CHAPTER 1

INTRODUCTION

1.1 Background

The tremendous growth of digital technology, especially in Internet and communication technology, has facilitated multimedia data exchange. Multimedia data is used in real-time voice and video conferencing, air traffic and control, broadcast monitoring, and voice-activated machine control and operation commands. However, sending confidential or sensitive information over networks and communication systems can be lethal as these networks are insecure and vulnerable to virus attacks. (Ramesh Shelke & Dr. Milind Nemade, 2018)

Audio, or sound, is a wave that contains many vital components (amplitude, wavelength, and frequency) that can make one sound into another. Computers can make sense of analog sound through analog-to-digital conversion (ADC). This process is performed by computer hardware called a sound card or sound card. Commonly used audio file formats are mp3, wav, and flax. (Syahputra, 2018)

Wave format (*.WAV) is a sound file format widely used in Windows operating systems for games and multimedia purposes. A *wave* is a raw form in which sound is recorded directly and digitally quantized. Ease of creation and processing This basic file format supports no compression by default and is known as PCM (Pulse Code Modulation). (Santoso & Fakhriza, 2018)

Encryption of audio data is a more difficult and complex process than the techniques used for text data. The US Department of Defense began work on voice encryption in the late 1940s. It was initially used in World War II for secure communications, so the enemy could not understand conversations between military personnel. The idea was first introduced by simply adding noise to the audio signal. The central concept is that the noise signal is added by engaging the sound signal and the recorded sound along the reception point, after which the noise signal is reduced to induce the original sound signal. However, since the same noise signal is required at both ends, the noise signal is generated in pairs for the transmitter and receiver. (Pawar et al., 2014)

With the rapid growth of communication technology, protecting audio from hackers has become an essential issue for engineers. Therefore, to protect your valuable information, you need a way to encrypt information and data before transmission securely. (Ramesh Shelke & Dr. Milind Nemade, 2018)

Cryptography is the science (or skill) of protecting sensitive information from intruders and hackers who want to use it for illegal purposes. It can be defined as ensuring the confidentiality of communications between both ends of a connection. It mainly includes encryption and decryption. Encryption deals with the encrypted content of a secure message so that it cannot be read or deciphered by unauthorized persons or programs. (Al-kateeb & Mohammed, 2020)

Vigenere Cipher is a classic cryptography that hides a message in plain text using a substitution technique that changes each character to another based on the key used. The Vigenere cipher is also an algorithm that uses a symmetric key and repeats the characters in the key until all the characters in the message have been processed.(Rahmasari Kinasih Gusti et al., 2020)

Playfair Cipher is a classical cryptographic algorithm with a Polygram cipher that converts plaintext into Polygram form and performs Polygram encryption and decryption processes. The encryption key comprises 25 characters arranged in a 5x5 grid, excluding the letter J from the alphabet. So the key probability is 25.

In this study, the authors use Vigenere and Playfair Cipher methods to design a system that can protect Wave format audio and maintain the confidentiality of transmitted audio files.

1.2 Identification of Problems

Against the background described, this study formulates the problem of how to protect voice messages using a combination of the Playfair Cipher and the Vigenere Cipher so that the confidentiality of the transmitted message is maintained?

1.3 Research Objectives

This research objective is to keep the audio files sent confidential using a combination of the Playfair cipher and Vigenere cipher methods.

1.4 Research Problem Boundaries

1. The programming language used in this study is Python programming language.
2. The files to be encrypted and decrypted are audio files in *.wav format.