BAB I
PENDAHULUAN

1.2 Latar Belakang

Digitalisasi membawa perubahan yang berdampak luas bagi masyarakat dan dalam perkembangannya memberikan solusi yang efektif guna mendukung berbagai aktivitas dalam banyak aspek kehidupan. Mudahnya mendapatkan akses informasi dengan berselancar di jejaring internet, perubahan ini membuka cara pandang baru dari prinsip-prinsip konvensional menjadi digital adalah suatu langkah perubahan hal ini yang menjadi dasar peneliti. Pengguna internet berdasarkan laporan terbaru situs https://dataindonesia.id/, pada tahun 2023 mencapati 212 juta pengguna internet di Indonesia. Pengguna internet, khususnya yang menggunakan komputer desktop/laptop, tentu saja akan memanfaatkan browser untuk mendapatkan informasi ketika mereka berselancar di dunia maya tersebut [1].

Pada saat berselancar di internet dan menemukan informasi yang menarik, biasanya mereka ingin berbagi kepada pengguna internet yang lainnya. Untuk membaginya, mereka akan menyalin alamat *url* dari berita/informasi yang mereka dapatkan. Biasanya *url* yang akan dibagikan itu panjang, sehingga sulit untuk di *share* kepada pengguna internet lainnya. Oleh karenanya, untuk mempermudahnya, mereka perlu memperpendek *url* tersebut, dengan pemendek *url* [1].

Perkembangan teknologi informasi pada zaman sekarang ini meningkat dengan pesat dan memungkinkan kita mendapatkan informasi secara cepat, tepat dan efisien serta mempunyai manfaat yang sangat besar. Kebutuhan akan informasi semakin meningkat sesuai dengan kebutuhannya. Hal ini membuktikan bahwa teknologi informasi dapat mempermudah dalam menyelesaikan suatu pekerjaan serta dapat mempersingkat waktu suatu pekerjaan khususnya pekerjaan yang berhubungan dengan pengolahan informasi atau data. Dengan semakin banyaknya penggunaan teknologi komputer saat ini, maka permasalahan pun akan bermunculan. Salah satunya yaitu masalah keamanan dan kerahasiaan data yang merupakan aspek penting dari suatu sistem informasi [2].

pada penelitian sebelumnya membahas mengenai penerapan pada sistem rekomendasi dengan memanfaatkan Algoritma Paillier Cryptosystem untuk mengenkripsi data aktivitas pengguna yang mana data tersebut akan memudahkan sampai 30% berdaskan penelitian yang telah dilakukan dengan beberapa percobaan pada saat pengembangan sistem tersebut [3].

Kriptografi dibedakan menjadi dua versi yaitu kriptografi modern dan kriptografi klasik. Kriptografi modern atau biasa dikenal sebagai kriptografi asimetris adalah kriptografi pada prosesnya melakukan komputasi enkripsi dan deskripsi dengan menggunakan kunci yang berbeda, sedangkan, kriptografi simetris menggunakan kunci yang sama pada proses enkripsi dan deskripsinya.

Shortlink memiliki urgensi yang signifikan dalam dunia digital dan pemasaran modern karena kemampuan mereka untuk mempermudah akses, berbagi informasi. Kemudahan akses Shortlink membantu dalam mempersingkat URL yang panjang dan rumit menjadi tautan singkat yang mudah dalam berbagi informasi dan mudah diakses. Ini sangat bermanfaat ketika berbagi tautan melalui media sosial, pesan teks, atau dalam cetakan. Shortlink memungkinkan Anda untuk dengan cepat mengarahkan orang ke sumber daya online tanpa harus memasukkan URL atau kata kunci yang panjang. Ini membantu menghemat waktu dan usaha pengguna, yang pada gilirannya meningkatkan peluang interaksi.

Paillier cryptosystem salah satu dari algoritma yang menggunakan prinsip homomorfik. Homomorfik adalah proses yang dapat memungkinkan berjalannya proses komputasi pada data cipher tanpa mendeskripsikan terlebih dahulu *cipher*. algoritma *Paillier Cryptosystem* ini menarik dengan prinsip homomorfik didalamnya. Oleh karena itu penulis mengangkat tema ini sebagai objek tugas akhir dengan judul ”**IMPLEMENTASI ALGORITMA PAILLIER CRYPTOSYSTEM UNTUK FITUR SHORTLINK BERBASIS WEB**”

1.3 Rumusan Masalah

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

1. Bagaimana penerapan algoritma *Paillier Cryptosystem* pada fitur *Shortlink* berbasis *web*?
2. Bagaimana kinerja dari proses enkripsi menggunakan algoritma paillier cryptosystem?

1.4 Tujuan

Adapun tujuan dari perancangan *Shortlink* dalam menggunakan algoritma *Paillier Cryptosystem* yaitu:

1. Memperoleh hasil penerapan algoritma Paillier Cryptosystem pada fitur *Shortlink*.
2. Memperoleh hasil efektivitas kinerja algortima paillier cryptosystem.

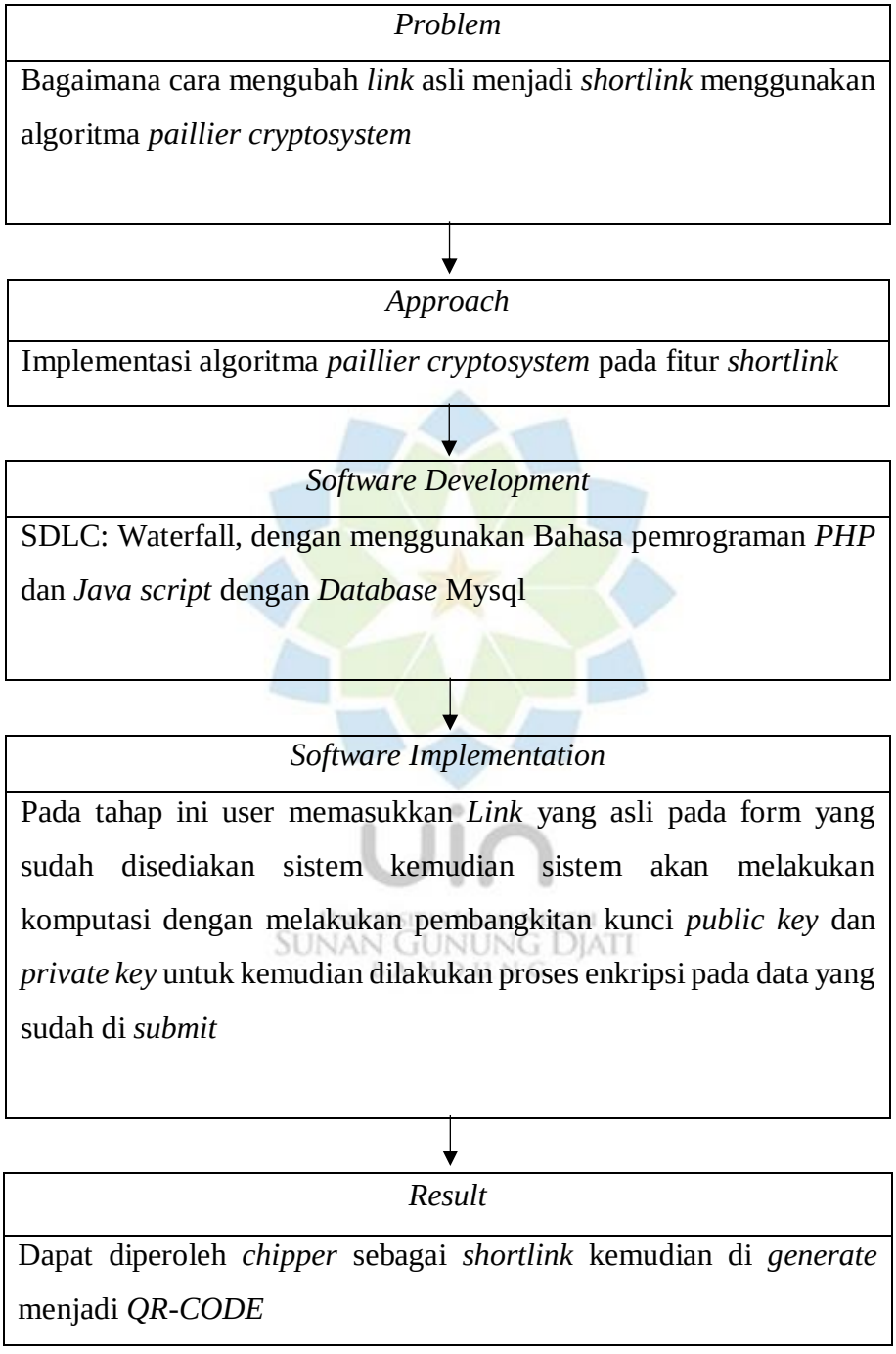
1.5 Batasan Masalah

Agar penelitian ini lebih terarah, penulis membatasi masalah yang akan dianalisa pada pembangunan sistem *shortlink* dengan menggunakan algoritma *pailler cryptosystem* yaitu :

1. Algortima yang digunakan dalam sistem ini adalah Paillier Cryptosystem.
2. Sistem ini digunakan untuk mengubah *URL* asli menjadi *Shortlink*.
3. Sistem ini dibangun menggunakan Bahasa PHP.

1.6 Kerangka Pemikiran

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



1.7 Metodologi

1.7.2 Teknik Pengumpulan Data

Untuk memperoleh data yang akurat sebagai bahan penelitian ini, ada beberapa teknik pengumpulan data yang bertujuan untuk memperoleh keterangan yang jelas dan rinci mengenai masalah yang ada. Berikut merupakan teknik pengumpulan data yang dipakai dalam penelitian ini :

1. **Studi Literatur**

Mengumpulkan bahan terkait topik yang dibahas melalui jurnal, buku-buku referensi, dokumen laporan penelitian dan bahan lainnya yang dapat di jadikan acuan.

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.

1.7.3 Metode Pengembangan

Dalam penelitian ini penulis menggunakan metode pengembangan perangkat lunak *Waterfall* pada sistematika penulisan adalah sebagai berikut;

1. Analisis 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 *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. Implementation

Proses penulisan *code* ada di tahap ini. Pembuatan *software* akan dipecah menjadi modul-modul kecil yang nantinya akan digabungkan dalam tahap selanjutnya.

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.

1.8 Sistematika Penulisan

Adapun sistematika penulisan yang terbagi menjadi 5 bab dalam membuat perangkat lunak. Yang setiap babnya terdapat masing-masing uraiannya. Penulisannya 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 : KAJIAN LITERATUR

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

BAB III : METODOLOGI PENELITIAN

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

BAB IV : HASIL DAN PEMBAHASAN

Tahap ini menjelaskan tentang proses 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 : SIMPULAN DAN SARAN

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.