BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Kriptografi merupakan teknik yang digunakan dalam mengamankan informasi. Seperti yang diketahui bahwa keamanan informasi terdiri dari tiga buah bagian, *confidentiality*, *integrity*, dan *availability* yang juga dikenal sebagai CIA *triad*. Di mana untuk *confidentiality*, informasi tidak tersedia ke semua pihak, hanya pihak tertentu saja yang dapat mengakses. *Integrity* dari keamanan informasi adalah dengan memastikan data yang ada tidak dimodifikasi, data dalam bentuk utuh. Dan *availability* adalah data dapat diakses dan digunakan oleh pihak yang memiliki akses terhadap data tersebut. Selain *confidentiality* dan *integrity*, *authentication* dan *nonrepudiation* memiliki peran penting pada kriptografi [1].

Kriptografi terdapat dua macam, yaitu *polyalphabetic* dan *monoalphabetic*. Vigenere merupakan salah satu dari banyak macam *polyalphabetic cipher*. Dalam penggunaannya, Vigenere sudah dapat dipecahkan karena penggunaan *key* yang berulang sehingga memungkinkan ditemukannya huruf asli dari *cipher* tersebut. Salah satunya adalah metode Kasiski yang didasarkan pada *cipher* hasil dari huruf *plaintext* dan *key* menghasilkan *symbol* yang sama [2]. Terlebih lagi adanya huruf yang sering digunakan pada suatu bahasa, misal pada bahasa Inggris adalah huruf E, T dan A. Sedangkan pada bahasa Indonesia salah satunya adalah huruf A [3], [4].

Dengan perulangan dari *key* untuk mendapat panjang yang sama dengan *plaintext*, tidak menutup kemungkinan memunculkan karakter cipher yang bersifat *repetitive* atau berulang. Cipher *repetitive* tersebut dapat dianalisa untuk menemukan huruf asli. Hal ini yang dimanfaatkan oleh *cryptanalyst* untuk membongkar *ciphertext*. Selain itu dengan adanya *key* yang kemungkinan besar dapat tersebar juga membuat pihak ketiga mengetahui isi dari pesan tersebut.

1.2. Rumusan Masalah

Berdasar latar belakang masalah di atas, didapatkan sebuah masalah yang ingin peneliti ketahui jawabannya, yaitu sebagai berikut.

1. Dapatkah tingkat keamanan Algoritma Vigenere Cipher dikembangkan dengan perluasan karakter, kombinasi Caesar dan *shuffled key*?

1.3. Batasan Masalah

Batasan masalah yang ada dalam penilitian ini adalah sebagai berikut.

1. Pembuktian terbatas hanya menggunakan Index of Coincidence.
2. Objek yang di-*encrypt* terbatas dalam bentuk *text input* dan bukan *file*.
3. Karakter yang digunakan terbatas pada 95 karakter ASCII.

1.4. Tujuan Penelitian

Tujuan dari penelitian adalah untuk mengetahui seberapa amankah hasil *encryption* dengan menggunakan pengembangan Algoritma Vigenere Cipher yang diusulkan berdasarkan *value* dari Index of Coincidence.

1.5. Manfaat Penelitian

Penelitian ini sebagai salah satu sarana untuk memecahkan masalah terkait Vigenere Cipher. Selain itu penelitian ini diharapkan dapat menjadi salah satu referensi penelitian pengembangan Vigenere Cipher kedepannya, baik mengenai perkembangan lebih lanjut dari usulan peneliti mau pun penelitian terkait yang lain.

1.6. Sistematika Penulisan

Berikut rincian singkat dari sistematika penulisan hasil penelitian.

BAB I PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi studi literatur atau tinjauan pustaka terkait dengan penelitian, dan juga berisi dasar-dasar teori yang digunakan seperti apa itu kriptografi, Index of Coincidence, dan lain-lain.

BAB III METODE PENELITIAN, didalamnya terdapat tinjauan umum tentang

objek penelitian, alur penelitian, alat dan bahan untuk penelitian, serta parameter pengujian.

BAB IV HASIL DAN PEMBAHASAN, bab ini merupakan tahapan yang penulis lakukan dalam pembuatan aplikasi enkripsi-dekripsi dan IoC, *testing*, hingga pembuktian dengan menganalisis hasil perbandingan Index of Coincidence.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.