BAB I
PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi yang berkembang pesat di zaman ini memberikan banyak manfaat bagi masyarakat, yakni kecepatan untuk memperoleh informasi, ketepatan mencari data, dan kemudahan untuk berkomunikasi. Salah satu kemajuan yang sangat pesat adalah internet, internet merupakan suatu jaringan komputer yang saling terhubung secara global dengan menggunakan TCP/IP (*Transmission Control Protocol/Internet Protocol*) sebagai protokol pertukaran data. Namun tak segalanya kemajuan teknologi berdampak positif, hal tersebut juga memiliki dampak negatif dimana salah satunya adalah rawan terjadinya pencurian data, sehingga data yang dicuri bisa saja dimanfaatkan atau disalahgunakan oleh pihak lain tersebut, sehingga tentu saja dapat merugikan pengguna sebagai pemilik data tersebut.

Pencurian data dapat terjadi karena banyak hal, pertama dapat terjadi dikarenakan pengguna tidak memiliki anti-virus yang memadai untuk melindungi datanya, lalu yang kedua pengguna dengan ceroboh memberikan identitasnya kepada pihak lain, kemudian yang ketiga adalah karena data tersebut disadap saat melakukan pengiriman data di internet, dan yang keempat dapat terjadi karena pengguna tidak menyandikan atau mengenkripsi datanya ke bentuk lain.

Pada dasarnya data yang disadap tidak akan bisa digunakan jika sebelumnya datanya sudah disandikan atau dienkripsi terlebih dahulu. Tujuan data tersebut dienkripsi dimaksudkan, apabila ada pihak yang menyadap pengiriman data, pihak tersebut tidak akan mengerti isi data karena data yang penyadap dapatkan masih membutuhkan kata kunci, dengan demikian isi data yang sebenarnya dapat tetap terjaga. Oleh karena itu penting sekali data yang akan dikirim mulai disandikan atau dienkripsi terlebih dahulu, lalu oleh penerima yang berhak, data tersebut dikembalikan ke bentuk aslinya sehingga data tersebut dapat dibaca dan dimengerti oleh sang penerimanya. Ilmu yang mempelajari tentang

penyandian data, atau mengartikan data dari bentuk yang sukar dimengerti menjadi dapat dimengerti disebut dengan ilmu kriptografi.

Kriptografi (*cryptography*) secara etimologi berasal dari bahasa yunani, terdiri dari dua suku kata yaitu *kryto* dan *graphia*. *Kryto* artinya menyembunyikan sedangkan *graphia* artinya tulisan. Sehingga secara umum, kriptografi merupakan keahlian atau ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Kriptografi dapat pula diartikan sebagai cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data. Beberapa contoh aplikasi dari penggunaan kriptografi adalah ATM (Anjungan Tunai Mandiri), siaran televisi berbayar, komunikasi dengan telepon seluler, penggunaan sidik jari, dll.

Dalam dunia kriptografi, terdapat dua buah konsep utama, yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana pesan yang akan dikirim (*plaintext*) diubah terlebih dahulu menjadi bentuk yang tidak dapat dipahami (*ciphertext*) sehingga orang tidak akan dapat memahaminya tanpa bantuan pengetahuan khusus. Sedangkan dekripsi adalah kebalikan dari enkripsi, yaitu proses mengubah kembali pesan yang tidak dapat dipahami itu (*ciphertext*) menjadi pesan yang dapat dipahami (*plaintext*).

Pada saat proses ini dibutuhkan kunci, kunci tersebut digunakan dalam proses mengenkripsi dan mendekripsi pesan rahasia. Kunci ini pula yang menentukan apakah pesan tersebut bisa dibaca atau tidak, sehingga kerahasiaan kunci tersebut justru menjadi hal yang lebih krusial dan penting dari pada kerahasiaan pesan itu sendiri. Berdasarkan kerahasiaan kuncinya, kunci dibedakan menjadi dua buah, yakni *public key* dan *private key*. Sebuah kunci dikatakan *public key* jika kunci tersebut diinformasikan secara bebas dan digunakan tanpa kerahasiaan, sedangkan *private key* dikatakan jika kunci tersebut hanya bisa digunakan secara khusus dan tidak pernah diinformasikan kepada orang lain, sehingga kunci ini terjaga kerahasiaannya.

Terdapat beberapa metode penyandian yang sangat terkenal sejak dahulu , dimana salah satunya adalah sandi *vigenere*. Sandi *Vigenere* pertama kali

diperkenalkan oleh Giovan Batista Belaso dalam bukunya yang berjudul *La cifra del. Sig. Giovan Batista Belaso*. Sandi *vigenere* adalah metode enkripsi abjad teks dengan menggunakan deretan sandi caesar berdasarkan huruf-huruf yang terdapat pada kata kunci. Sandi *Vigenere* merupakan salah satu algoritma kriptografi simetri yang memiliki satu kunci yang akan digunakan pada proses enkripsi serta dekripsinya.

Pada zaman ini sudah banyak orang yang mengetahui sandi *Vigenere*, sehingga tak sedikit pula orang melakukan penelitian-penelitian mengenai sandi tersebut. Salah satu penelitian yang pernah dilakukan yakni berjudul "Penyandian *One Time Pad* dengan Menggunakan Sandi *Vigenere*" tahun 2014, dimana penelitian tersebut menitik beratkan pada penggabungan dua buah konsep sandi kriptografi. Namun penelitian tersebut memiliki sebuah kelemahan, yakni sandi *Vigenere* membutuhkan sebuah kunci, tentunya kunci tersebut sangat dijaga kerahasiannya, karena jika tidak dijaga, isi pesan aslinya akan mudah diketahui oleh pihak lain. Lalu seiring berkembangnya zaman sudah ada suatu metode yang dapat memecahkan sandi *Vigenere* tanpa harus mengetahui kuncinya yaitu yang pertama dengan menggunakan indeks koinsidensi untuk mencari panjang kata kuncinya, dan kedua menggunakan metode *Chi-Square* untuk menentukan kuncinya. Atas dasar itulah dalam skripsi ini akan dibahas mengenai bagaimana konsep yang digunakan *Chi-Square* dalam memecahkan sandi *vigenere*, tanpa terlebih dahulu mengetahui kata kuncinya.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan di atas, maka rumusan masalah pada skripsi ini adalah:

1. Bagaimana penggunaan indeks koinsidensi dan metode *Chi-Square* dalam memecahkan sandi *vigenere*?
2. Bagaimana membuat program aplikasi untuk memecahkan sandi *vigenere*?
3. Bagaimana akurasi indeks koinsidensi dan metode *Chi-Square* dalam memecahkan sandi *vigenere*?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah diuraikan di atas, maka skripsi ini bertujuan untuk memberikan gambaran mengenai:

1. Mengetahui penggunaan indeks koinsidensi dan metode *Chi-Square* untuk mencari kunci dalam memecahkan sandi *vigenere*.
2. Mengetahui membuat program aplikasi untuk memecahkan sandi *vigenere*.
3. Mengetahui akurasi metode *Chi-Square* dalam memecahkan sandi *vigenere*.

1.4. Batasan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka perlu dibatasi permasalahan dalam skripsi ini, yakni pengambilan *ciphertext* dan *plaintext* hanya dalam bahasa inggris, dan panjang kunci yang telah diketahui maksimal panjangnya 5 satuan.

1.5. Manfaat Penelitian

Manfaat dari penulisan skripsi ini diharapkan dapat memberikan pengetahuan tentang konsep matematis metode *Chi-Square* dalam memecahkan sandi *vigenere*, dan selain itu program aplikasinya nantinya dapat digunakan untuk menyandikan data-data rahasia.