CHAPTER 2
LITERATURE REVIEW

2.1 Theoretical Basis

2.1.1 Cryptography

The art and science of cryptography work together to protect your messages (cryptography is the art and science of keeping your messages safe). In the discussion above, "art" refers to a particular way of encoding a message. The word "graphic" in "crypto" implies an artistic endeavor. For a cryptographic mechanism to work correctly, it requires four main components that are most closely related. That is:

1. Plain Text

   Data or information that can be read and understood.

2. Cipher Text

   A secret message or plaintext encrypted using cryptography. You can convert this ciphertext back to plaintext using the provided key.

3. Cryptography Key

   A term used to describe the cryptographic mechanism and keys used to perform encryption. The encryption and decryption process can only be adequately completed using the same key. The complex information governing the encryption process is called a key.

4. Encryption Decryption Algorithm

   Encryption is the process of encoding data or information into ciphertext whose contents (plaintext) can be read and understood, and decryption is the process of turning ciphertext back into plaintext.

There are two types of cryptography, also known as symmetric and asymmetric algorithms, symmetric cryptographic algorithms or conventional cryptographic algorithms, which use the same key for the encryption and decryption processes. Symmetric cipher algorithms fall into stream algorithms (stream ciphers) and block algorithms (block ciphers). On the other hand, asymmetric encryption algorithms use different keys for the encryption and decryption processes. The encryption key can be publicly distributed and is called the public key, while the decryption key is kept for private use and is called the private key.

2.1.2 Vigenere Cipher

One of the oldest cipher forms, the Vigenere cipher, was first used around 1986. The Vigenere cipher works similarly to the Caesar cipher, encrypting plaintext by alphabetically shifting message characters to key values. A key in the form of a string of words encrypts each plaintext character with a different key. If the key length is less than the length of the plaintext, the key is repeated until it has the same length as the plaintext. The Vigenere Cipher method is A=0; B=1; C=2; D=3; E=4; F=5; G=6; H=7; I=8; J=9; K=10; L=11; M=12; N=13; O=14; P=15; Q=16; R=17; S=18; T=19; U=20; V=21; W=22; X=23; Y=24; Z=25.(Lestari et al., 2019)

Vigenere Cipher is a text encryption method using Vigenere tables. However, this table can be created in a digitally based system as a reference for processing programs. The formulas applied during encryption and decryption are:

$$C_1 = (P_1 + K_1) \, mod \, 26 \qquad \textbf{(2.1)}$$

$$P_1 = (C_1 - K_1) \, mod \, 26 \qquad \textbf{(2.2)}$$

Explanation:

C = Ciphertext

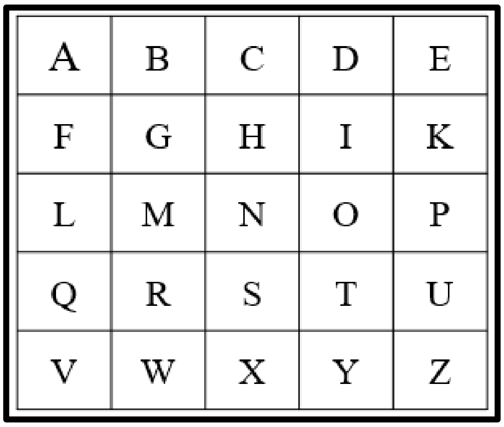
P = Plaintext

K = Key

2.1.3 Playfair Cipher

The Playfair cipher is part of the Polygram cipher invented by Sir Charles Wheatstone but popularised by Baron Lyon Playfair in 1854. This technique encrypts pairs of characters, not single characters, in contrast to conventional ciphers. The characters in the ciphertext appear at a constant frequency, which is intended to complicate the frequency analysis. (Syahputra, 2018)

An algorithm key consisting of 25 characters (letters) is entered in the 5x5 table without the letter J. can be seen in Figure 2.3



A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Figure 2. 1 Playfair Polygram

Several possible keys :

25! = 15.511.210.043.330.985.984.000.000

The keys used in the encryption process are predetermined according to the following rules:

1. Specify the desired key, for example;
   JADI JALAN KAH HARI INI
2. Discard repeated letters and the letter j (if any), examples like ;
   ADILKNKHR
3. Then add the missing letters (except J), for example;
   ADILNKHRBCEFGMOPQSTUVWXYZ
4. Then enter it into a 5x5 square, an example like;

A	D	I	L	N
K	H	R	B	C
E	F	G	M	O
P	Q	S	T	U
V	W	X	Y	Z

Figure 2. 2 Example of a Playfair Polygram

Encrypted messages are preconfigured according to the following rules:

SIAPA YANG JADI PENJAHAT DISINI

1. Replacing the letter J (if any) with “I”.

   SIAPA YANG IADI PENIAHAT DISINI

2. Write the message in pairs of letters (bigrams)

   SI AP AY AN GI AD IP EN IA HA TD IS IN I

3. Don't let there be pairs of the same letters if you insert “x" in the middle.

4. If the number of letters is odd, add “x” as a partner or at the end.

   SI AP AY AN GI AD IP EN IA HA TD IS IN IX

The algorithm for encrypting can be done with the following rules:

1. If two letters are in the same key row, then each letter is replaced with the letter on the right (is cyclic).

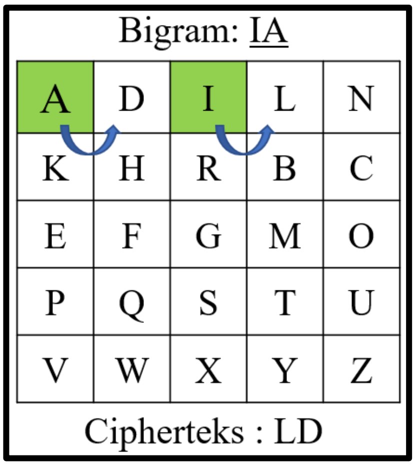
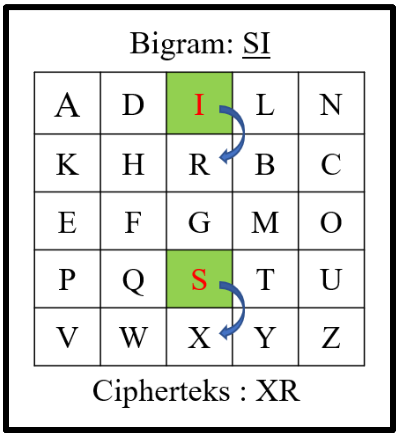


Figure 2. 3 Playfair Cipher Encryption (1)

2. If two letters are in the same key column, then each letter is replaced with the letter below it (is cyclic).



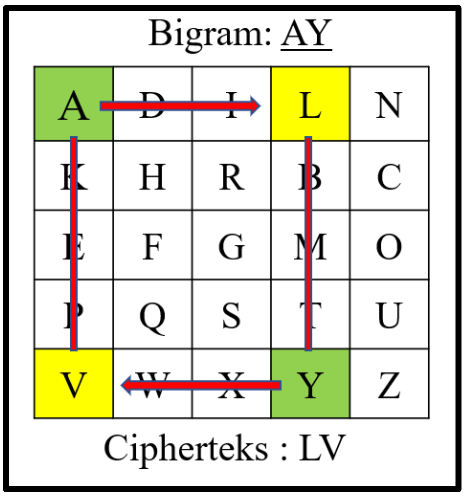
Bigram: SI

A	D	I	L	N
K	H	R	B	C
E	F	G	M	O
P	Q	S	T	U
V	W	X	Y	Z

Cipherteks : XR

Figure 2. 4 Playfair Cipher Encryption (2)

3. If the two letters are not in the same row or the same column, then
   1) The first letter is replaced with the note at the intersection of the first letter row and the second letter column.
   2) The note replaces the second letter at the fourth corner point of the rectangle formed from the three letters used so far.



Bigram: AY

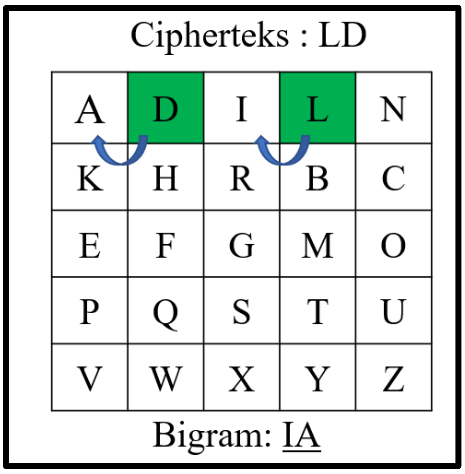
A	D	I	L	N
K	H	R	B	C
E	F	G	M	O
P	Q	S	T	U
V	W	X	Y	Z

Cipherteks : LV

Figure 2. 5 Playfair Cipher Encryption (3)

The decryption algorithm is the opposite of the encryption algorithm. Here are the steps:

1. If two letters are in the same square row, each letter is replaced with the left letter.



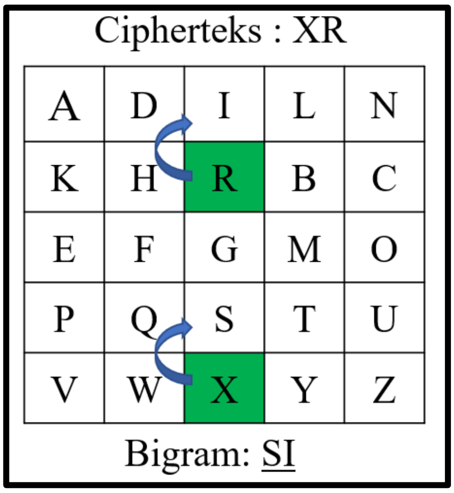
Cipherteks : LD

A	D	I	L	N
K	H	R	B	C
E	F	G	M	O
P	Q	S	T	U
V	W	X	Y	Z

Bigram: IA

Figure 2. 6 Playfair Cipher Decryption (1)

2. If two letters are in the same square column, each letter is replaced with the letter above it.



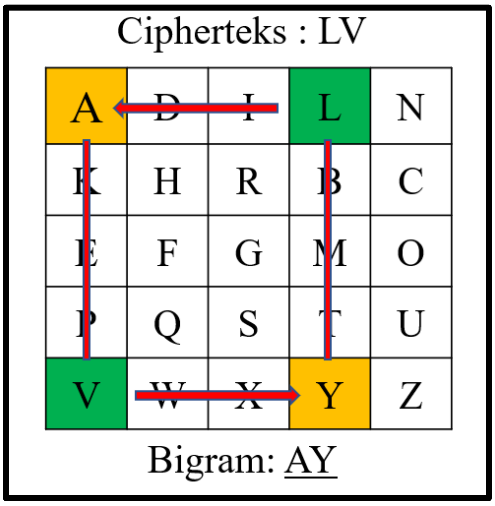
Cipherteks : XR

A	D	I	L	N
K	H	R	B	C
E	F	G	M	O
P	Q	S	T	U
V	W	X	Y	Z

Bigram: SI

Figure 2. 7 Playfair Cipher Decryption (2)

3. If the two letters are not in the same row or the same column, then
   1) The first letter is replaced with the note at the intersection of the first letter row and the second letter column.
   2) The note replaces the second letter at the fourth corner point of the rectangle formed from the three letters used so far.



Cipherteks : LV

A	D	I	L	N
K	H	R	B	C
E	F	G	M	O
P	Q	S	T	U
V	W	X	Y	Z

Bigram: AY

Figure 2. 8 Playfair Cipher Decryption (3)

4. Remove the letter X that does not contain meaning.

2.1.4 *Audio *.wav*

WAV is an audio file format, precisely a container format for storing multimedia files. Formerly called WAVE (Waveform Audio File Format), it is called WAV because of its extension (.wav or wave). WAVE was first released in August 1991 and last updated in March 2007. WAV and WAVE are used interchangeably and jointly developed by Microsoft and IBM. It is a subset of Microsoft's RIFF (Resource Interchange File Format) standard, which stores data in chunks.

RIFF (Resource Interchange File Format) is a container format for storing data and is widely used for various multimedia files in Windows. File formats are marked with their extensions. For example, Audio-Video Interleaved (.AVI), MIDI files (.RMI), color palette files (.PAL), animated mouse cursor file formats (.ANI), and Waveform audio file formats (.WAV) are all based on RIFF. Because a WAVE file is the substance or part of a RIFF file, it inherits the RIFF file structure. Just as a RIFF file consists of a file header at the beginning and is followed by several data chunks, WAVE begins with a file header, which requires the two subsections "fmt " and "data," and a data chunk, which includes the data ID and size, and data the actual raw of the audio.(Lindawati & Rita Siburian, 2017)

Figure 2.18 illustrates the file structure of the canonical WAV file format, which stores PCM data:

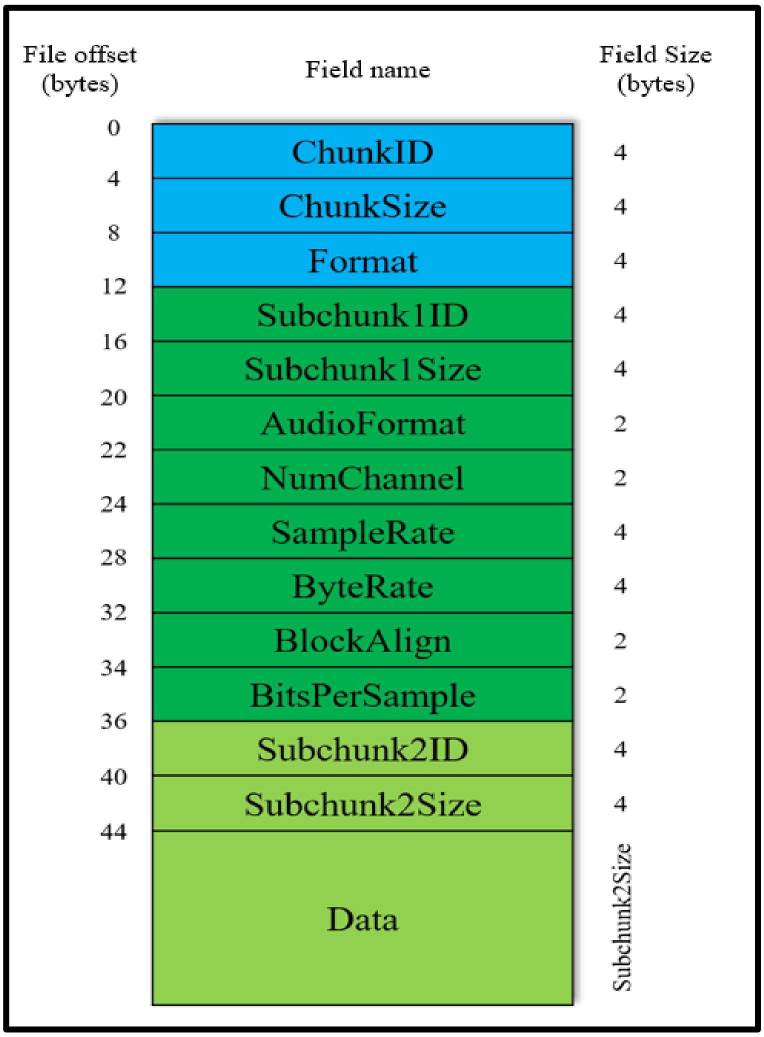


Figure 2. 9 The canonical WAV file format

Explanation :

Table 2. 1 Description of the canonical WAV file format

Offset	Size	Name	Description
0	4	*ChunkID*	Usually contains "RIFF" of an ASCII text string (0x52494646 big-endian form). (note: Endianness is a term that describes the order in which bytes are stored in computer memory. Endianness can be major or minor, with the adjective referring to which value is stored first.

			Big-endian is an order where the "big end" (the most significant value in the sequence) is stored first at the lowest storage address. Little-endian is the sequence where the "little end" (least important value in the line) is stored first.)
4	4	*ChunkSize*	Usually contains 8 bytes (32-bit integer) of total file size - in bytes. It is generally filled after creation.
8	4	*Format*	Header Type Files. Usually contains "WAVE" of an ASCII text string (0x57415645 big-endian form).
12	4	*Subchunk1ID*	Usually contains "fmt " of an ASCII text string (0x666d7420 big-endian form). (note: there is a space after writing "fmt")
16	4	Subchunk1Size	WAV type format size (2 bytes) + mono/stereo flag (2 bytes) + sample rate (4 bytes) + byte/sec (4 bytes) + block alignment (2 bytes) + bit/sample (2 bytes). This is usually 16.
20	2	*AudioFormat*	The audio format usually contains 1 for PCM, and other values represent other forms of compression. Endian litter, so 0001 hexadecimal is 1 in decimal.
22	2	*NumChannel*	The Number of channels usually contains 1 = Mono, 2 = Stereo.
24	4	*SampleRate*	Sample Rate – 32-byte integer. Typical values are 44100 (CD), 48000 (DAT).

			Sample Rate = Number of Samples per second, or Hertz.
28	4	*ByteRate*	Average Bytes Per Second (ByteRate). ByteRates are obtained from (Sample Rate * Bits Per Sample * Channel Numbers) / 8
32	2	*BlockAlign*	Usually contains from (NumChannels * BitsPerSample) / 8.
34	2	*BitsPerSample*	Usually contains 16 bits = 1000 (little endian 0010); 32 bits = 2000 (little endian 0020); etc., or 8 bits = 8, 16 bits = 16, etc.
36	4	*Subchunk2ID*	Usually contains "data" of an ASCII text string (0x64617461 big-endian form).
40	4	*Subchunk2Size*	Usually contains the Number of bytes in the data obtained from (NumSamples * NumChannels * BitsPerSample) / 8.
44	*	*Data*	Contains actual sound data.

2.2 Previous Researches

In preparing this work, we will conduct a literature search on previous research related to the background of this work. Studies used as references for the current study, namely:

1. Andri Syahputra (2018) researched Analysis of Implementation of Audio File Security Using the Playfair Algorithm. The rapid development of information technology makes the use of MP3 format digital audio format files prevalent and facilitates their distribution. Therefore, you need an application that protects MP3 files by encrypting and decrypting them. As a result, applying

encryption algorithms to audio files can save the data from modification. (Syahputra, 2018)

2. Awang Harsa K et al (2017) researched Audio Data Encryption Using RSA Cryptography Method. Because audio files are often used as private messages, encryption techniques are needed to change the form of the data so that it is not easily read or seen by others. The result is that the time to carry out the encryption process depends on the file size and key digits used. Encryption cannot work in the audio format registered in the application. The larger the audio file size, the longer the estimated time for the encryption process. This is due to the length of the calculation process, and encryption of audio files with the RSA method results in a different file that can`t be used at all. (Harsa et al., 2017)
3. Heri Santoso, M. Fakhriza (2018) researched Designing a Wav Format Audio File Security Application (Waveform) Using the RSA Algorithm. Due to the rapidly increasing development of information technology, audio data transmission has also increased because it facilitates the exchange of information in various places. It is necessary to secure confidential data so that third parties do not know it. The result is that the software can encode audio data by applying the RSA algorithm and the WAV audio data structure, and the size of the WAV audio file becomes larger after being encrypted using the RSA algorithm based on the key size used.(Santoso & Fakhriza, 2018)
4. Ramesh Shelke and Dr. Milind Nemade (2018) researched Audio Encryption Algorithms using Modified Elliptical Curve Cryptography and Arnold Transform for Audio Watermarking. Due to the extraordinary growth in digital technology, especially in the internet and communication science and engineering, sharing multimedia data becomes easier to transmit through networks and communication systems, which can be fatal because these networks are insecure and vulnerable to virus attacks. It is, therefore, mandatory to encrypt information or data before sending it to protect valuable information. With the results, the proposed algorithm is best suited

for audio signal encryption in terms of complexity, security, and loss. It is strong against compression attacks and satisfies all encryption parameters, such as correlation coefficient, SCR, and UAC. It can be implemented in audio watermarking systems using the transform domain approach.(Ramesh Shelke & Dr. Milind Nemade, 2018)

5. Juni Ade Nawer Purba et al (2019) researched Implementation of the Cryptosystem Paillier Algorithm in securing Audio. Because information security is essential, it is necessary to maintain its authenticity and integrity if it is to be sent because third parties can intercept and know the data during transmission. The result is that the paillier cryptosystem algorithm can encrypt audio, and audio encryption is very dependent on the size of the audio itself. The larger the audio size, the longer it takes for encryption.(Juni Ade Nawer Purba et al., 2019)
6. Roayat Ismail Abdelfatah (2020) researched Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations. Because multimedia data security is a big challenge for open communication systems that various types of attacks can threaten. The primary tool for achieving this security is encryption. In the study, the method used consisted of three phases with three secret keys and two multi-chaotic pseudo-random generators, which were newly designed and evaluated using different measurements, including signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR), correlation coefficient, histogram, key sensitivity, UACI, NSCR, RMS, and CF. The results prove that the proposed scheme is highly secure and more substantial than many similar recent audio encryption schemes against various types of attacks. (Abdelfatah, 2020)
7. Ekhlas Abbas Albahrani (2017) conducted research related to A New Audio Encryption Algorithm Based on a Chaotic Block Cipher to achieve a good balance between performance and security. Chaotic-based cryptosystems have many properties that make them suitable for encrypting multimedia such as images, videos, or audio data. Unlike text messages and pictures,

audio information has a higher repetition and a stronger correlation between samples. Many scholars have made efforts to investigate audio encryption algorithms but have yet to find the algorithm to be called the best that is algorithm if it achieves a good balance between performance and security. The test results show that the proposed audio algorithm is secure because of its sizeable key space, uniform histogram, low PSNR, low correlation, high entropy, and high MSR, indicating that the algorithm is a good choice for encrypting audio and other multimedia data such as images and videos. like that.(Dr. Ekhlas Abbas Albahrani, 2017)

8. Chloe Albin et al (2018) researched the DWT-based Audio Encryption scheme. When data is transferred from one person to another, a very high level of security is required. For this reason, the author wants to build cryptography using the SHA-256 hashing algorithm to help fight various hackers who will not be able to decipher confidential data and use Discrete Wavelet Transform (DWT) to improve performance efficiency. With experimental results and analyses such as PSNR, correlation, and histogram, we can conclude that the design is robust and very useful for audio encryption.(Chloe Albin et al., 2018)
9. Rahmadani Harahap (2021) conducted research related to the Implementation of the Skipjack Algorithm to Secure Audio. Because one of the things that are important to ensure the confidentiality of data or information is encryption. So we need observation of details in the form of audio recordings in MP3 format using cryptography. The results show that the Skipjack Algorithm provides robust security to prevent the audio from being spread to unauthorized people. (Harahap, 2021)
10. Zeena N. Al-kateeb & Saja J. Mohammed (2020) conducted research related to A novel approach for audio file encryption using hand geometry. Secret information and its transmission method have occupied the most critical position since ancient times. The methods used to encrypt data varied, and the algorithms used in this domain were developed into what they are today. Due to the significant development and electronic revolution, the emergence

of biometric information, and the introduction of this concept into remote data encryption systems, bio-encryption has crystallized. Based on the above problems, the author proposes to build an audio file encryption/decryption algorithm based on discrete wavelet transform (DWT) and biometric features and uses several hand geometry measurement properties to secure audio files. The result is a new proposed algorithm for audio file encryption/decryption based on discrete wavelet transform (DWT) and biometric features to provide a high level of confidentiality and reliability. Subjective and objective measures are applied based on the generated signal. (Al-kateeb & Mohammed, 2020)

11. Arief Susanto et al (2018) researched image encryption using vigenere cipher with bit circular shift. Because data and information are essential commodities for individuals and organizations, information can be presented in text, images, audio, video, or a mixture thereof. Some information is available and accessible to the public, whereas some are confidential. To secure information, cryptography can be applied. Cryptography is the science of keeping secrets. Therefore, the author wants to spread the vigenere cipher method with circular bit shifts to secure information data in images. Image encryption using the Vigenere cipher with circular bit shifts gives better results than using the Vigenere cipher alone. Vigenere cipher with circular shift bits produces better randomness images, resulting in images that are difficult to recognize. (Susanto, 2021)

In previous studies, one of the methods used in this study was RSA (Rivest Shamir Adleman). The result is that encryption cannot work in audio formats registered in the application. The larger the audio file size, the longer the estimated time for the encryption process due to the length of the calculation process, and the implementation of RSA audio file encryption only produces a different file that cannot be used at all.

However, the research discussed this time will use two methods, namely the Vigenere Cipher method and the Playfair Cipher method. Vigenere Cipher is used for encrypting audio files because Vigenere Cipher is symmetric cryptography, which means that the encryption and decryption processes use the same key. Hence, the role of Playfair Cipher is to encrypt Secret Keys so that security is maintained. Vigenere Cipher and Playfair Cipher are classic cryptography. Therefore, these methods are used with the hope that they will produce faster calculations and computation processes. In audio files, it is the data part that will be encrypted, so the audio file will still be able to run with the result that the information in it is encrypted.