BAB I

PENDAHULUAN

1.1. Latar Belakang Penelitian

Keamanan termasuk salah satu bagian yang penting dalam sebuah sistem informasi. Masih banyak yang tidak tahu bagaimana cara mengamankan berkas yang dibuat atau diterimanya atau tidak tahu bagaimana cara melindungi berkas yang dibuat atau diterimanya agar tidak terjadi pencurian berkas yang menyebabkan bocornya informasi dari berkas tersebut. Kriptografi merupakan suatu ilmu yang mempelajari bagaimana cara menjaga keamananan suatu pesan (*plaintext*). Tugas atau fungsi utama dari kriptografi adalah untuk menjaga agar pesan serta kunci tetap terjaga keamanan dan kerahasiaannya dari para penyadap (*attacker*).

Vigenere cipher adalah *cipher* blok polialfabetik, tetapi jika dilihat dengan cara lain, ini adalah *stream cipher* yang merupakan generalisasi alami dari sandi geser (Smart, 2013). *Vigenere cipher* adalah salah satu bentuk pengembangan dari *caesar cipher*. Keunggulan dari sandi ini dibanding *caesar cipher* dan *cipher* polialfabetik lain adalah *cipher* ini tidak begitu rentan terhadap metode pemecahan *cipher* yang biasa disebut sebagai analisis frekuensi. *Cipher* ini juga dikenal dikhalayak ramai karena cara kerjanya yang cukup mudah untuk dimengerti dan dioperasikan penggunaanya, dan bagi para pemula sandi ini cukup sulit untuk dipecahkan. Pada saat kejayaannya, dalam Bahasa prancis *cipher* ini dijuluki *le chiffre indechiffrable* yang artinya *cipher* yang tak terpecahkan.

Kemudian metode untuk pemecahan *cipher* ini baru ditemukan sekitar abad ke-19. Tahun 1854, Charles Babbage yang disebut sebagai *Father of Computer* akhirnya menemukan cara untuk memecahkan *vigenere cipher*. Metode ini kemudian dikenal dengan nama metode kasiski karena Friedrich Kasiski-lah yang pertama mempublikasikan metode ini ke publik. Berbeda dengan *caesar cipher* yang setiap huruf harus digeser dengan besar geseran yang sama, pada *vigenere cipher* ini setiap huruf harus digeser dengan besar yang berbeda sesuai dengan kuncinya. Untuk menjaga keamanan dari *file*, *file* tersebut dapat di lakukan enksipsi dan juga deskripsi. Enkripsi dan dekripsi umumnya membutuhkan sejumlah informasi rahasia, atau yang biasanya disebut sebagai kunci.

Pada penelitian ini penulis menemukan adanya permasalahan di PT. Pioneer Offshore Indo Raya. Penulis menemukan adanya masalah keamanan pada *file* penting perusahaan yang tidak diamankan dengan baik. *File* penting yang harus dijaga kerahasiannya, seperti dokumen perusahaan, dokumen pribadi dan lainnya. Sehingga mengharuskan karyawan untuk lebih waspada ketika *file* tersebut diambil oleh orang yang tidak bertanggung jawab. *File* ini bisa saja dicuri dan diubah oleh orang yang ingin mengetahui rahasia perusahaan melalui jaringan atau wifii yang sama. Sehingga diperlukan perangkat lunak yang bisa menjaga kerahasiaan dan keamanan dokumen tersebut. khususnya untuk pekerja kantor agar dapat diterima dengan aman dari pengirimnya.

Penelitian ini sudah pernah ada yang dilakukan oleh (Purnama, 2014) membahas tentang pengamanan pesan melalui kriptografi *vigenere cipher* dengan kunci berlapis. Dalam kesimpulannya berisi ” Penggunaan kunci berlapis pada

pengamanan pesan melalui metode *vigenere cipher* dapat menkan kelemahan yang terjadi pada metode *vigenere cipher*, khususnya jika kita menggunakan metode kasiski. Namun *cryptanalyst* mengetahui terlebih dahulu mengetahui lapisan kunci yang digunakan maka metode ini masih ada kemungkinan bisa dipecahkan". Dalam penelitian yang dilakukan oleh (Hendro Eko Prabowo dan Arimaz Hangga, 2015). Membahas tentang enkripsi teks menggunakan metode modifikasi *Vigenere Cipher*. Dari kesimpulannya berisi " metode *vigenere cipher* sendiri memiliki pengulangan kata pada *final key* yang membuat ini pesan tersebut dapat ditebak atau diprediksi. Sedangkan metode modifikasi *vigenere cipher* tidak memiliki pengulangan kata pada *final key* sehingga informasi pesan tidak dapat diprediksi. Pada metode *vigenere cipher* memiliki nilai peluang terbesar informasi dapat diprediksi sebesar 74,07 %. Kelebihan algoritma modifikasi *vigenere cipher* adalah hasil enkripsi tidak memiliki pola perulangan huruf atau kata". Penelitian lain yang dilakukan oleh (Amrulloh & Ujianto, 2019). Berisi tentang " aplikasi hasil pengembangan memiliki kesesuaian dengan hasil *test* manual menggunakan tabel vigenere cipher sedangkan pada aplikasi online ditemukan ketidaksesuaian pada perulangan kata kunci dan *ciperteks*.". Ada juga penelitian yang telah dilakukan oleh (Firmansyah, 2019) yang membahas masalah kriptografi algoritma *RSA* menggunakan metode *waterfall* berbasis java dalam penelitiannya mengungkapkan bahwa kriptografi *RSA* ini cukup aman, karena kunci *RSA* tidak asal dibuat. Hasil dari kriptografi ini juga cukup membingungkan bagi pembaca yang tidak mempunyai kunci dekripsi, karena yang dihasilkan hanya berupa bilangan bulat.

Pada tugas akhir ini, penulis akan mambuat perangkat lunak kriptografi *vigenere cipher*. Perangkat lunak ini akan mengamankan *file* dokuman PT. Pioneer Offshore Indo Raya berformat **.pdf, *.xls, *.doc, dan *.txt*. Dari latar belakang yang telah dijelaskan tersebut penulis akan melakukan penelitian dengan judul **"PERANGKAT LUNAK KEAMANAN BERBASIS *FILE* MENGGUNAKAN ALGORITMA KRIPTOGRAFI *VIGENERE CIPHER*".**

1.2. Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, berikut ini identifikasi masalah yang dapat diambil adalah :

1. Kurangnya pengguna dalam mengamankan *file* menggunakan algoritma kriptografi *vigenere cipher.*
2. Kurangnya pengetahuan *user* akan pentingnya keamanan sebuah data.
3. Kurangnya pengetahuan *user* terhadap kriptografi *vigenere cipher.*

1.3. Pembatasan Masalah

Agar penelitian bisa lebih focus dan terarah, maka penulis perlu membatasinya agar pembahasan menjadi tidak terlalu luas. Adapun pembatasan masalah pada penelitian ini adalah :

1. Jenis data yang digunakan adalah *file* teks *(*.txt, *.pdf, *.xls dan *.doc).*
2. Proses mengamankan *file* meliputi proses enkripsi *file* menggunakan perangkat lunak dengan algoritma kriptografi *vigenere cipher*.

3. Proses mengamankan *file* meliputi proses dekripsi *file* menggunakan perangkat lunak dengan algoritma kriptografi *vigenere cipher*.

4. Bahasa pemrograman yang akan digunakan adalah bahasa pemrograman *java*.

1.4. Perumusan Masalah

Berdasarkan latar belakang di atas, maka yang menjadi rumusan masalah pada penelitian ini adalah :

1. Bagaimana cara mengamankan *file (*.txt, *.pdf, *.xls dan *.doc)* menggunakan algoritma kriptografi *vigenere cipher* ?.

2. Bagaimana merancang perangkat lunak sistem enkripsi dan dekripsi algoritma kriptografi *vigenere cipher* menggunakan pemrograman *java*?

1.5. Tujuan Penelitian

Berdasarkan pada rumusan masalah yang diuraikan sebelumnya, maka tujuan penelitian ini adalah :

1. Mengamankan *file (*.txt, *.pdf, *.xls dan *.doc)* menggunakan algoritma kriptografi *vigenere cipher* ?

2. Merancang perangkat lunak sistem enkripsi dan dekripsi algoritma kriptografi *vigenere cipher* menggunakan pemrograman *java*.

1.6. Manfaat Penelitian

Adapun manfaat dari penelitian yang akan didapatkan dari penelitian ini terdiri dari 2 aspek yaitu:

1.6.1 Aspek Teoritis

Manfaat dari aspek praktis yang diharapkan dari dilakukannya penelitian ini antara lain :

1. Menberikan wawasan pengetahuan tentang keuntungan *file* yang sudah terenkripsi dengan algoritma kriptografi *Vigenere Cipher*.
2. Diharapkan juga penelitian ini dapat menjadi masukan maupun bahan referensi untuk melakukan penelitian yang berhubungan dengan sistem keamanan *file* dengan kriptografi *Vigenere Cipher*.
3. Diharapkan penelitian ini juga kelak dapat menjadi buku referensi dan informasi bagi mahasiswa yang membutuhkan informasi mengenai dengan sistem keamanan *file* dengan kriptografi *Vigenere Cipher*.

1.6.2 Aspek Praktis

Manfaat dari aspek praktis yang diharapkan dari diadakanya penelitian ini adalah :

1. Dapat membantu masalah keamanan data berupa *file*, sehingga *file* tetap dapat terjaga kerahasiaan dan keutuhannya.
2. Dapat menjadi pertimbangan bagi organisasi atau perusahaan untuk menjaga *file* pentingnya.