BAB I
PENDAHULUAN

1.1. Latar Belakang

Akses terhadap informasi, pertukaran data, penyebaran informasi, komunikasi, dan lain sebagainya semuanya dipermudah karena pertumbuhan eksponensial teknologi informasi di masa modern.Meskipun hal ini mempermudah akses terhadap data, hal ini juga berarti bahwa pemilik data harus lebih waspada dalam menjaga keamanan informasi sensitif dari pengintaian.Oleh karena itu, keamanan data sangat penting untuk melindungi privasi setiap dan seluruh informasi, terutama informasi yang berisi informasi sensitif atau rahasia yang harus disembunyikan dari mata publik yakni informasi yang hanya diperbolehkan bagi individu. Apalagi jika data dikirimkan melalui jaringan publik tanpa dilindungi terlebih dahulu, maka isi informasi tersebut dapat dengan mudah disadap atau diretas dan diketahui oleh pihak yang tidak bertanggung jawab serta pihak yang tidak berhak atas data tersebut.Keamanan data berkaitan dengan pencegahan penghancuran, perubahan, atau pengungkapan data yang tidak disengaja atau berbahaya.

Selain dokumen teks, dokumen audio juga dapat digunakan untuk komunikasi online.Terlebih sekarang sudah sangat mudah untuk melakukan komunikasi yang dapat merekam dan mengirimkan pesan suara.Apalagi jika ada dua pihak atau lebih yang saling berjauhan maka melakukan komunikasi dalam jaringan merupakan salah satu cara untuk berbicara dan mendengarkan pesan dari pihak yang jauh darinya.Data komunikasi dalam jaringan tersebut juga merupakan sebuah dokumen dimana dokumen itu berupa pesan dalam bentuk suara.Seperti yang sudah kita ketahui bahwasanya jika melakukan pengiriman ataupun pertukaran pesan dalam suatu jaringan maka akan adanya kemungkinan penyadapan atau peretasan terhadap pesan tersebut.Maka dari itu jika pemilik pesan ingin agar pesan tersebut tidak dapat di akses maupun dimanipulasi oleh pihak yang tidak berhak menerima pesan tersebut alangkah baiknya melakukan penyandian pada pesannya.Penyandian pesan dilakukan sebelum pesan tersebut akan dikirimkan ke penerima sehingga jika ada pihak yang tidak berwewenang yang berhasil meretas pesan tersebut maka siperetas tidak akan bisa memahami isi pesan itu walaupun sudah bisa diakses olehnya.

Salah satu masalah paling krusial dalam komputasi adalah tantangan pengkodean data.Setiap orang memerlukan program yang dapat mengenkripsi informasi sensitif dan hanya mengizinkan pengguna yang berwenang untuk mengaksesnya.Ada beberapa solusi untuk memperbaiki masalah keamanan informasi ini.Menggunakan algoritma kriptografi adalah salah satu metode untuk menyandikan pesan.Mengingat kriptografi adalah ilmu sekaligus seni yang dimana fokus utamanya adalah menemukan cara untuk menjaga kerahasiaan informasi.Enkripsi mengacu pada proses penggunaan teknik kriptografi untuk mengubah pesan menjadi kode yang tidak dapat diuraikan oleh manusia.Sedangkan apabila si penerima ingin mengetahui isi dari pesan tersebut adalah dengan cara mengembalikan pesan yang sudah disandikan ke bentuk semula,proses ini yang disebut dengan proses dekripsi.Jika pesan sudah diamankan atau disandikan dengan kriptografi maka meskipun pihak tidak berwewenang berhasil meretas atau menyadap pesan tersebut,maka mereka hanya akan mendapatkan pesan acak yang tidak bermakna.

Bergantung pada seberapa banyak kemajuan yang telah dicapai di bidang ini sejak awal ditemukannya algoritma kriptigrafi,maka kriptografi diklasifikasikan sebagai algoritma kriptografi klasik dan algoritma kriptografi modern.Namun jika ditinjau dari kesamaan kunci,algoritma kriptografi dipecah menjadi dua jenis yang berbeda yaitu algoritma yang menggunakan kunci simetris dan algoritma yang menggunakan kunci asimetris.Begitu pula ketika algoritma kriptografi ditinjau dari perspektif kerahasiaan kunci, algoritma kriptografi juga terbagi kepada dua macam yakni diklasifikasikan menjadi kunci rahasia dan kunci publik.Secara umum,ruang lingkup pengamanan kriptografi terdiri dari pengamanan secara fisik,pengamana secara akses,pengamanan data dan pengamanan komunikasi jaringan.Contoh dari implementasi algoritma kriptografi adalah pada tanda tangan digital dan mesin ATM.

Penulis mengambil beberapa referensi dari jurnal-jurnal terdahulu dalam penelitian ini guna untuk memperluas pemahaman tentang pembahasan yang penulis teliti.

1. Penelitian berjudul “Kombinasi Algortima RSA dan Algoritma Cipher Tranposisi untuk Keamanan *Database*,” diambil dari jurnal penelitian Ajib Susanto dan Rico Tritanto.Isi dari jurnal ini bertujuan untuk membuat sistem *database* keamanan.Sistem keamanan ini diharapkan dengan penelitian ini dapat mendukung proses perlindungan pesan atau data yang tidak mudah dicuri atau dibobol, serta dapat digunakan untuk mengamankan data yang sangat penting agar tetap terjaga kerahasiaannya.Diharapkan dengan penggunaan

sistem kombinasi dua kriptografi yang berbeda maka algoritma kriptografi tersebut dapat menjamin keamanan yang lebih baik.

2. Data dari penelitian “Implementasi Algoritma One Time Pad pada Pesan” yang ditulis oleh Nidia Enjelita Saragih.Artikel dalam publikasi ini berfokus pada pengembangan perangkat lunak yang dapat menjamin privasi komunikasi antara dua orang atau lebih,terutama jika informasi yang dibagikan bersifat sangat rahasia.
3. Menurut kajian akademis Muhammad Khoiruddin Harahap dan Nurul Khairina dalam penelitian mereka yang berjudul “Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks,” yang diterbitkan dalam jurnal Kriptografi dan Keamanan Data. Pembahasan yang dibahas dalam penelitian ini yaitu algoritma sangat penting dalam bidang pemrograman komputer, di mana mereka digunakan untuk merakit program dan memecahkan masalah.
4. Penelitian yang berjudul “Peranan Kriptografi Sebagai Keamanan Sistem Informasi Usaha Kecil dan Menengah” ditulis oleh Buyung Solihin Hasugian. Studi ini menganalisis tentang pentingnya kriptografi dalam melindungi sistem informasi perusahaan, baik perusahaan menengah keatas maupun perusahaan kecil.
5. Menurut penelitian yang diterbitkan dalam jurnal Basri, “Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi,” Penelitian ini menganalisis tentang implementasi sistem yang berkaitan dalam hal ketepatan dan keakuratan data yang telah terenkripsi, tingkat kompleksitas, tingkat keamanan, dan jumlah waktu yang dibutuhkan untuk menyelesaikan prosedur.Memiliki kompleksitas pemecahan kunci yang tinggi dalam sistem keamanan data adalah suatu keharusan.Terdapat keuntungan dan kerugian dalam menggunakan kriptografi simetris atau asimetris itu sendiri, oleh karena itu lebih baik menggunakan teknik yang menggabungkan kedua ide kriptografi (hibrida) dalam pengembangan di masa depan.

1.2. Rumusan Masalah

Adapun rumusan masalah yang dapat diambil dari latar belakang di atas yaitu bagaimana membuat sistem keamanan pesan suara mengggunakan metode *One Time Pad*.

1.3. Batasan Masalah

Berdasarkan rumusan masalah, maka penulis membatasi masalah yang akan dijabarkan.Mengingat karena terbatasnya waktu, tenaga serta pikiran dalam penyusunan tugas akhir ini,maka penulis akan membatasi beberapa masalah, yaitu:

1. Proses penyandian pesan suara menggunakan metode *One Time Pad*.
2. Bahasa pemrograman yang digunakan adalah *Python*.
3. Input yang digunakan berupa pesan suara yang sudah direkam.

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk membuat sebuah sistem keamanan file pada pesan suara dengan menggunakan metode *One Time Pad* (OTP).

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Dengan melakukan penyandian pesan suara menggunakan algoritma *One Time Pad* kita dapat meningkatkan keamanan suatu pesan suara sehingga pesan suara tersebut akan lebih terjamin keamanannya.
2. Sebagai ilmu bagi penulis dan para pembaca serta sebagai bahan referensi untuk penelitian-penelitian yang akan dilakukan berikutnya tentang sistem keamanan pesan suara dengan menggunakan algoritma *One Time Pad*.

1.6. Relevansi

Setelah penelitian ini selesai maka hasil dari aplikasi sistem keamanan pesan suara ini adalah dapat membuat data lebih aman dari pihak yang tidak berhak untuk mengakses apalagi memanipulasi data ini.