BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi jaringan komputer bukan hanya membuka banyak peluang dalam pengembangan aplikasi komputer. Namun, juga membuat adanya ancaman terhadap pengubahan dan pencurian data (Rifki, 2012). Tahun 2018, jumlah data yang dicuri atau diretas sebanyak 4,5 miliar data berdasarkan laporan perusahaan keamanan *Gemalto.* Pada 2018, jumlah kasus pencurian data sebanyak 945 kasus. Sementara, pada 2017 kasus pencurian data mencapai 1.162 kasus. *Gemalto* melaporkan, jumlah data yang dibobol per harinya mencapai 6,9 juta data. Hal ini berdasarkan laporan pencurian data sejak tahun 2013 hingga tahun 2018 yang jumlahnya sebanyak 14,6 miliar. Hal yang menyedihkan, hanya 4% dari jumlah tersebut yang dilindungi *enkripsi* oleh pemiliknya. Jika dihitung secara statistik, jumlah data yang hilang paling banyak berasal dari perusahaan media *social* sebanyak 56,11% diikuti data milik instansi pemerintah dengan persentasi 26,62% dari keseluruhan data yang dibobol. *Gemalto* mengklasifikasi, tipe pelanggaran data yang ada, antara lain adalah pencurian data (64,55%), akses akun (17,47%), akses finansial (13,02%), berbagai gangguan, hingga data eksistensial (Liputan 6, 2018).

Perlindungan data terhadap akses, pengubahan yang dilakukan oleh pihak yang tidak berwenang perlu ditingkatkan. Untuk mewujudkan layanan keamanan jaringan komputer dapat menggunakan mekanisme keamanan jaringan yang direkomendasikan oleh ITU-T (X.800). Salah satu mekanisme keamanan jaringan yaitu *encipherment*. *Encipherment* merupakan mekanisme keamanan jaringan

untuk menyembunyikan data yang menyediakan layanan kerahasiaan data (*confidentiality*). Salah satu teknik yang digunakan untuk mewujudkan mekanisme *encipherment* yaitu kriptografi (Rifki, 2012).

Seiring berkembangnya teknik penyandian pesan dengan metode kriptografi. Beberapa peneliti melakukan kombinasi beberapa metode untuk meningkatkan keamanan pada teknik penyandian pesan. Hal ini karenakan proses kriptografi akan sangat baik jika dikombinasikan dengan metode lain (Putri, Putera, & Siahaan, 2018). Seperti yang dilakukan oleh Putri dan Siahaan pada tahun 2018 menggunakan metode *gronsfeld* dan *vigenere* pada *Three-Pass Protocol Scheme*. Implementasi *gronsfeld* dan *vigenere* dengan kode ASCII pada *Mod* 256. Hasil penelitian ini mengungkap bahwa keamanan informasi lebih baik dengan kombinasi kriptografi *Gronsfeld* dan *Vigenere* yang diimplementasikan pada konsep *Three-Pass Protocol Scheme* (Putri et al., 2018).

Metode *vigenere* juga pernah dikombinasikan dengan beberapa metode kriptografi lainnya seperti *beaufort vigenere* (Ignatius et al., 2018). 4 kriptografi berlapis lainnya yaitu *caesar, transposisi, vigenere* dan *blok chiper* (Basuki, Paranita, & Hidayat, 2016). *Vigenere transposisi* (Pradipta, 2016).*Vigenere transposis* kolom (Sinaga & Chaerul, 2018). *Caesar vigenere* (Zuli & Irawan, 2014). Modifikasi tersebut menghasilkan kualitas *dekripsi* yang lebih baik. Sehingga teks sandi (*ciphertext*) yang dihasilkan lebih sulit untuk dipecahkan.

Kriptografi *vigenere* merupakan kriptografi klasik yang populer dan mudah digunakan (Putri et al., 2018) (Andhika, 2011). Sehingga, kriptografi klasik sering diretas oleh penyerang dan algoritma kriptografi klasik rentan terhadap serangan

pada kunci (Putri et al., 2018). Metode kriptografi klasik termasuk kriptografi yang aman digunakan pada zamannya. Apabila metode tersebut digunakan pada masa sekarang, maka sudah tidak efektif lagi karena zaman komputasi dapat mengetahuinya dengan cepat (Latifah, Ambo, & Kurnia, 2017).

Berbagai jenis sandi algoritma kriptografi telah ditemukan oleh ahli kriptografi, begitu juga dengan penyerang (*cracker)* telah melakukan banyak usaha untuk memecahkan sandi algoritma kriptografi yang telah diciptakan. Hal ini mendorong para *cryptographers* untuk menciptakan algoritma yang lebih sulit dan aman (Latifah et al., 2017).

Berdasarkan hal tersebut penelitian ini membahas kemananan jaringan dengan teknik penyandian pesan menggunakan kriptografi sandi berlapis. Sandi berlapis dalam penelitian ini dengan mengkombinasikan metode *vigenere* dan *gronsfeld* yang merupakan pengembangan dari kriptografi *vigenere*. Sehingga dalam implementasinya menggunakan dua kunci. Kunci pertama karakter huruf dan kunci kedua karakter angka.

1.2 Perumusan Masalah

Adapun rumusan masalahan dalam penelitian ini diantaranya :

1. Bagaimana hasil penerapan kombinasi metode *vigenere* dan *gronsfeld* untuk meningkatkan keamanan dalam sandi berlapis?
2. Bagaimana perbandingan hasil enkripsi dan dekripsi pada metode *vigenere* dan *gronsfeld* secara masing-masing dan bersamaan ?

1.3 Batasan Masalah

Adapun batasan dalam penelitian ini yaitu :

1. Menggunakan dua metode kriptografi klasik yaitu *vigenere* dan *gronsfeld* dengan perhitungan *mod* 26
2. Menggunakan teks dalam format huruf kapital dari A sampai Z tanpa spasi
3. Menggunakan kunci *vigenere* dalam format huruf kapital A sampai Z tanpa spasi
4. Menggunakan kunci *gronsfeld* dalam format angka dari 0 sampai 9 tanpa spasi
5. Menggunakan kunci simetrik pada metode *vigenere* dan *gronfeld*
6. Jumlah maksimum untuk plainteks adalah 255 karakter.

1.4 Tujuan Penelitian

Adapun tujuan dalam penelitian ini diantaranya :

1. Mengetahui hasil penerapan kombinasi metode *vigenere* dan *gronsfeld* untuk meningkatkan keamanan dalam sandi berlapis.
2. Mengetahui perbandingan hasil enkripsi dan dekripsi pada metode *vigenere* dan *gronsfeld* secara masing-masing dan bersamaan.

1.5 Manfaat Penelitian

Adapun manfaat dalam penelitian ini antara lain:

1. Pertukaran data dan informasi menjadi lebih aman.
2. Keamanan penyandian pesan dengan teknik kriptografi sandi berlapis menjadi lebih baik.
3. Penyerang lebih sulit untuk memecahkan *chipertext* sandi berlapis dengan hasil yang lebih acak.
4. Penggunaan lebih mudah dalam melakukan penyandian pesan menggunakan kriptografi *vigenere* dan *gronsfeld* dengan adanya sistem yang dibangun.