BAB 1

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi yang pesat telah mengubah secara fundamental cara kita hidup, berkomunikasi, dan berinteraksi dengan dunia. Kemajuan ini telah membawa manfaat besar, tetapi juga memunculkan tantangan baru, terutama dalam hal keamanan data. Keamanan data merupakan aspek penting dalam era digital, karena informasi sensitif dapat menjadi sasaran serangan dan penyalahgunaan oleh pihak yang tidak berwenang.

Dalam menghadapi tantangan keamanan data, kriptografi memainkan peran yang sangat penting. Kriptografi adalah ilmu yang berkaitan dengan teknik-teknik matematika dan komputer yang digunakan untuk melindungi informasi dan data. Melalui proses enkripsi, data dapat diubah menjadi bentuk yang tidak dapat dimengerti oleh pihak yang tidak berwenang, sehingga menjaga kerahasiaan dan integritasnya.

Salah satu sistem kriptografi yang menonjol adalah Paillier Cryptosystem. Paillier Cryptosystem merupakan sistem kriptografi asimetris yang memungkinkan enkripsi dan dekripsi data dengan tingkat keamanan yang tinggi [1] Sistem ini memiliki keunggulan dalam melakukan komputasi homomorfik, yang memungkinkan operasi matematika dilakukan pada data yang dienkripsi tanpa perlu mendekripsinya terlebih dahulu.

Namun, penggunaan Paillier Cryptosystem pada enkripsi gambar masih belum banyak diteliti. Enkripsi gambar memiliki tantangan tersendiri karena

gambar memiliki kompleksitas yang tinggi dan ukuran yang besar. Oleh karena itu, penelitian yang mendalam diperlukan untuk mengkaji dan menerapkan Paillier Cryptosystem dengan efisiensi dan keamanan yang optimal dalam konteks enkripsi gambar.

Selain itu, perubahan teknologi juga memberikan dampak signifikan pada keamanan data dan kriptografi. Perkembangan teknologi seperti komputasi awan, Internet of Things (IoT), dan komputasi berbasis blockchain telah mengubah lanskap keamanan data. Dalam menghadapi perubahan ini, penting untuk mempelajari bagaimana teknologi baru tersebut dapat mempengaruhi keamanan data dan bagaimana kriptografi dapat beradaptasi dengan perubahan tersebut.

Keamanan data dalam konteks enkripsi gambar juga melibatkan aspek integritas dan keaslian gambar. Dalam proses enkripsi gambar, perlu ada mekanisme yang dapat memastikan bahwa gambar yang dienkripsi tidak mengalami modifikasi yang tidak sah. Oleh karena itu, analisis mengenai kelemahan dan tantangan dalam memastikan integritas dan keaslian gambar perlu dilakukan.

Penelitian terkait enkripsi gambar menggunakan Paillier Cryptosystem juga dapat memberikan kontribusi dalam pengembangan aplikasi keamanan data yang lebih luas. Dengan mengkaji efisiensi dan keamanan enkripsi gambar dengan menggunakan Paillier Cryptosystem, penelitian ini dapat memberikan panduan dan rekomendasi praktis bagi pengembang perangkat lunak dan sistem yang berhubungan dengan keamanan data.

Dalam penelitian ini, akan dilakukan eksplorasi dan analisis mendalam terkait perubahan teknologi dalam keamanan data melalui penggunaan Paillier Cryptosystem pada enkripsi gambar. Fokus penelitian akan diberikan pada pemahaman dan pemecahan masalah yang terkait dengan efisiensi, keamanan, dan integritas enkripsi gambar menggunakan Paillier Cryptosystem.

Algoritma ini adalah algoritma yang masih dikembangkan sampai hari ini. Dalam prosesnya algoritma ini memerlukan kunci kunci yang berbeda pada setiap tahapan prosesnya dimana kunci pribadi atau private key digunakan pada proses deskripsi dan kunci umum atau public key untuk proses enkripsi. Paillier cryptosystem salah satu dari algoritma yang menggunakan prinsip homomorfik. Homomorfik adalah proses yang dapat memungkinkan berjalan secara independen. Proses komputasi pada data cipher tanpa mendeskripsikan terlebih dahulu cipher. algoritma Paillier Cryptosystem ini menarik dengan prinsip homomorfik didalamnya. Oleh karena itu penulis mengusung judul **"Implementasi Algoritma *Paillier Cryptosystem* Pada *Image Signature*".**

1.2. Rumusan Masalah

Meninjau pada latar belakang yang telah diuraikan, didapati rumusan masalah sebagaimana berikut:

1. Bagaimana penerapan Algoritma Paillier Cryptosystem pada Gambar Tanda Tangan Digital
2. Bagaimana efektivitas dari Algoritma Paillier Cryptosystem pada media citra digital

1.3. Tujuan Penelitian

Penelitian ini dilakukan dengan maksud tujuan yang akan dicapai adalah sebagai berikut:

1. Memperoleh hasil penerapan algoritma paillier cryptosystem pada media citra digital
2. Mengetahui efektivitas algoritma paillier cryptosystem pada fitur Enkripsi Gambar

1.4. Batasan Masalah

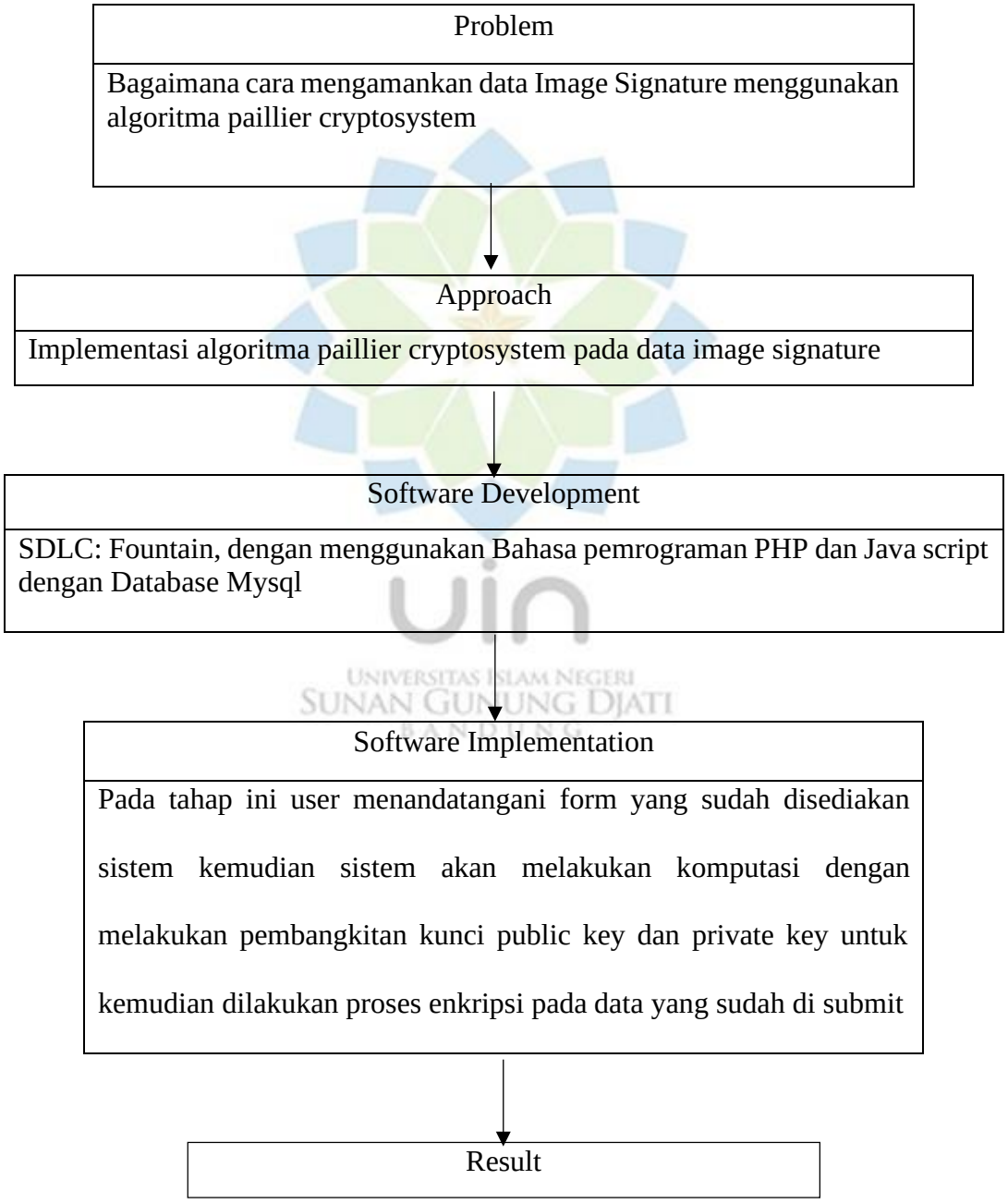
Dalam perkembangan dan pembahasannya terkait penelitian ini dapat ditinjau dalam permasalahan di atas batasan-batasan masalah yang akan diselesaikan dalam penelitian ini, di antaranya adalah :

1. Pendataan tanda tangan digital dalam penelitian ini menggunakan algoritma paillier cryptosystem.
2. Data dari Gambar hasil dari proses komputasi akan disimpan kedalam database.

Data dari Gambar Tanda tangan akan di deskripsikan secara otomatis sebelum ditampilkan.

1.5. Kerangka Pemikiran

Adapun kerangka pemikiran pada penelitian ini sebagaimana yang terdapat pada gambar dibawah ini.



Sehingga didapati Data Efisiensi Algoritma

Gambar 1.1 Kerangka Pemikiran

Pada gambar diatas kerangka pemikiran terdiri dari beberapa prosedur diantaranya.

1. Problem

Bagaimana cara mengamankan data Tanda Tangan Digital menggunakan algoritma paillier cryptosystem

2. Approach

Implementasi algoritma paillier cryptosystem pada data Tanda Tangan Digital

3. Software Development

SDLC: Fountain, dengan menggunakan Bahasa pemrograman PHP dan Java script dengan Database Mysql

4. Software Implementation

Pada tahap ini user menandatangani form yang sudah disediakan sistem kemudian sistem akan melakukan komputasi dengan melakukan pembangkitan kunci public key dan private key untuk kemudian dilakukan proses enkripsi pada data yang sudah di submit

5. Result

Sehingga didapati Data Image Tangan Digital aman

1.6. Metodologi

Pada penelitian ini penulis membagi menjadi dua metodologi diantaranya adalah sebagai berikut:

1. Metode Pengumpulan Data

Metode pengumpulan data yang penulis gunakan pada penelitian ini:

1. Penulisan Studi Literatur

   Pada metode ini penulis mencari banyak literatur terkait pembahasan pada penelitian guna menambah informasi-informasi penting tentang algoritma yang akan dibahas informasi itu sendiri seperti prinsip dasar dari algoritma dan cara kerja algoritma.

2. Eksperimental

   Pada tahapan ini penulis melakukan beberapa kali percobaan baik mulai dari proses pembangkit kunci public key dan private key dan proses enkripsi berdasarkan rumus pada prinsip prinsip algoritma. Hingga nantinya di dapatin hasil yang mendekati harapan.

2. Metode Pengembangan

Dalam penelitian ini penulis menggunakan metode pengembangan perangkat lunak Fountain [2]pada sistematika penulisan adalah sebagai berikut;

1. Analisa Kebutuhan Software

Dalam proses Analisa kebutuhan software berguna untuk melihat kebutuhan secara mendetail terkait dokumentasi dan interface yang digunakan sebagai acuan untuk menentukan solusi software yang akan dilaksanakan pada tahapan penelitian.

2. Desain

Dalam proses desain ini, disesuaikan berdasarkan kebutuhan sistem yang akan dibuat berdasarkan perencanaan kebutuhan termasuk didalamnya nya database, software architecture, dan User Interface pada penelitian ini. Selain daripada itu penulispun menggunakan Unified Modeling Language (UML) dengan tujuan untuk memberikan informasi lebih dalam rancangan database. UML yang akan digunakan adalah Activity Diagram.

3. Development

Pada Poin ini adalah tahapan implementasi desain dalam proses pembuatan program aplikasi perangkat lunak. Pada tahap ini penulis menggunakan Visual Studio Code untuk membuat aplikasi dengan menggunakan Bahasa pemrograman PHP & JS dengan MYSQL sebagai database.

4. Testing

Penulis melakukan pengujian dengan menggunakan black box dengan harapan dapat menghasilkan sesuai yang direncanakan. Penggunaan black box dalam pengujian aplikasi akan memberikan penjelasan terkait kesesuain rencana dalam pembuatan aplikasi.

5. Maintenance

Proses pemeliharaan ini penulis berupaya sistem ini dapat dilakukan pengembangan lebih lanjut yang mana nantinya dapat digunakan.

Struktur dalam dokumentasi penelitian tugas akhir ini penulis menggunakan konsep konsep dasar dalam membangun perangkat lunak diantaranya sebagai berikut:

BAB I : PENDAHULUAN

Di awal penulis berusaha untuk menggambarkan latar belakang permasalahan, hingga di dapatinya rumusan masalah, Batasan, hingga mendapati tujuan dari penelitian menggunakan metode yang sistematik dan

terstruktur pada penulisan

BAB II : STUDI PUSTAKA

Tahap ini menggambarkan tentang referensi terkait bahan penelitian yang digunakan secara teoritis, sistematis, dan logis guna mendukung pembuatan aplikasi kriptografi keamanan data Tanda Tangan Digital dan beberapa definisi yang dikemukakan oleh para ahli terkait dalam penulisan ini.

BAB III : ANALISA DAN PERANCANGAN

Bab ini menerangkan seputar analisa kebutuhan dasar pada saat membangun sistem dan perancangan yang akan dilakukan penulis dalam penelitiannya.

BAB IV : IMPLEMENTASI DAN PENGUJIAN

Tahap ini menjelaskan tentang proses pengejawantahan dari algoritma yang diimplementasikan pada sebuah sistem berjalan yang terkait pada entitas entitas yang saling terhubung baik software, hardware, database, brainware tak lepas pula user interface hingga mendapatkan hasil dari proses komputasi yang berlangsung.

BAB V : PENUTUP

Bab Kelima menerangkan tentang hasil dari penelitian yang bermuara pada kesimpulan dalam penelitian yang dilakukan secara garis besar serta berisi saran-saran dan kritik untuk pengembangan penelitian ini dimasa depan.