

BAB I PENDAHULUAN

1.1 Latar Belakang

Ketergantungan pada komputer dalam berbagai disiplin ilmu mempercepat transfer informasi. Pengiriman informasi mungkin tidak disertai dengan keamanan data yang memadai. Kemampuan mengirim informasi penting dan sensitif menggunakan dokumen PDF dapat dicuri oleh pengguna lain yang tidak berwenang, sehingga keamanan data sangat penting. Berbagai teknik biasa digunakan untuk melindungi data, salah satunya adalah enkripsi. Kriptografi secara umum merupakan ilmu dan teknologi menjaga kerahasiaan pesan dan dikaitkan dengan aspek keamanan informasi seperti kerahasiaan data, validitas data, integritas data, dan otentikasi data yang dilakukan oleh kriptografer.

Segala sesuatu yang melanggar privasi dapat diartikan sebagai tindakan mengumpulkan, mengubah, atau mengakses informasi pribadi seseorang tanpa persetujuan sebelumnya dari pemiliknya. Berdasarkan pemahaman ini, kita dapat menyimpulkan bahwa mencuri informasi penting dan sensitif dalam dokumen PDF adalah pelanggaran privasi. Pencurian informasi sensitif dalam dokumen PDF termasuk dalam kategori kejahatan dunia maya. Islam telah menerangkan dengan jelas pentingnya menjaga privasi

. Di dalam QS. An-Nur ayat 27 disebutkan :

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا
وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

Yang artinya : “Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu selalu ingat”.

Ayat tersebut menjelaskan pentingnya dalam menjaga suatu privasi dimana pada penelitian ini yang menjadi privasi adalah sebuah informasi yang bersifat rahasia yang terdapat pada sebuah dokumen PDF. Untuk itu akan diterapkan suatu

teknik yang dapat dimanfaatkan dalam meningkatkan keamanan sebuah dokumen PDF. Oleh karena itu, informasi yang terkandung di dalamnya tidak dapat diambil oleh orang yang tidak berwenang.

Kriptografi diketahui sebagai teknik penyandian untuk mengenkripsi data serta informasi dari pihak ketiga yang sekiranya tidak berwenang. Dengan menggunakan teknik kriptografi, data yang ada atau tertera pada dokumen PDF tersebut dienkripsi menjadi simbol - simbol tertentu sehingga hanya pihak berwenang saja yang dapat mengetahui data/informasi hasil enkripsi. Pengertian lain dari kriptografi dikenal sebagai ilmu untuk memperoleh kerahasiaan, integritas dan autentikasi data dengan cara mempelajari cara penyandian data. Hingga saat ini sudah berbagai macam jenis kriptografi telah dikembangkan, misalnya algoritma vernam. Dapat disebut juga bahwa vernam merupakan versi lain dari *One-TimePadCipher*. Karena Algoritma Vernam itu sendiri diadopsi dari *One Time Pad Cipher*, yang dimana karakter diganti dengan bilangan bit (0 atau 1).

Berdasarkan penelitian yang dilakukan Pratika Sari Eka. (2018), dengan menggunakan algoritma vernam, pada penelitian tersebut dihasilkan sebuah aplikasi yang dapat dimanfaatkan untuk mengamankan data yang terdapat dalam filetext. Sehingga pengguna dapat menyandikan filetext yang berisikan informasi rahasia. Penelitian lainnya oleh Janter Manuel Gultom, et. al. (2021), pada penelitian tersebut data pegawai dinas lingkungan hidup yang bersifat rahasia itu kemudian diamankan menggunakan algoritma vernam tersebut. Sehingga dengan penggunaan algoritma tersebut informasi yang bersifat pribadi tidak dapat diketahui oleh pihak ketiga yang tidak memiliki kepentingan apapun. Berdasarkan penelitian terdahulu tersebut, pada penelitian ini akan dimanfaatkan penggunaan algoritma vernam untuk mengamankan dokumen PDF.

Penelitian ini bertujuan untuk mengamankan dokumen PDF sehingga tidak dapat diketahui informasi di dalamnya oleh pihak yang tidak bertanggung jawab dan tidak memiliki kepentingan. Pada proses pengamanannya pada penelitian ini algoritma yang akan digunakan dalam mengamankan dokumen PDF adalah algoritma vernam. Berdasarkan latar belakang yang telah dipaparkan diatas, maka

pada penelitian ini akan ditarik sebuah judul “**Penerapan Algoritma Vernam Dalam Mengamankan Dokumen PDF**”.

1.2 Rumusan Masalah

Berikut rumusan masalah yang akan dicari pemecahannya melalui penelitian ini, antara lain :

- a. Bagaimana mengamankan sebuah dokumen PDF yang berisikan informasi yang bersifat rahasia?
- b. Bagaimana penerapan algoritma vernam dalam mengamankan dokumen PDF?
- c. Bagaimana membangun sebuah aplikasi berbasis android untuk digunakan dalam mengamankan dokumen PDF?

1.3 Batasan Masalah

Dalam penulisan penelitian ini dibatasi permasalahannya sebagai berikut :

- a. Sistem yang akan dibangun akan digunakan untuk mengamankan dokumen PDF.
- b. Algoritma yang digunakan dalam sistem untuk mengamankan dokumen PDF adalah algoritma vernam.
- c. Informasi yang akan diamankan berupa teks yang menjadi isi dari dokumen PDF.
- d. Bilangan biner tanpa karakter akan kembali ke notasi asli dari karakter aslinya
- e. Sistem akan dibangun menggunakan perangkat lunak Android Studio dan akan digunakan pada *smartphone* Android.
- f. Bahasa pemrograman yang akan digunakan dalam membangun sistem adalah Java.

1.4 Tujuan Penelitian

Tujuan dari pelaksanaan penelitian ini dapat disimpulkan menjadi poin sebagai berikut :

- a. Mengamankan informasi yang terdapa pada dokumen PDF menggunakan teknik kriptografi.
- b. Menerapkan penggunaan algoritma vernam dalam mengamankan dokumen PDF.
- c. Membangun sebuah aplikasi berbasis android untuk digunakan dalam proses mengamankan dokumen PDF.

1.5 Manfaat Penelitian

Yang menjadi manfaat dari pelaksanaan penelitian ini dapat dilihat sebagai berikut :

- a. Dapat digunakan sebagai media untuk mengamankan sebuah dokumen PDF.
- b. Penggunaan algoritma vernam dapat digunakan untuk mengamankan dokumen PDF.
- c. Penggunaan aplikasi berbasis android dapat mempermudah pengguna dalam mengamankan dokumen PDF secara *mobile* kapanpun dan dimanapun.

