

# BAB 1

## PENDAHULUAN

### A. Latar Belakang Masalah

Di era digital yang semakin berkembang, keamanan data telah menjadi aspek yang sangat penting dan tidak dapat dipisahkan dalam aktivitas bisnis dan kehidupan sehari-hari. Setiap hari, jutaan *gigabyte* data dipertukarkan melalui jaringan *global*, termasuk informasi pribadi, keuangan, dan informasi sensitif lainnya. Oleh karena itu, pentingnya menjaga data ini terlindungi dengan baik dari potensi ancaman dan risiko. Serangan siber yang semakin canggih dan terkoordinasi terbukti berpotensi menimbulkan kerugian yang signifikan terhadap individu, dunia usaha, dan lembaga pemerintah. Dalam konteks ini, pemahaman mendalam tentang strategi keamanan data diperlukan untuk mengatasi tantangan ini secara efektif. Adapun ayat Al-Qur'an yang tercantum mengenai keamanan dalam surat An Nur ayat 27 yang berbunyi:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَتَذَكَّرُونَ ﴿٢٧﴾

Artinya: "Wahai orang-orang yang beriman, janganlah memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Demikian itu lebih baik bagimu agar kamu mengambil pelajaran."

LPK Farafi Kursus Komputer yang berlokasi di Jl. Kunang, No.80, Kauman, Kec. Metro Pusat, Kota Metro, Lampung. Merupakan salah satu lembaga pendidikan dan kursus computer yang menyediakan berbagai program pelatihan dan penerimaan siswa PKL (Praktek Kerja Lapangan) seperti administrasi profesional ( *microsoft word, microsoft excel, microsoft power point*), desain grafis, fotografi, TKJ (Tehnik Komputer Jaringan), RPL (Rekayasa Perangkat Lunak) akutansi, pemasaran dan multimedia. LPK Farafi Kursus Komputer juga mempunyai unit usaha, yaitu fotografi yang terdiri dari *photobox*, foto studio dan *self photo*, dan juga injek digital printing yang menerima pemesanan mug *custom*, ganci, jam dinding *custom*, *totebag*, dan pin *custom*.

Di LPK Farafi Kursus Komputer, proses setelah peserta didik memenuhi persyaratan untuk pendaftaran, data tersebut di kumpulkan dan di simpan di format *excel* atau *word* tergantung kebutuhan yang diperlukan *admin*. Jika data-

data tersebut sudah lengkap dan masuk ke data resmi LPK Farafi Kursus Komputer, maka selanjutnya akan di masukan juga ke dapodik (Data Pokok Peserta Didik) karena sudah di bawah naungan kemendikbud dan kemenker. Data-data sensitif seperti *photocopy* kartu pelajar atau KTP (Kartu Tanda Penduduk), *photocopy* kartu keluarga, nomor kontak, informasi keuangan pembayaran peserta, pembayaran gaji pegawai dan data penting lainnya yang terdaftar di *database* mereka masih di simpan di lokal komputer admin atau flashdisk dengan menggunakan komputer yang terinstall windows 7.

Pada LPK Farafi Kursus Komputer dalam proses keamanan menggunakan alat *fuzzing*. Meskipun pengamanan *fuzzing* termasuk kuat, namun masih di nilai memiliki kelamahan dan kurang teliti dalam mendeteksi semua kerentanan atau *bug*, terutama yang memerlukan kondisi *input* yang sangat spesifik atau kompleks, dan juga tidak dapat secara langsung memeriksa kondisi fisik atau kerusakan pada flashdisk yang masuk, yang dapat membuat resiko akan terjadinya pencurian data atau peretasan pada komputer tersebut.

Seiring berkembangnya lembaga dan bertambahnya peserta didik di LPK Farafi Kursus Komputer, kemudian menimbulkan kekhawatiran terhadap masalah dalam pemanfaatan data dikarenakan data sensitif peserta didik yang bisa digunakan oleh pihak atau orang yang tidak bertanggung jawab seperti melakukan pencurian identitas untuk membuat identitas palsu, peminjaman uang atau pemalsuan dokumen. Oleh karena itu, pihak LPK Farafi Kursus Komputer menyadari bahwa pentingnya pengamanan data peserta didik yang khusus untuk mencegah hal-hal tersebut terjadi serta tidak dapat dibaca langsung oleh orang-orang tidak bertanggung jawab yang bisa menimbulkan ancaman *cybersecurity*, karena memiliki kelemahan keamanan yang tidak memadai dari segi prasarana ataupun *software*.

Dalam meningkatkan pengamanan data-data peserta didik membutuhkan sebuah metode untuk memberikan keamanan, langkah yang perlu diambil adalah dengan cara mengenkripsi file dokumen. Penerapan kriptografi dengan menggunakan algoritma RSA (*Rivest-Shamir-Adleman*) menjadi solusi yang dipertimbangkan dalam proses penelitian ini. Algoritma tersebut memberikan keamanan dengan cara mengenkripsi data yang bisa terbaca menjadi tidak bisa terbaca. Dengan demikian, diharapkan data dapat lebih aman dan terlindungi dari ancaman keamanan. Serta memberikan perlindungan yang lebih baik terhadap data yang dimiliki LPK Farafi Kursus Komputer.

Berdasarkan permasalahan latar belakang diatas penulis mencoba membuat keamanan data menggunakan algoritma RSA (*Rivest-Shamir-Aldeman*) yang dapat membantu dalam pengamanan data-data penting. Maka penulis berkeinginan untuk menyusun tugas skripsi dengan judul **“IMPLEMENTASI ALGORITMA RSA (*RIVEST-SHAMIR-ADLEMAN*) UNTUK KEAMANAN DATA PADA LPK FARAFI KURSUS KOMPUTER”**.

### **B. Rumusan Masalah**

Dari latar belakang diatas, maka dapat diketahui perumusan masalah dalam pembuatan skripsi ini adalah “Bagaimana cara merancang algoritma RSA (*Rivest-Shamir-Aldeman*) untuk keamanan data pada LPK Farafi Kursus Komputer?”.

### **C. Pembatasan Masalah**

Untuk menghindari perluasan atau percabangan penelitian, maka berdasarkan rumusan masalah di atas, maka batasan masalah antara lain:

1. Penelitian ini akan difokuskan pada analisis penggunaan metode algoritma RSA (*Rivest-Shamir-Adleman*) untuk keamanan data di LPK Farafi Kursus Komputer.
2. Membahas enkripsi dan dekripsi file dokumen menggunakan algoritma RSA (*Rivest-Shamir-Adleman*).
3. File yang diamankan hanya berformat file tipe, .xls .xlsx .docx.
4. Metode yang digunakan adalah SDLC (*System Development Life Cycle*)

### **D. Tujuan Penelitian**

Berdasarkan perumusan masalah diatas, adapun tujuan penelitian kali ini sebagai berikut:

1. Sebagai pengamanan data yang tersimpan dengan menggunakan algoritma RSA (*Rivest-Shamir-Adleman*).

### **E. Kegunaan Penelitian**

Diharapkan hasil dari penelitian ini memiliki manfaat sebagai berikut:

1. Bagi pihak LPK Farafi Kursus Komputer

Penelitian ini dapat berguna untuk sistem pengamanan data yang andal bagi instansi.

## 2. Program Studi Ilmu Komputer

Dalam penelitian ini diharapkan dapat menambah jumlah referensi terkait keamanan data menggunakan algoritma RSA (*Rivest-Shamir-Adleman*) bagi mahasiswa yang akan melakukan penelitian yang sejenis.

## 3. Bagi Penulis

Untuk meningkatkan ilmu pengetahuan dan kemampuan dibidang pengamanan data, menjadikan bukti bagi penulis atas ilmu yang sudah dipelajari saat menjadi mahasiswa dan juga dapat mengimplementasikan ilmu yang di dapat dalam bentuk tugas akhir.

## **F. Metode Penelitian**

Metode penelitian adalah salah satu cara memahami suatu masalah penelitian dengan membimbing peneliti melalui serangkaian langkah dalam melakukan penelitian, termasuk metode dan prosedur yang digunakan dalam penelitian. Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kualitatif.

Adlini M.N, (2022: 3) menarik kesimpulan sebagai berikut:

Penelitian kualitatif merupakan suatu metode penelitian yang bertujuan untuk memahami kenyataan melalui proses penalaran induktif. Dalam penelitian ini peneliti terlibat dengan situasi atau lingkungan dari fenomena yang diteliti. Peneliti dituntut untuk selalu fokus pada fakta dan peristiwa dalam konteks penelitiannya.

## **G. Teknik Analisis Data**

Teknik analisis data merupakan sebuah metode yang membahas tentang proses pengolahan data dan informasi yang diperoleh selama penelitian untuk memperoleh hasil penelitian. Dalam melakukan pengumpulan data menggunakan beberapa teknik antara lain:

### **a. Observasi**

Observasi adalah salah satu cara untuk mendapatkan informasi apapun dari suatu peristiwa dengan cara mengamati secara langsung.

Retno D.P (2022: 102) menarik kesimpulan sebagai berikut:

Observasi dalam penelitian adalah perolehan data dengan menggunakan seluruh indera seperti melihat, mendengarkan, dan mencatat jumlah dan luasnya kegiatan tertentu atau situasi tertentu yang berkaitan dengan masalah yang diteliti.

Adapun data yang peneliti peroleh dengan teknik observasi seperti, LPK Farafi Kursus Komputer mempunyai 3 lantai, kegiatan kursus komputer dilakukan pada lantai 3, lantai 2 untuk studio foto dan lantai 1 untuk administrasi pendaftaran dan lain-lain.

#### **b. Wawancara**

Wawancara adalah percakapan dua orang atau lebih yang berlangsung antara narasumber dan pewawancara dengan tujuan mengumpulkan data-data berupa informasi.

Wulan Dari N.T (2023: 523) menyimpulkan:

Wawancara adalah metode yang digunakan peneliti untuk menyelidiki keakuratan informasi. Metode ini biasanya dikomunikasikan oleh peneliti dengan menggunakan teknologi dari satu orang ke orang lain, baik secara lisan maupun tertulis kepada subjek penelitian ini.

Dari wawancara yang peneliti lakukan dengan teknisi dan admin LPK Farafi Kursus Komputer. Kak Fikry dan Kak Annisa, di peroleh informasi sistem penyimpanan data masih menggunakan file dokumen dan flashdisk, sistem keamanan menggunakan alat fuzzing, dan juga informasi terkait data-data yang ada di LPK Farafi Kursus Komputer.

#### **c. Dokumentasi**

Dokumentasi adalah kegiatan penyediaan dokumen-dokumen dengan menggunakan bukti yang akurat berdasarkan pencarian dari berbagai sumber. Dokumentasi juga dapat diartikan sebagai "Memberikan atau mengumpulkan bukti atau informasi (seperti gambar, kutipan, kliping koran, atau referensi lainnya)." (Pahlepi R.D, 2022).

Pada metode Dokumentasi, peneliti memperoleh beberapa data seperti gambar dari ruangan yang ada di LPK Farafi Kursus Komputer.

#### **H. Sistematika Penulisan**

Berikut ini merupakan sistematika penulisan yang dibuat untuk menyusun skripsi ini adalah sebagai berikut:

## **BAB I PENDAHULUAN**

Pada bab i ini berisikan tentang latar belakang masalah, perumusan masalah, pembatasan masalah, tujuan masalah, kegunaan penelitian, metode penelitian, dan sistematika penelitian.

## **BAB II KAJIAN LITERATUR**

Pada bab ii ini membahas tentang definisi kriptografi dan juga algoritma RSA (*Rivest-Shamir-Adleman*), teori yang digunakan sebagai landasan penelitian serta konsep dasar yang diperlukan untuk menganalisa masalah yang diteliti.

## **BAB III GAMBARAN UMUM PERUSAHAAN**

Pada bab ini menjabarkan secara singkat tentang organisasi, struktur organisasi, tugas dan fungsi dari keanggotaan organisasi, visi dan misi organisasi dan sistem jaringan yang sedang berjalan.

## **BAB IV ANALISIS DAN PEMBAHASAN**

Pada bab iv ini membahas mengenai proses perancangan dan hasil dari perancangan tentang Penerapan keamanan data menggunakan algoritma RSA (*Rivest-Shamir-Adleman*)

## **BAB V PENUTUP**

Pada bab v ini berisikan kesimpulan dari serangkaian pembahasan skripsi dari penelitian yang sudah dilakukan serta saran-saran untuk disampaikan kepada obyek penelitian atau bagi penelitian selanjutnya.

## **DAFTAR LITERATUR**

Bab ini merupakan sumber dari kutipan yang peneliti gunakan dalam mengerjakan proposal skripsi.

## **LAMPIRAN**