BAB I
PENDAHULUAN

4.1 Latar Belakang

Di dalamkehidupan sehari-hari terkadang seseorangmemerlukan sistemkeamanan dalam berinteraksi dengan oranglain. Sistem keamanan tersebut bertujuan untuk mencegah tindakan pencurian informasi yang bersifat rahasia. Pada saat ini teknik yang dapat digunakan untuk mengamankan suatu data adalah teknik kriptografi. Kriptografi adalah suatu teknik pengamanan data dengan melakukan perhitungan matematika antara data dengan kunci yang digunakan untuk mengubah suatu data ke dalam bentuk lain yang tidak dapat dibaca. Sehingga hanya pemilik kunci saja yang dapat merubah kembali data ke bentuk aslinya agar informasi yang terdapat di dalamnya dapat dibaca.

Segala tindakan yang melanggar privasi dapat diartikan sebagai perolehan, perubahan, atau akses yang tidak sah terhadap data pribadi seseorang tanpa persetujuan pemiliknya. Hal ini merupakan kejahatan dunia maya. Kejahatan dunia maya mengacu pada tindakan ilegal yang dilakukan menggunakan komputer atau platform internet. Kegiatan-kegiatan kejahatan ini sudah mempunyai hukum yang mana di negara-negara masih sebagian terdapat perdebatan mengenai bentuk dan status hukumnya. Definisi ini menggolongkan kejahatan dunia maya sebagai perilaku yang menggunakan komputer atau internet sebagai sarana atau tujuan tindak pidana (Sari et al., 2020). Islam telah secara jelas menggambarkan perlunya menjaga privasi individu. Di dalam QS. An-Nur ayat 27 disebutkan :

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

Yang artinya : “Wahaiorang-orang yang beriman! Janganlah kamu memasuki rumah yang bukanrumahmu 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. Pada penelitian ini

yang dimaksud sebagai privasi adalah informasi rahasia yang terkandung di dalam sebuah file dokumen, sehingga dibutuhkan suatu cara agar dapat melindungi informasi tersebut.

Seiring berkembangnya waktu, banyak algoritma-algoritma yang menerapkan teknik kriptografi untuk digunakan dalam proses pengamanan data diantaranya adalah algoritma beaufort cipher dan algoritma hill cipher. Beaufort cipher dan Hill Cipher adalah dua metode kriptografi yang menggunakan pendekatan berbeda dalam proses enkripsi dan dekripsi pesan. Beaufort cipher merupakan varian dari vigenère cipher, dengan prosedur enkripsi dan dekripsi yang serupa dengan metode induknya. Sementara itu, Hill Cipher adalah algoritma kriptografi yang menggunakan matriks sebagai kunci utama dalam proses pengamanan pesan.

Karakteristik utama Hill Cipher adalah konversi setiap karakter pada plainteks maupun cipherteks ke dalam representasi numerik, dengan operasi matematika dilakukan menggunakan aritmatika modulo. Hal ini memungkinkan proses transformasi pesan menjadi lebih kompleks dan sulit untuk dipecahkan. Kedua metode ini menggambarkan kompleksitas dan keragaman teknik enkripsi dalam bidang kriptografi, di mana setiap algoritma memiliki mekanisme unik untuk melindungi kerahasiaan informasi.

Penelitian ini bertujuan untuk mengamankan suatu file dokumen yang memiliki informasi yang bersifat rahasia atau pribadi. Sehingga dibutuhkan suatu sistem yang dapat digunakan untuk mengamankan file dokumen sehingga tidak dapat diakses oleh orang lain yang tidak berkepentingan. Untuk itu pada penelitian ini akan dikombinasikan algoritma beaufort cipher dan hill cipher ke dalam sebuah sistem untuk mengamankan file dokumen. Penggunaan dua algoritma kriptografi dalam mengamankan file dokumen bertujuan untuk menghasilkan tingkat keamanan yang lebih baik dalam mengamankan sebuah file dokumen. Sehingga file dokumen yang telah diamankan tidak dapat dijebol dengan mudah oleh para kriptanalisis.

Berdasarkan latar belakang diatas, maka dalam penelitian ini akan dibangun sebuah aplikasi yang dapat digunakan untuk mengamankan sebuah file dokumen

menggunakan algoritma beaufort cipher dan hill cipher. Aplikasi keamanan file dokumen pada penelitian ini akan dibangun berbasis mobile dengan tujuan agar dapat digunakan secara mudah dan efisien dengan memanfaatkan smartphone android. Oleh sebab itu pada penelitian ini akan ditarik sebuah judul **"Kombinasi Algoritma Beaufort Chiper dan Hill Chiper Dalam Mengamankan File Dokumen Berbasis Mobile"**.

4.2 Rumusan Masalah

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

a. Bagaimana mengamankan sebuahfile dokumen menggunakan teknik kriptografi ?
b. Bagaimana menerapkan dan mengkombinasikan algoritma beaufort cipher dan hill cipherdalam mengamankan file dokumen ?
c. Bagaimana membangun aplikasi pengamanan file dokumen menggunakan kombinasi algoritma beaufort cipher dan hill cipher berbasis mobile ?

4.3 Batasan Masalah

Dalam penulisan penelitian ini dibatasi permasalahannya sebagai berikut :

a. Aplikasi ini dirancang dan dibangun untuk digunakan pada perangkat mobile dengan sistem operasi android untuk mengamankan file dokumen.
b. File dokumen yang dapat diamankan menggunakan aplikasi pada penelitian ini adalah file dokumen dengan ekstensi .doc/.docx, .xls/.xlsx dan .pdf.
c. Algoritma yang digunakan untuk mengamankan file dokumen adalah kombinasi algoritma beaufort cipher dan hill cipher.
d. Aplikasi pada penelitian ini akan dikembangkan menggunakan perangkat lunak Android Studio.
e. Bahasa pemrograman yang digunakan untuk mengembangkan aplikasi adalah Java dan XML.

4.4 Tujuan Penelitian

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

a. Mengamankan sebuah file dokumen yang bersifat pribadi atau rahasia menggunakan teknik kriptografi.
b. Menerapkan dan mengkombinasikan algoritma beaufort cipher dan hill cipher dalam mengamankan file dokumen.
c. Membangun aplikasi berbasis mobile untuk digunakan dalam proses mengamankan file dokumen.

4.5 Manfaat Penelitian

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

a. Aplikasi yang dihasilkan pada penelitian ini dapat digunakan untuk mengamankan file dokumen.
b. File dokumen yang telah di amankan dapat mencegah tindakan pelanggaran privasi yang akan dilakukan oleh orang yang tidak berhak.