BAB I PENDAHULUAN

A. Latar Belakang

Pada masa ini komputer merupakan salah satu kebutuhan bagi semua orang. Komputer bukan hal yang langka, hampir semua kalangan pelajar, mahasiswa, pekerja, pengusaha, bahkan pengajar pun mengenal dan menggunakan komputer. Komputer banyak digunakan sebagai media pencarian informasi, untuk menyelesaikan tugas bagi pelajar. Memproses jual beli serta menginput data barang bagi pekerja. Mempermudah pendataan dengan aplikasi maupun sistem yang terdapat pada komputer.

Setiap penggunaan komputer terdapat informasi yang harus dijaga, informasi tersebut dalam bentuk data. Komputer sangat membutuhkan media penyimpanan data agar dapat tersimpan. Media utama penyimpanan data pada komputer adalah *harddisk*. *Harddisk* merupakan penyimpanan permanen yang dapat menjaga data agar tetap ada dan aman. Walaupun penyimpanan dalam *harddisk* bersifat permanen, tidak menutup kemungkinan terjadi kerusakan dan kehilangan data.

Banyak persoalan-persoalan hilang atau rusaknya data terjadi karena serangan virus. Salah satunya pada sebuah perusahaan terdapat serangan virus yang berjenis *ransomware* dimana serangan virus yang sengaja disebarkan oleh *hacker* dengan cara mengenkripsi data komputer membuat semua data yang ada didalamnya terkunci. Hanya *hacker* yang mengetahui kunci dari data tersebut dan meminta sejumlah uang dalam bentuk notepad. Virus ini tersebar melalui internet, dan dilampirkan di email dalam bentuk link atau tautan.

Ransomware adalah perangkat lunak yang menemukan semua file didalam komputer dan mengenkripsinya serta kemudian meninggalkan pesan untuk pengguna. Jika pengguna ingin memperoleh kembali akses ke data-data milik pengguna, maka pengguna harus membayar tebusan (Peter Reiher, 2017).

Dalam hal ini, tempat objek penelitian memiliki tingkat keamanan yang lemah menyebabkan terserangnya data pengguna maupun data lama dari virus yang telah menyebar. Oleh karena itu, dibutuhkannya keamanan yang lebih baik dalam penyimpanan dan *backup* data.

Security & Trust dalam ilmu komputer merupakan suatu teknologi dalam mengamankan informasi berbentuk data yang ada didalam komputer. Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau jaringan yang tidak bertanggung jawab (Howard, 1998).

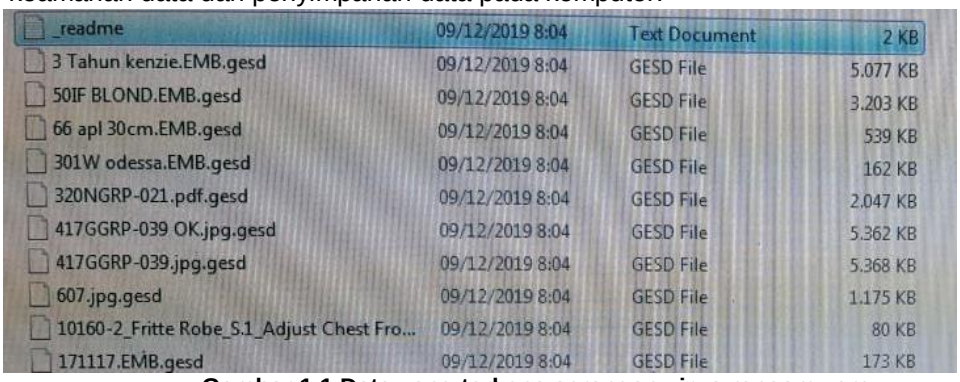
Ruang lingkup untuk sistem keamanan komputer terdapat istilah kriptografi sebagai ilmu yang mempelajari teknik matematika yang menjaga kerahasiaan data dengan cara mengubah data kedalam bentuk yang tidak mempunyai makna.

Kriptografi terdapat dua jenis yaitu simetris dan asimetris. Yang akan digunakan dalam penelitian ini yaitu *cipher* subtitusi yang termasuk dalam kriptografi simetris. *Cipher* subtitusi mengantikan *plaintext* dengan karakter lain sesuai dengan yang ditetapkan, salah satunya *Affine Cipher* yang menjadi pengembangan dari *Caesar Cipher* bekerja dengan mengalikan *plaintext* dengan sebuah nilai dan menambahkan dengan sebuah pergeseran. *Affine Cipher* memiliki beberapa kelebihan diantaranya teknik algoritma kriptografi yang sederhana, mudah untuk digunakan, perluasan dari *Caesar Cipher* sehingga membuat informasi lebih sulit untuk dipecahkan oleh peretas.

Oleh karena itu, dalam penelitian ini dilakukan keamanan data *storage* yang menggunakan *Affine Cipher* sebagai penerapan metode kriptografi.

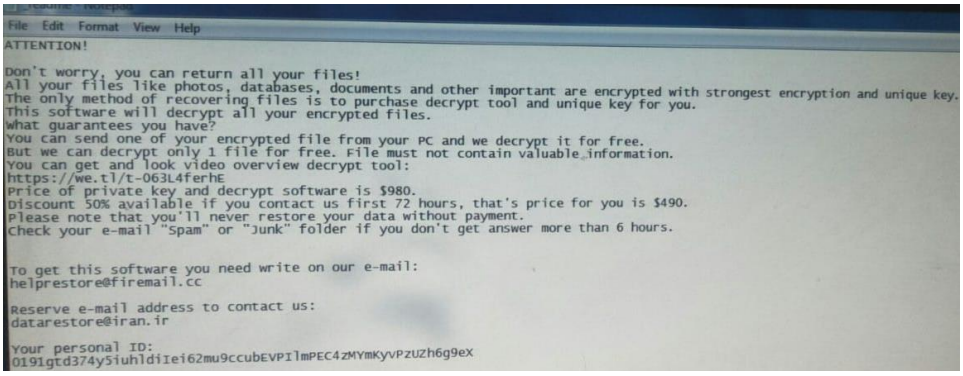
B. Permasalahan

Dari hasil yang dilakukan pada tempat objek penelitian, diketahui bahwa terdapat masalah yaitu terkuncinya data komputer sehingga user tidak dapat mengakses data tersebut dan media penyimpanan yang terbatas menyebabkan komputer tidak memiliki *backup*. Dalam hal ini permasalahan terdapat pada keamanan data dan penyimpanan data pada komputer.



Gambar 1.1 Data yang terkena serangan virus ransomware

Gambar 1.1 menunjukkan data komputer user yang terenkripsi dan terkunci dalam bentuk format GESD sehingga tidak dapat diakses atau dibuka.



Gambar 1.2 Notepad berisi peringatan dari *Hacker*

Gambar 1.2 menunjukkan pesan yang diberikan oleh *hacker* kepada pengguna komputer sebagai panduan bagaimana cara membuka data yang sudah terkunci atau terkena *brute force attack* dengan meminta mengirimkan sejumlah uang.

Biaya media penyimpanan yang mahal menjadi kendala dalam mencadangkan data di perusahaan tersebut, sehingga saat ini masih menggunakan penyimpanan data yang hanya mengandalkan *harddisk* pada setiap komputer. Lemahnya antivirus menjadi kendala dalam keamanan data di perusahaan tersebut, sehingga saat ini masih menggunakan *firewall* sistem operasi dan kurangnya pertahanan antivirus setiap komputer.

Berdasarkan permasalahan yang telah didefinisikan, maka diidentifikasi masalah yaitu:

1. Identifikasi Masalah

a. Lemahnya keamanan data pada komputer yang terhubung dengan jaringan.
b. Belum efektifnya pengamanan dalam penyimpanan data.

2. Pernyataan Penelitian (*Problem Statement*)

Berdasarkan identifikasi masalah maka dapat disimpulkan pokok masalah yaitu lemahnya keamanan dan belum efektifnya pengaman data *storage*.

3. Pertanyaan Penelitian (*Research Question*)

a. Bagaimana penerapan *Affine Cipher* untuk meningkatkan keamanan data *storage*?
b. Berapa tingkat efektifitas penerapan *Affine Cipher* untuk meningkatkan keamanan data storage?

C. Maksud dan Tujuan Penelitian

Maksud dari penelitian ini adalah menerapkan *Affine Cipher* untuk meningkatkan keamanan data *storage.*

Tujuan dari penelitian ini adalah

a. Meningkatkan pengamanan data dengan pendekatan *Affine Cipher*.
b. Mendapatkan pengamanan *data storage* yang lebih efektif.
c. Mengembangkan *prototype* aplikasi pengamanan *data storage*.
d. Mengukur tingkat ketercapaian peningkatan keamanan dan efektifitas pengaman *data storage*.

D. Spesifikasi Produk yang Diharapkan

Melalui penelitian ini diharapkan terciptanya produk berupa proses dan pengembangan sistem keamanan untuk data storage pada perusahaan:

1. Aplikasi digunakan untuk menyimpan data dalam bentuk enkripsi.
2. Aplikasi digunakan untuk berbagi data dengan aman.
3. Menjadikan data *user* terpusat.
4. Mengontrol data yang tersimpan didalam server data melalui jaringan yang menggunakan *user* autentikasi untuk aksesnya.

E. Signifikansi Penelitian

Pentingnya penelitian ini dilakukan dalam rangka mengembangkan penerapan teknik komputasi pemodelan *Affine Cipher* untuk meningkatkan keamanan data jaringan. Adapun manfaat dari penelitian ini, yaitu:

1. Manfaat teoritis dari penelitian ini yaitu memberikan sumbangan ilmu pengetahuan mengenai penerapan *Affine Cipher.*
2. Manfaat praktis dari penelitian ini yaitu membantu pengguna dalam pengamanan *data storage*.
3. Manfaat kebijakan penelitian ini yaitu dapat dijadikan acuan dalam pengelolaan keamanan data pada komputer yang terhubung ke jaringan.

F. Asumsi dan Keterbatasan

Asumsi dari penelitian ini adalah sebagai berikut:

1. Dengan adanya penelitian ini dapat memudahkan pengguna dalam menyimpan data dengan teratur dan terpusat.
2. Metode Affine Cipher dapat mengamankan data yang terdapat pada aplikasi dalam meningkatkan efektifitas proses penyimpanan data perusahaan.

Keterbatasan dari penelitian ini adalah sebagai berikut:

1. Aplikasi digunakan hanya untuk menyimpan dan mengunggah data yang terdapat pada perusahaan.
2. Apllikasi hanya bisa diakses melalui jaringan internal perusahaan.
3. Menggunakan pc server sebagai media penyimpanan data.

G. Definisi Istilah atau Definisi Operasional

1. *Backup* = proses membuat cadangan data dengan cara menyalin dan mengarsipkannya agar bisa diambil kembali sewaktu-waktu data tersebut dibutuhkan.
2. Subtitusi = pergantian atau menggantikan.
3. *Harddisk* = perangkat keras komputer yang berfungsi sebagai tempat penyimpanan data.
4. *Plaintext* = teks biasa yang dapat terbaca sebelum dienkripsi.
5. *Hacker* = orang yang mempelajari, menganalisis, memodifikasi, serta menerobos masuk ke dalam sistem komputer dan jaringan komputer, baik untuk keuntungan pribadi atau dimotivasi oleh tantangan.
6. *Ransomware* = virus komputer berjenis malware yang bekerja mengunci data sehingga tidak dapat diakses oleh pengguna.
7. *Security&Trust* = suatu teknologi dalam mengamankan informasi berbentuk data didalam komputer.
8. *Brute force attack*= sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin.
9. *Firewall* = suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal.
10. Antivirus = software yang berguna untuk mendeteksi dan menghapus file yang dianggap sebagai virus.