BAB I

PENDAHULUAN

I.1. Latar Belakang

Pemanfaatan aplikasi komputer dalam suatu perusahaan atau organisasi dewasa ini sudah merupakan suatu kebutuhan. Hampir di semua bidang pekerjaan menggunakan alat bantu berupa aplikasi komputer. Dalam satu perusahaan misalnya, aplikasi komputer sering dibuat sendiri oleh team komputer dari perusahaan tersebut.

Keamanan sistem komputer menjadi semakin penting seiring dengan berkembangnya proses bisnis yang terkomputerisasi. Proses bisnis terkomputerisasi merupakan proses bisnis yang sebagian besar kegiatannya menggunakan teknologi komputer serta menjadikan komputer sebagai media penyimpanan data-data penting sehingga bisa dikatakan media komputer menjadi faktor penting di dalam proses-proses bisnis yang dijalankan. Keamanan sistem komputer yang menjadi sorotan bukan hanya dari perangkat komputernya saja, namun juga keamanan bagi jaringan, *software* atau program aplikasi dan juga keamanan *database*.

Pengolahan data merupakan suatu hal rutinitas pada lembaga pendidikan, khususnya di Pondok Pesantren Darul Hikmah TPI Medan. Sebagai contoh dalam kegiatan proses belajar mengajar dan melakukan evaluasi terhadap nilai hasil belajar siswa pada setiap akhir semester. Evaluasi ini akan rentan apabila proses kerja yang dilakukan masih menggunakan sistem yang lama. Sistem masih

menggunakan cara sederhana yaitu tulis tangan dan pengolahan data yang menggunakan sistem komputer yang mengandalkan Microsoft Excel.

Keamanan dan kerahasiaan data yang tersimpan dalam *database* merupakan salah satu aspek penting dari suatu sistem informasi, seperti data - data tersebut aman dari kebocoran informasi. Pengamanan terhadap jaringan komputer yang terhubung dengan *database* sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh orang dalam atau pihak - pihak yang langsung berhubungan dengan *database* seperti *administrator database* (Siburian et al., 2017).

Keamanan database dapat dilakukan dengan berbagai cara, dimulai dari pembatasan hak akses *user* terhadap database itu sendiri, penggunaan nama *field* yang hanya dimengerti oleh administrator sehingga tidak semua pegawai yang diberi izin mengakses database mengerti alur database yang ada guna menghindari pencurian data, perusakan data dan lain sebagainya, hingga pengimplementasian algoritma kriptografi oleh administrator terhadap *record* dalam databasenya dengan tujuan membuat *record* yang tersimpan menjadi lebih rahasia dan sulit dibaca oleh pihak lain (Surbakti et al., 2018).

Karena penggunaanya yang tidak efisien maka algoritma rahasia mulai ditinggalkan dan diperkenalkan suatu metode baru yang disebut dengan algoritma kunci. Metode ini tidak menumpukan keamanan pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses penyandian. Algoritmanya dapat diketahui, digunakan dan dipelajari oleh siapapun. Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yan lebih baik dibandingkan dengan

algoritma rahasia. Sampai sekarang algoritma kunci masih digunakan secara luas di internet dan terus dikembangkan untuk mendapatkan keamanan yang lebih baik.

Salah satu mekanisme untuk meningkatkan keamanan data dalam *database* adalah dengan menggunakan teknologi enkripsi. Data-data yang disimpan dalam database diubah sedemikian rupa sehingga tidak mudah dibaca. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data (yang disebut *plaintext*) menjadi data yang tersembunyi (disebut *ciphertext*). *Ciphertext* adalah data yang sudah tidak dapat dibaca dengan mudah (Sakti, 2018).

Salah satu metode yang dapat digunakan untuk pengamanan *database* adalah Algoritma Elgamal. Algoritma Elgamal ditemukan oleh ilmuwan Mesir, yaitu Taher Elgamal pada tahun 1985, merupakan algoritma kriptografi kunci publik. Proses algoritma Elgamal terdiri menjadi tiga proses, yaitu proses pembentukan kunci, proses enkripsi, dan proses dekripsi. Kriptografi Elgamal pada awalnya digunakan untuk kebutuhan digital signature, namun kemudian dimodifikasi sehingga dapat digunakan untuk pengamanan seperti enkripsi dan deskripsi. Kriptografi Elgamal digunakan kedalam perangkat lunak *security* yang dikembangkan di sistem security lainnya (Ammary et al., 2018).

Keamanan Elgamal didasarkan pada masalah logaritma diskrit untuk mengenkripsi dan mendekripsi pesan secara terpisah. Penyusup yang berusaha mendekripsi pesan yang terputus dapat mencoba memulihkan kunci pribadi. Untuk tujuan ini logaritma perlu dihitung. Tidak ada metode aktual untuk ini,

mengingat kebutuhan tertentu pada kelompok awal terpenuhi (Kaur & Wadhwa, 2017).

Pembangkitan bilangan prima adalah sebuah permasalahan yang esensial di dalam ilmu komputer dan teori bilangan, terutama dalam bidang kriptografi. Hal ini dikarenakan protokol-protokol enkripsi kunci publik didasarkan pada penggunaan dari bilangan prima dengan ukuran besar. Sedangkan keamanan sistem kriptografi kunci publik sering didasarkan pada kesulitan untuk mendpatkan faktor-faktor prima dari suatu bilangan prima yang sangat besar. Meskipun algoritma untuk menentukan keprimaan suatu bilangan yang sudah ditemukan masih terhitung lambat untuk permasalahan saat ini, suatu algoritma probabilistic dapat dibentuk dengan menggunakan metode Fermat (Aziz, 2018).

Bilangan prima banyak dimanfaatkan oleh bidang kriptografi. Meskipun begitu belum ada algoritma eksak yang dapat menentukan keprimaan suatu bilangan secara efisien. Dengan menggunakan Teorema Fermat, suatu alternatif dapat dilakukan yaitu menciptakan algoritma yang bersifat probabilistik untuk menentukan nilai keprimaan suatu bilangan (Mahendra et al., 2022).

Karena sifat probabilistik ini, hasil dari algoritma ini tidaklah eksak melainkan merupakan probabilistik. Meskipun begitu, kemungkinan algoritma ini menghasilkan kesalahan dapat diminimalisasi dengan menggunakan beberapa perhitungan. Dalam dunia komputer sudah ditemukan beberapa cara untuk mencari bilangan prima tersebut, salah satunya adalah dengan menggunakan metode Fermat untuk mencari bilangan prima tersebut.

Berdasarkan latar belakang permasalahan di atas, penulis dalam penulisan ini mengangkat judul **"Kerahasiaan Database Santri Menggunakan Algoritma Elgamal dan Fermat"**.

I.2. Rumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat diambil rumusan masalah sebagai berikut :

1. Bagaimana membangkitkan keacakan bilangan prima menggunakan metode Fermat?
2. Bagaimana menetapkan kunci publik dan kunci privat pada proses enkripsi dan proses dekripsi menggunakan algoritma Elgamal?

I.3. Tujuan

Berdasarkan rumusan masalah yang telah diuraikan, maka penelitian ini bertujuan untuk:

1. Membangkitkan keacakan bilangan prima menggunakan metode Fermat dengan menelusuri *trial* dan melakukan pengujian bilangan prima acak beberapa kali untuk lebih menjamin sebuah bilangan prima tersebut adalah prima (*non-composit*)
2. Menetapkan kunci publik dan kunci privat pada proses enkripsi dan proses dekripsi menggunakan algoritma Elgamal

I.4. Manfaat

1. Mengetahui cara membangkitkan bilangan prima acak dengan menggunakan Fermat yang nantinya akan digunakan sebagai kunci untuk melakukan proses enkripsi dan dekripsi di dalam simulasi program.
2. Dapat meningkatkan keabsahan sebuah bilangan yang telah ditentukan tersebut adalah prima, yang nantinya dapat digunakan sebagai kunci untuk melakukan enkripsi dan dekripsi.
3. Menjaga keaslian isi dokumen tersebut menggunakan fungsi kriptografi ElGamal.

I.5. Batasan Masalah

Mengingat luasnya materi, maka maka penulis menetapkan batasan-batasan terhadap masalah yang akan diteliti. Dalam melakukan penelitian ini penulis memberikan batasan – batasan sebagai berikut :

1. Algoritma yang digunakan dalam pengamanan database ini adalah Algoritma Elgamal dan pembangkitan keacakan bilangan prima menggunakan metode Fermat.
2. Data yang digunakan dan diamankan adalah data dari database santri Pondok Pesantren Darul Hikmah TPI Medan.
3. Proses mengenkripsi dan mendekripsi data hanya berupa teks atau tulisan, bukan suara maupun gambar.

I.6. Sistematika Pembahasan

Sistematika penulisan skripsi ini dibagi menjadi lima bab yang merangkum tiap tahapan yang penulis lakukan, antara lain :

BAB I : PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika pembahasan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menguraikan tentang beberapa penjelasan dan pengertian yang berdasarkan dengan judul.

BAB III : METODOLOGI PENELITIAN

Pada bab ini dijelaskan kerangka kerja (*framework*) yang dipakai untuk penulisan tesis ini.

BAB IV : HASIL

Bab ini memuat pembahasan mengenai hasil pelaksanaan metode/teknik penelitian dan menyajikan data yang mendukung hasil tersebut. Penyajian data dan penjelasannya dilakukan secara terurut dan logis menggunakan teks dan ilustrasi lainnya.

BAB V : PEMBAHASAN

Bab ini menerjemahkan makna dari hasil yang diperoleh untuk menjawab pertanyaan atau masalah penelitian serta menjelaskan pemahaman baru yang didapatkan dari hasil penelitian, yang diharapkan berguna dalam pengembangan keilmuan.

BAB VI : KESIMPULAN DAN SARAN

Bab ini memuat tentang kesimpulan dari penelitian yang telah dilakukan dan saran yang dapat digunakan oleh pihak-pihak yang terkait maupun pihak lain yang membahas permasalahan yang sama.