BAB I

PENDAHULUAN

1.1 Latar Belakang

Berbagi kabar, bertukar informasi, menambahkan informasi, berinteraksi dengan manusia lain, dan sejenisnya, adalah proses yang kita kenal dengan istilah pengiriman pesan. Untuk melakukan proses pengiriman pesan adalah metode yang paling mudah untuk saling bertukar informasi kesesama manusia lainnya. Banyak faktor yang mendukung dan membelakangi mengapa pengiriman pesan terus terjadi. Dalam bidang psikologi menurut seorang ahli bernama *Homo ludens* Mengatakan bahwa komunikasi dipengaruhi oleh psikologi humanistik yang menyatakan bahwa manusia adalah pelaku aktif dalam interaksi dengan lingkungannya. Sehingga dapat diambil hipotesis bahwa pengiriman pesan dalam menyampaikan informasi akan dan tetap terus terjadi sampai kedepannya.

Manusia telah berikirim pesan sejak dari zaman dahulu, Dimulai sejak proses pertukaran informasi dalam bentuk primitif, bahkan sampai dimasa modern yang membawa segala aspek kehidupan ketingkat yang lebih canggih. Dalam contoh metode pengiriman pesan secara primitif, salah satunya dikenal dengan teknik penyampaian pesan yang digunakan oleh suku *Navajo*, penduduk asli Amerika (suku indian) (TribalDirectory, 2016). Mereka menggunakan api yang diatur asapnya agar dapat dikumpulkan dan dilepaskan diudara dan membentuk

sebuah pola asap tertentu yang merupakan sebuah cara penyampaian pesan pada anggota suku yang lain agar dapat berkomunikasi.

Seiring dengan perkembangan waktu, mulai dirasakan kebutuhan akan sebuah kerahasiaan dari pesan – pesan yang akan dikirimkan, agar tidak dapat diketahui isinya oleh pihak yang tidak berhak mengetahuinya. Tidak semua orang berhak untuk mengetahui pesan yang bersifat privasi, sensitif dan sangat rahasia. Oleh karena itu, pengiriman pesan dalam penyampaian informasi harus diberlakukan dengan sangat khusus dengan menggunakan metode khusus pula. Dapat dibayangkan jika sebuah perusahaan besar yang sedang melakukan transaksi melalui media *online* karena letak perbedaan geografis berbeda dan dalam keadaan mendesak, ternyata transaksinya sedang di dengarkan juga oleh peretas (*Hacker*) dan dijual informasinya pada perusahaan saingan, sehingga perusahaan saingan tersebut dapat memanfaatkan informasi tersebut untuk membuat perusahaan tersebut kalah produksi dan mengalami kerugian.

Itu semua dapat terjadi karena kurangnya metode keamanan dalam pengiriman dan penyampaian pesan yang dipakai. Salah satu kasus kebocoran informasi yang terjadi di negara Indonesia, tepatnya setelah pernyataan Marciano Norman, yang saat itu sedang menjabat sebagai kepala satuan Badan Intelijen Negara (BIN). Marciano mengatakan bahwa "Penyadapan ini memang yang terbuka dari 2007-2009, Tetapi dari informasi yang kita terima bahwa ada data – data yang terjadi pelanggaran pada kurun waktu itu", beliau mengklarifikasi bahwa telah terjadi penyadapan dari pihak aparat Intelijen Australia terhadap

presiden yang bertugas pada saat itu yaitu Susilo Bambang Yudhoyono, istrinya Ani yudhoyono, dan beberapa pejabat lainnya (BBC, 2013).

Metode untuk menjaga kerahasiaan pesan ini bernama metode enkripsi. yang merupakan metode dimana dilakukan upaya – upaya memanipulasi pesan sehingga pesan tersebut akan terlihat seperti kumpulan teks yang tidak ada artinya. Apabila pembaca tidak tau cara membacanya, Atau Menurut Wahana & Andi "Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca)".

Bermula pada tahun 1900 sebelum masehi, cendikiawan mesir menggunakan *Hieroglyph* yang tidak biasa pada prasasti mereka. Dan ini disebut oleh kahn dalam bukunya *The Codebrekaer* sebagai sebuah dokumen dengan kriptografi pertama (Khan, 1967). Kemudian *Glovan* metode penyajian teks alphabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf – huruf pada kata kunci. Selanjutnya pada tahun pada sekitar tahun 725-790 sebelum masehi, Abu 'Abdul-Rahman al-Khalil ibnu Ahmad' Amr ibn Tammam al-Farahid ibn al-Zadi al-Yahmadi telah menuliskan sebuah buku terkait kriptografi yang terinspirasi dari kriptogram Yunani yang sering dipakai pada masa kerajaan *byzantine,* yang kemudian oleh ahli pemecah kriptografi untuk membongkar mesin enigma (Jackob, 2020). Mesin Enigma sendiri adalah alat enkripsi yang berbentuk seperti koper dengan isi berupa motor mekanis listrik dan diadopsi oleh kebanyakan Negara yang ikut perang dunia kedua seperti Jerman, Jepang, dan

Italia dalam menyampaikan pesannya agar tidak mudah diketahui oleh pihak musuh.

Teknik enkripsi hadir disaat masa klasik dimana semua pesan masih diubah ke dalam bentuk *ciphertext* yang dituliskan diatas kertas, hingga masa kini yang sudah serba dibumbui penggunaannya dengan teknologi. Manusia modern kini hidupnya dipenuhi dengan *smartphone* yang memiliki kedudukan sebagai alat primer pemuas kebutuhnnya. Menurut data lembaga penghitung digital, akan ada 2,53 milyar total manusia pengguna smartphone ditahun 2018 ini (Statista.com, 2020). Namun sepertinya kenyataan ini juga tidak menggeser penggunaan dari *desktop* PC dan *Notebook* yang sudah melegenda kebutuhan pemakaiannya. Pemakaian *desktop* PC dan *Notebook* tetap bertambah dan tidak mengalami penurunan karena meskipun *smartphone* sudah menjamur, masih banyak hal yang lebih nyaman dikerjakan menggunakan *desktop* maupun *Notebook* pada beberapa kondisi dan waktu tertentu. Sehingga, keamanan dari pengiriman pesan baik secara messenger maupun *email* akan sangat diperlukan agar setiap informasi yang keluar, baik itu bersifat privasi maupun tidak, dapat sampai kepada pihak yang memang menjadi tujuan pesan itu tanpa bocor kepada pihak lain. Bocor dalam konteks ini tidak selalu dalam artian peretasan digital, *Desktop* dan *Notebook* biasanya bisa saja dipinjamkan kepada pihak yang pemiliknya sudah dipercayai. Seperti kerabat, keluarga, maupun pihak berwajib. Untuk mencegah informasi tertentu yang dimiliki pesan tersebut dapat diketahui orang lain, maka penulis berkeinginan untuk mengajukan penelitian berupa pembuatan aplikasi yang dapat melakukan enkripsi pesan menggunakan metode *vigenere* dan

menggunakan algoritma *three transposition VC* yang berbasis *Windows desktop* sebagai solusi masalah yang ada ini dengan judul "**Impelementasi Algoritma *Three Transposition Vigenere cipher* Dalam Pengamanan komunikasi Internal Berbasis Dekstop** ".

1.2 Identifikasi masalah

Berdasarkan latar belakang yang sudah dikemukakan sebelumnya, maka identifikasi masalah yang akan dijadikan bahan pembuatan skripsi adalah sebagai berikut :

1. Terjadinya kebocoran informasi terhadap pesan teks yang ingin disampaikan.
2. Isi pesan teks yang diketahui oleh pihak lain selain tujuannya sangat beresiko tinggi.
3. Banyak orang yang menyampaikan pesan sensitif tanpa perlindungan enkripsi.

1.3 Pembatasan masalah

Agar pembuatan penelitian skripsi ini akan terarah dan sesuai tujuan, maka akan dibatasi masalahnyanya pada :

1. pembuatan aplikasi enkripsi berbasis *windows* desktop
2. perancangan program mengggunakan PHP
3. metode *vigenere* yang digunakan adalah algoritma *three transposition*
4. enkripsi hanya terjadi pada angka dan huruf
5. aplikasi berguna sebagai *plain-text* menjadi *ciphertext,* begitu sebaliknya.

1.4 Perumusan masalah

Berdasarkan penjelesan latar belakang diatas, maka akan dirumuskan masalahnya berupa :

1. Bagaimana cara merancang aplikasi berbasis *Three transposition vigenere cipher*?
2. Bagaimana Algoritma *Three transposition vigenere cipher* bekerja?
3. Bagaimana implementasi *Three transposition vigenere cipher* untuk melindungi pesan?

1.5 Tujuan Penelitian

Berdasarkan dengan apa yang sudah dijelaskan sebelumnya, maka tujuan penelitian ini antara lain adalah :

1. Menerapkan metode *vigenere cipher* dalam mengenkripsi pesan teks
2. Membuktikan bahwa enkripsi klasik masih bermanfaat

1.6 Manfaat penelitian

Manfaat dari penelitian ini merupakan imbas positif yang dapat dirasakan oleh pihak tertentu atas dilakukannya penelitian ini setelah selesai nantinya. Adapun manfaaat penelitian berupa teoritis dan praktis.

1.6.1 Manfaat teoritis

Manfaat dari hasil skripsi ini adalah menghasilkan output yang dapat menerapkan fungsi dan prinsip – prinsip yang dimiliki oleh *vigenere cipher* yang dapat mengenkripsi teks.

1.6.2 Manfaat praktis

Manfaat praktis yang dapat dihasilkan dari skripsi ini antara lain:

1. Bagi pengguna aplikasi, dapat lebih mengamankan lagi teks pesan yang akan dibuat agar tidak terjadi kebocoran informasi.
2. Bagi peneliti akan lebih memahami algoritma *vigenere cipher* serta lebih memahami ilmu tentang kriptografi.