma tersebut dalam bentuk Tugas Akhir dengan judul "**Implementasi Algoritma RSA dan Steganografi Dengan Metode LSB Matching Untuk Keamanan Pengiriman Informasi**".

1.2 Perumusan Masalah

Berdasarkan dari latar belakang yang telah diuraikan di atas, maka penyusun dapat merumuskan masalah yaitu :

1. Bagaimana cara mengenkrip dan dekrip informasi yang dikirim dan diterima dengan menggunakan kriptografi *RSA*?
2. Bagaimana cara menyisipkan dan mengembalikan informasi yang dikirim dan diterima dengan menggunakan steganografi teks metode *LSB Matching*?
3. Bagaimana cara membangun aplikasi yang menggabungkan algoritma kriptografi *RSA* dan steganografi teks metode *LSB Matching* untuk menambah keamanan penyampaian informasi yang dikirim dan diterima?

1.3 Batasan Masalah

Batasan masalah yang terdapat pada penelitian ini yaitu :

1. Algoritma yang digunakan dalam proses enkripsi dan dekripsi adalah algoritma kriptografi *RSA* standar.
2. Metode yang digunakan dalam proses steganografi adalah metode *LSB Matching* dengan tambahan *stego key*.
3. Jenis steganografi yang dipakai adalah steganografi teks ke dalam teks.

4. Format file yang didukung dalam steganografi adalah format *.txt*, *.docx*, dan *.doc* saja.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah :

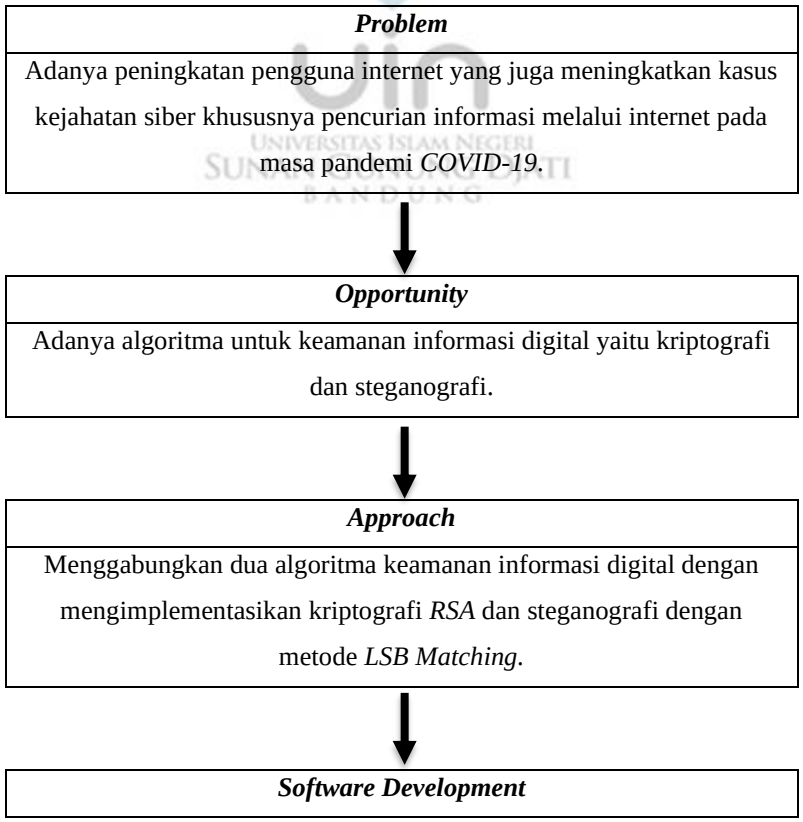
1. Memahami cara mengenkrip dan dekrip informasi yang dikirim dan diterima dengan menggunakan algoritma kriptografi *RSA*.
2. Memahami cara menyisipkan dan mengembalikan informasi yang dikirim dan diterima dengan menggunakan steganografi teks metode *LSB Matching*.
3. Membangun aplikasi yang menggabungkan algoritma kriptografi *RSA* dan steganografi teks metode *LSB Matching* untuk menambah keamanan penyampaian informasi yang dikirim dan diterima.

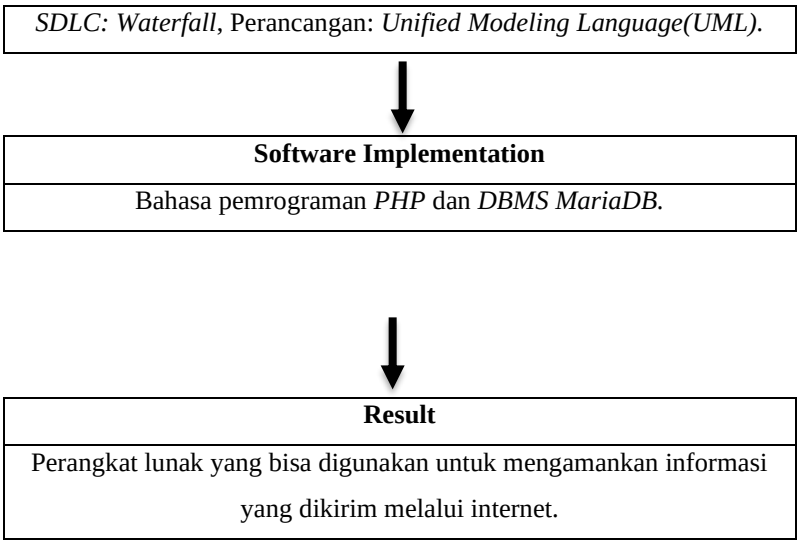
1.5 Manfaat Penelitian

Penelitian ini bermanfaat sebagai referensi pengetahuan tentang teknik kriptografi dan steganografi bagi dunia akademik dan alternatif bagi masyarakat umum untuk mengamankan informasi digital mereka.

1.6 Kerangka Pemikiran

Kerangka pemikiran mengenai penelitian ini akan digambarkan melalui diagram di bawah ini.





1.7 Metodologi Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode eksperimental. Dalam penelitian ini peneliti menguji coba objek yang dibuat, lalu melakukan pengamatan, merekam hasil uji coba yang dilakukan dan melihat bagaimana relasi setiap inputan untuk dianalisa pengaruhnya terhadap output yang dihasilkan.

1.7.1 Tahap Pengumpulan Data

Adapun metode yang digunakan dalam pengumpulan datanya adalah sebagai berikut:

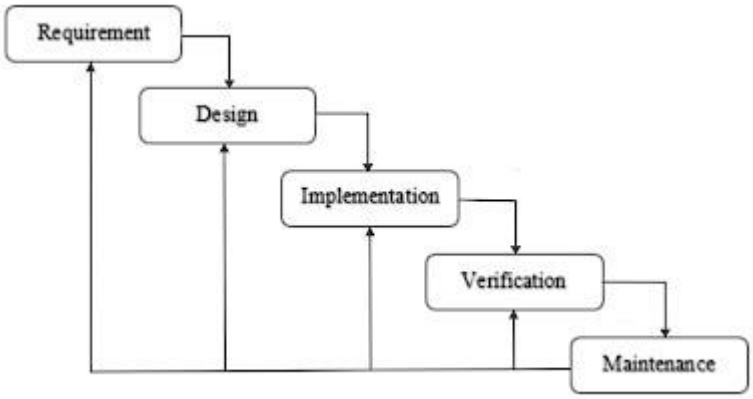
a. Observasi,

Observasi adalah proses mengamati secara langsung kepada objek yang ingin diteliti untuk mendapatkan informasi yang dibutuhkan.

b. Studi Literatur

Studi literatur adalah proses mengumpulkan data melalui review literatur seperti buku, jurnal dan laporan penelitian yang berkaitan dengan objek penelitian.

1.7.2 Tahap Pengembangan Perangkat Lunak



Gambar 1. 1 SDLC Waterfall

Model ini berjalan secara sistematis dari tahap satu ke yang lainnya seperti namanya yang berarti air terjun [2]. Terdapat beberapa tahapan dalam model *Waterfall*, diantaranya:

a. Analisa Kebutuhan (Requirement)

Pada tahap ini, pengembang mencari informasi melalui diskusi, survey atau wawancara untuk memahami perangkat lunak yang akan digunakan oleh penggunanya juga mengetahui batasan dari perangkat lunaknya.

b. Perancangan Sistem (Design)

Hasil dari tahap analisa kebutuhan kemudian diterjemahkan ke dalam rancangan perangkat lunak. Rancangan tersebut biasanya terdiri dari struktur data, arsitektur sistem, antarmuka dan detail algoritma yang digunakan.

c. Implementasi (Implementation)

Pada tahap ini, pengembang menerjemahkan rancangan sistem yang sudah dibuat ke dalam suatu bahasa pemrograman yang dimengerti oleh mesin komputer. Hasilnya berupa modul-modul kecil yang nantinya akan digabungkan.

d. Pengujian (Testing)

Setiap modul yang telah dibuat pada tahap coding akan dilakukan pengujian untuk menghindari masalah yang lebih besar pada setiap modul digabungkan.

e. Pemeliharaan (Maintenance)

Tahap terakhir dari model waterfall. Perangkat lunak yang telah selesai dibuat selanjutnya akan dijalankan dan dilakukan pemeliharaan.

1.8 Sistematika Penulisan

Penyusunan laporan tugas akhir ini dibagi menjadi lima bagian yaitu:

BAB I PENDAHULUAN

Pada bagian ini akan ada delapan bahasan yaitu latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, kerangkan pemikiran, metode penelitian dan sistematika penulisan laporan.

BAB II STUDI PUSTAKA

Pada bagian ini akan dijelaskan teori-teori yang berhubungan dengan tema penelitian dan *state of the art* dari penelitian yang terkait selama lima tahun kebelakang.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bagian ini akan dibahas analisis masalah, data, solusi dan juga algoritma yang digunakan. Selain itu, di bagian ini juga akan dibahas arsitektur sistem hingga ke perancangan sistemnya.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bagian ini akan dibahas bagaimana sistem akan diimplementasikan mulai dari perangkat apa yang digunakan sampai ke tahap pengujian sistem.

BAB V PENUTUP

Pada bagian ini akan dibahas hasil dari penelitian yang dilakukan dalam bentuk kesimpulan dan saran yang berikan terhadap penelitian penulis.