KALINGA INSTITUTE
OF INDUSTRIAL TECHNOLOGY
Deemed to be University U/S 3 of the UGC Act, 1956

**6th Semester**
**CSCE**
**Minor Project**

# Data Security Using Cryptography and Steganography

**Submitted By:**
Tushar Bhatt 2129119
Rahul Bagaria 2129140
Vishesh Raj Solanki 2129124
Rakesh Kumar 2129144
Avi Bhagat 2129062

**Submitted to**
Prof. Dayal Kumar Behera
School Of Computer Engineering

# Index

## Introduction:

Recent advancements in steganography analysis have made it more challenging to use steganography to secure private messages, digital photos, or other materials. The presence of concealed information in carrier files is amply demonstrated by steganography analysis. The strategy used in this project centers on the application of both steganographic and cryptographic approaches. By doing this, we can retain the data more securely, preventing unauthorized network users from accessing the data that is already available. The message from the data should only be decoded by the sender and receiver.

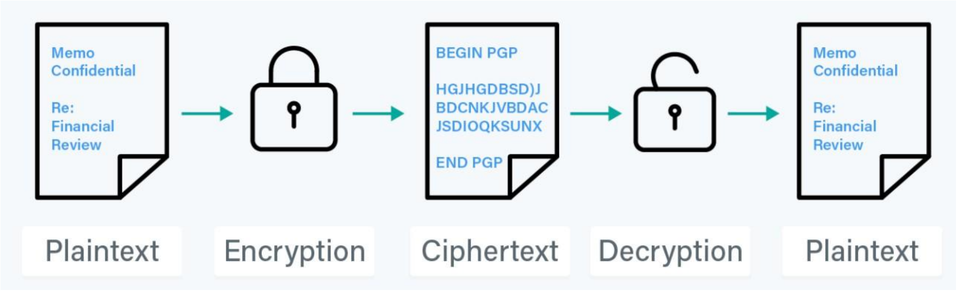
## Abstract:

Data masking is crucial for protecting the security and integrity of the information that will be transferred in addition to preventing data tampering. An opponent uses someone else's data not just for their own purposes but also for their own gain. The basic purpose of data concealing is to safeguard information from outsiders who might abuse it. The method of data concealing is intended to be used in a variety of ways to secure and protect the data while it is being transmitted. Two of the five ways to hide data are cryptography and steganography. This project offers a way to conceal data for any type of media, including audio, utilizing a variety of algorithms at the user's option.When encrypting material, a number of algorithms are combined and implemented in the application according to the preference or option of the user.

# Area of Study

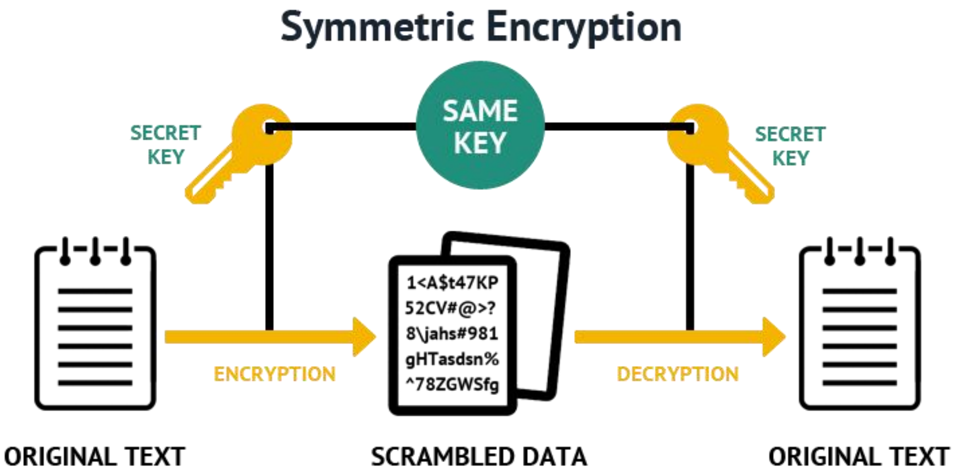
## Cryptography:

Cryptography techniques have been employed since the dawn of time to ensure the confidentiality of interparty communications. This technique, known as the art of information hiding, encrypts plaintext into ciphertext using a suitable key and sends it across an insecure channel to the other parties. The original plaintext is recovered by decrypting the ciphertext using a secret key. Plaintext cannot be decoded without the key's knowledge. Confidentiality, secrecy, nonrepudiation, key exchange, and authentication are just a few of the numerous elements that cryptography plays a crucial role in.



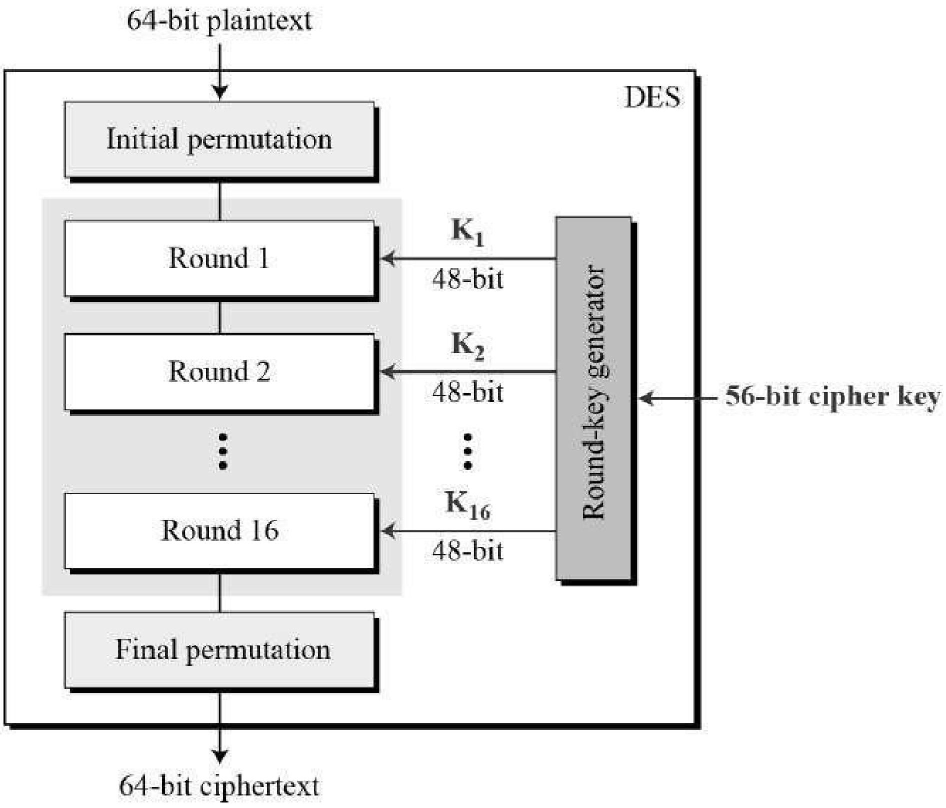
## Symmetric Key Cryptography:

The method of secret key encryption is sometimes referred to as symmetric-key, shared-key, single-key, and ultimately private-key encryption. Secret data is encrypted and decrypted using the private key mechanism on all sides. The transmitter encrypts the original data, or plaintext, using a key, and the receiver uses a key to decrypt a message to get the plaintext. Only those with permission to encrypt or decode data will have access to the key. Although the method provides adequate transmission security, there is a problem with key distribution. One can easily obtain all of the data if they steal or discover the key. DES Algorithm is an illustration of a symmetric-key.



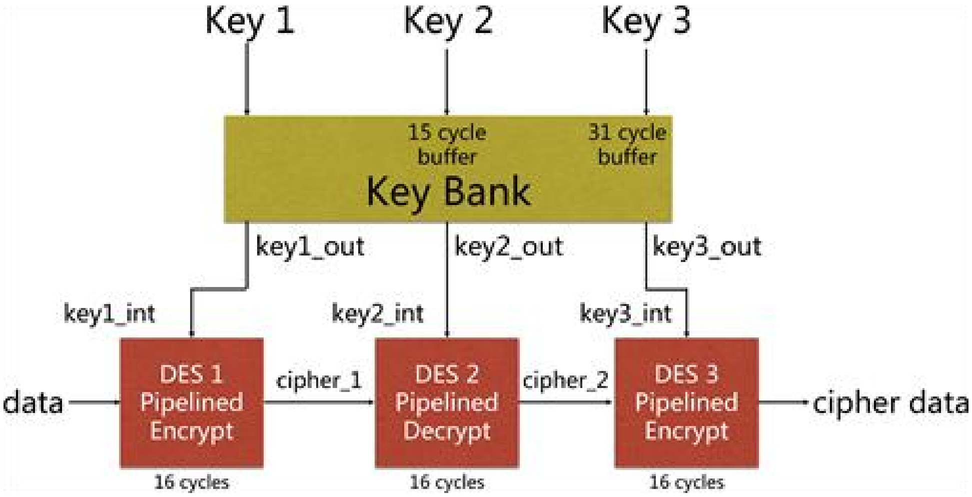
# DES:

The symmetric-key algorithm DES uses a Feistel network as its foundation. It is a symmetric key cypher because it use the same key for both encryption and decryption. Both of these procedures are nearly identical thanks to the Feistel network, making the resulting algorithm easier to use. Although the block and key sizes for DES are both 64 bits, the actual security offered by the key is just 56 bits.



## Triple DES:

The short key length of DES led to the development of 3DES as a more secure substitute. The DES algorithm is repeated three times with three different keys in 3DES, although it is only regarded as secure when three different keys are utilised. The Triple Data Encryption Algorithm (TDEA or Triple DEA), sometimes known as Triple DES (3DES or TDES), is a symmetric-key block cipher that uses the DES cypher algorithm three times to encrypt each data block.

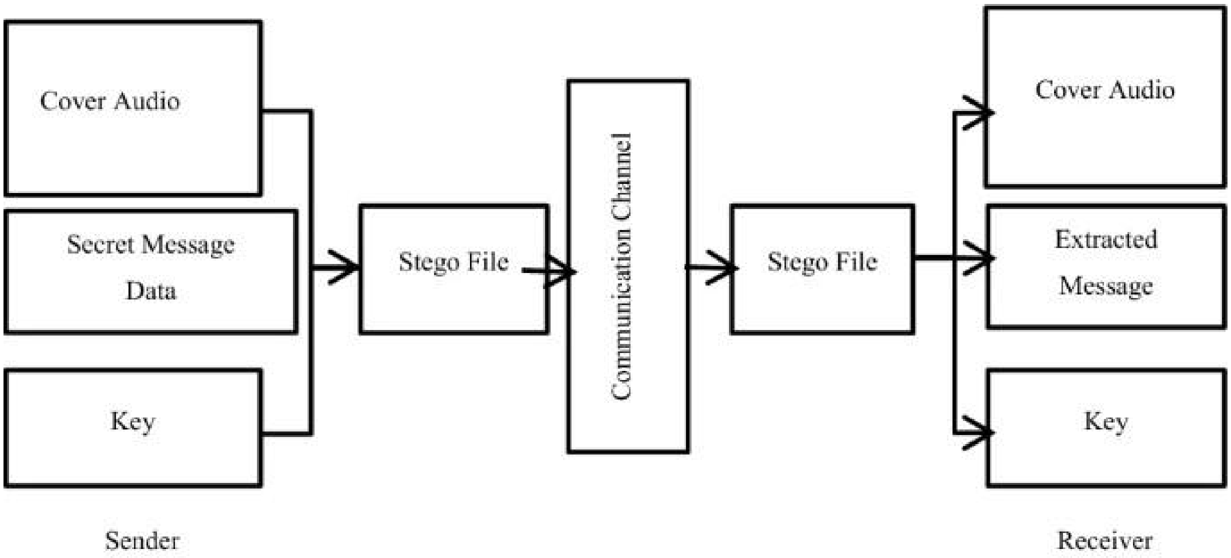


## Steganography

The science of concealing and transmitting data over ostensibly dependable carriers in an effort to conceal the data's presence might be described as its main focus. Thus, the message's existence was never known to begin with. The individual won't try to decode the data if they view the cover where it is buried because they won't know there is any covering data there. By applying a certain algorithm, the stego system encoder can introduce the secret information into the cover medium. After the secret data has been embedded in the cover object, the cover object will be referred to as a stego object. The stego object also sends to the receiver by selecting the suitable channel, where the decoder system is used with the same stego method to obtain the original information as the sender would like to transfer.

## Audio Steganography:

The goal of audio steganography is to encrypt the audio with a hidden message. It is a method used to protect the transfer of sensitive information or to conceal its presence. If the message is encrypted, it might also guarantee confidentiality for secret messages.
The Human Auditory System (HAS) has properties like huge power, powerful range of hearing, and great range of audible frequency, which make audio steganography more impressive than images.



## Fernet Algorithm:

Fernet algorithm provides symmetric encryption and authentication to data. It is a part of the cryptography library for Python, which is developed by the Python Cryptographic Authority (PYCA).It automatically generates a fresh fernet key and uses key rotation which makes it easy to replace old keys. So we can add your new key at the front of the list to start encrypting new messages, and remove old keys as they are no longer needed.Hence , it helps in securing data without running into all of the risks that come with implementing cryptographic primitives yourself.

## Motivation:

Due to recent advancements in steganography analysis, it has become challenging to use steganography to secure private data, communications, audio files, or digital photos. This is the primary reason and driving force behind the project selection. It is simple to find out whether there is concealed data in carrier files by employing steganography analysis. As a result, after learning about these issues, we were inspired to work on this project, in which two separate strategies are used to convey information completely. It is only necessary to choose a cover audio and use that audio to convey the information.

## Problem Statement

Our programme will give you more Security to the data present in the network which will be transported from the sender to the recipient utilizing audio steganography and TDES.

Only the Authorized users i.e., who are using our application will be there on the Network. The suggested approach is to hide the textual data effectively in an audio file without any suspicion of the data being hidden in the image.

It is to work against the attacks by using a distinct new carrier file that isn’t possible to compare.

The project's goal is to use steganography to conceal data in an audio while ensuring that the quality of the data concealment is maintained. In order to securely transport data over the network without anyone seeing that it was hidden, we used a technique for hiding the data in a separate audio file.

This approach will safeguard the data even if it necessitates a distinctive audio that we may use as a carrier and conceal the data that is well within the threshold that the audio can hide.

# Literature Survey:

| S.No | Paper Title | Journal Name and Publication | Work Done | Technique Used | Disadvantage |
|---|---|---|---|---|---|
| 1 | Encryption and Decryption using Password Based Encryption, MD5, and DES | Advances in Social Science, Education and Humanities Research (ASSEHR), volume 141 International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (PDF) Encryption and Decryption using Password Based Encryption, MD5, and DES (researchgate.net) (2017) | Password-Based Encryption = Encryption hashing + 64-bit symmetric randomly added to password and hash using MD5. | Steganography ,Cryptography, DES3 ,Hashing. | installation of a typical active attack and the ability to collect information from participant interactions. |
| 2 | Base64 Character Encoding and Decoding Modeling | International Journal of Recent Trends in Engineering & Research, 2016 (PDF) Base64 Character Encoding and Decoding Modeling (researchgate.net) (2016) | Data encryption and decryption using Base-64 to avoid errors and enhance security of data to overcome the weakness. | Base 64 encoding, Encryption and Decryption. | It is not a standalone algorithm and requires an extra method to make the security level high. |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Data (Video) Encryption in Mobile Devices | Kurdistan Journal of Applied Research (KJAR) (semanticscholar.org ) (2017) | Implementation of video protection of fully encrypted using Elliptic Curve Cryptography (ECC) on a mobile device (Android) | Elliptic Curve Cryptography Encryption and Decryption | ECC increases the size of the encrypted message significantly more than RSA encryption. Furthermore, the ECC algorithm is more complex and more difficult to implement than RSA, which increases the likelihood of implementation errors, thereby reducing the security of the algorithm. |
| 4 | Document Security within Institutions Using Image Steganograp hy Technique | INTERNATIONAL JOURNAL OF SCIENCE AND RESEARCH (IJSR) Volume 3 Issue 4, April 2014 Document Security within Institutions Using Image Steganography Technique (ijsr.net) (2014) | Hiding information using steganography and how to decrypt the hidden Files. Altered picture closely resembles the original. Not susceptible to attacks such as rotation and translation. | Algorithm Used in Steganography i.e LSB Method. | Only using Steganography is not the best way to encrypt data. There is immense scope for an improved LSB technique which will perform better on parameters such as: security, capacity, imperceptibility, computational complexity and tamper resistance. |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Multilayer Security in Protecting and Hiding Multimedia Data using Cryptograph y and Steganograp hy Techniques | Multilayer Security in Protecting and Hiding Multimedia Data Multilayer Security in Protecting and Hiding Multimedia Data using Cryptography and Steganography Techniques \| IEEE Conference Publication \| IEEE Xplore (2019) | This paper combination of encryption and Steganograph y to enhance the security of the data to be sent. | Cryptography, Steganography , DES, LSB | Data is hidden within image, audio and video using techniques so sometimes it may not be secured. |
| 6 | Combined Audio Steganograp hy and AES Encryption to Hide the Text and Image into Audio using DCT. | Combined Audio Steganography and AES Encryption to Hide the Text and Image into Audio using DCT International Journal of Soft Computing and Engineering (ijrte.org) (2019) | Proposed a model that hides AES encrypted data inside a cover audio file. | Discrete Cosine Transform, Multimedia Steganography, AES Encryption. | Large overhead to hide very tiny amounts of information. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication. |
| 7 | A Survey of Video Encryption Algorithms Implemented In Various Stages of Compression | International Journal of Engineering Research & Technology (IJERT) A Survey of Video Encryption Algorithms Implemented In Various Stages of Compression (ijert.org) (2013) | Analysis and Comparison of various Video Encryption Algorithms during Compression | Selection Video Encryption Algorithm, Motion vector encryption algorithm, ExpGolomb Encryption Algorithm,CA V L C Encryption Algorithm , Sign Encryption | A concrete summary of the comparison of the various encryption algorithms during compression in the form of a table could be given to provide a faster access/revision to the reader |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Algorithm,Une q ual Secure Encryption, Huffman's Tables techniques | |
| 8 | Research on RealTime Video Encryption Algorithm Based on Moving Objects | The Open Cybernetics & Systemics Journal Microsoft Word - Wei Chen (C 4210767)_TOCSJ. do c (benthamopen.com ) 2014 | Video Encryption on Real time Data with Moving Objects | MV Prediction Method, Macro Block Encryption Method | computational complexity and ratedistortion performance of MV prediction are two factors difficult to balance |
| 9 | A Survey on Audio Steganograp hy Approaches | international Journal of Computer Applications (0975 – 8887) Volume 95– No. 14, June 2014 A Survey on Audio Steganography Approaches (ijcaonline.org) (2014) | To carry out intensive literature reviews of the existing techniques and demonstrate the advantage and the disadvantage of every technique. | Stego signal, audio steganography, H.A.S, information hiding | Most of the methods seen have low data capacity and the data is easy to extract. |
| 10 | audio Steganograp hy: LSB Technique Using a Pyramid Structure and Range of Bytes | International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-20, September2015 ,pp.233- 248 Microsoft Word - Audio Steganography | To provide relatively good improvement in the payload capacity by dividing the bytes of cover media into ranges to hide the bits of secret | The combination of a Pyramid Structure and Range of Bytes | The size of the covert media file had not mentioned, therefore the payload capacity is unpredictable |

| | | | | | |
|---|---|---|---|---|---|
| | | New Approach.docx (arxiv.org) (2015) | message appropriately | | |
| 11 | Information Hiding Using Audio Steganograp hy - A Survey | The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011 (PDF) Information Hiding Using Audio Steganography - A Survey (researchgate.net) (2011) | To discuss different types of audio steganographic methods, advantages and disadvantages | Echo hiding, spread spectrum, Phase coding, LSB coding and parity coding | Human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness. Phase coding has the main disadvantage of low data transmission rate because of the fact that the secret message is encoded only in the first signal segment |

## Working Methodology

Our model is based on 2 way encryption using Steganography and Triple DES Algorithm.

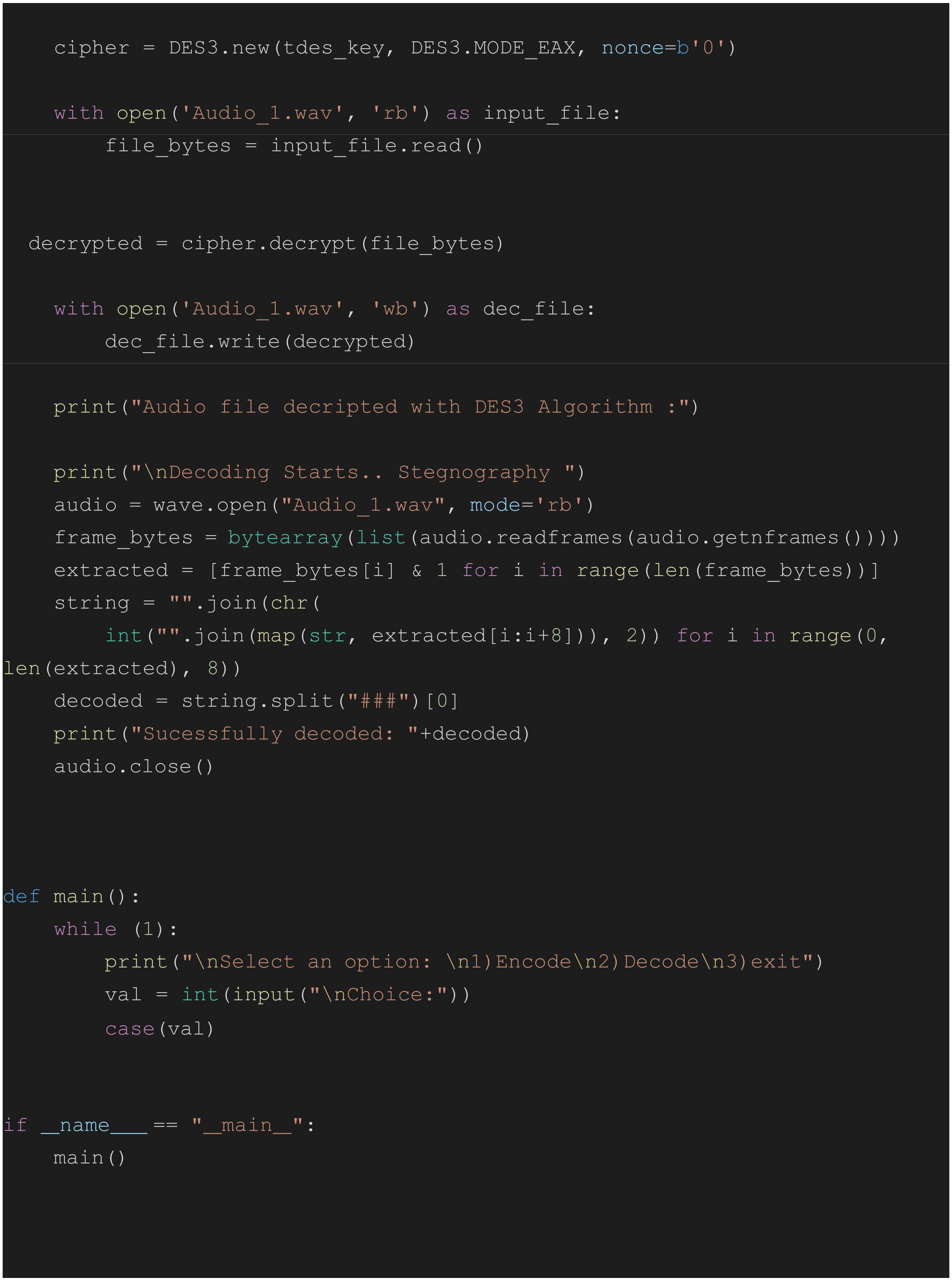
- Enter Text to be encrypted.
- The Text will be encrypted in an Audio File using Steganography.
- Now to ensure the confidentiality of our text we will again encrypt the Audio File using Tripel DES Algorithm.
- For this sender has to have a Triple DES Key.
- After Encryption is processed successfully we can now send the audio file to whomever we want.
- The receiver will have the Triple DES Key.
- The receiver will first decrypt the Audio File by using the Triple DES key.
- After decoding the Audio file we will now perform steganography to extract the hidden text message.
- After decryption is successfully done the receiver will obtain the hidden text message.

# Code

## Using Steganography and Triple DES Algorithm

```
import wave
from Crypto.Cipher import DES3
from hashlib import md5

key = input("Enter TDES Key : ")
key_hash = md5(key.encode('ascii')).digest()   # 16-byte key

tdes_key = DES3.adjust_key_parity(key_hash)
cipher = DES3.new(tdes_key, DES3.MODE_EAX, nonce=b'0')


def case(a):
    if a == 1:
        encode()
    elif a == 2:
        decode()
    elif a == 3:
        quit()
    else:
        print("\nEnter valid Choice!")


def encode():
    print("\nEncoding Starts..")
    audio = wave.open("pink.wav", mode="rb")
    frame_bytes = bytearray(list(audio.readframes(audio.getnframes())))

    string = str(input("Enter Text to be Incription : "))

    string = string + int((len(frame_bytes)-(len(string)*8*8))/8) * '#'
```

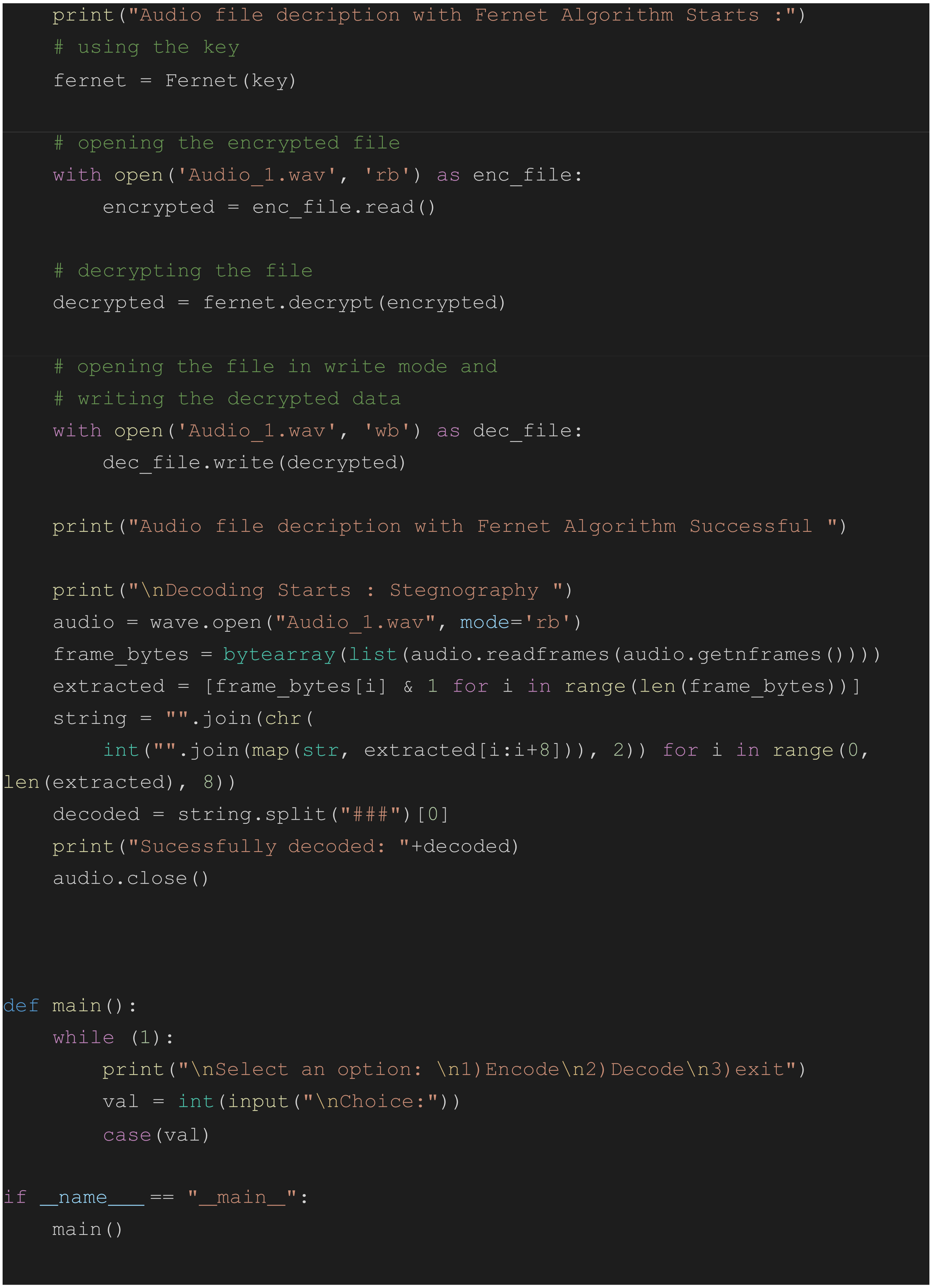
```
      bits = list(
        map(int, ''.join([bin(ord(i)).lstrip('0b').rjust(8, '0') for i in string])))

    for i, bit in enumerate(bits):
        frame_bytes[i] = (frame_bytes[i] & 254) | bit
    frame_modified = bytes(frame_bytes)
    for i in range(0, 10):
        print(frame_bytes[i])
    newAudio = wave.open('Audio_1.wav', 'wb')
    newAudio.setparams(audio.getparams())
    newAudio.writeframes(frame_modified)


    newAudio.close()
    audio.close()
    print(" |----> Succesfully encoded text inside Audio_1.wav using Stegnography ")

    print("Applying Triple DES Encription on Audio 1 file ")

    with open('Audio_1.wav', 'rb') as input_file:
        file_bytes = input_file.read()

    encrypted = cipher.encrypt(file_bytes)
    with open('Audio_1.wav', 'wb') as encrypted_file:
        encrypted_file.write(encrypted)

    print("Audio file encripted with DES3 Algorithm Successful ")


def decode():

    print("Audio file decription with DES3 Algorithm Successful ")

    key = input("Enter TDES Key : ")

    key_hash = md5(key.encode('ascii')).digest()  # 16-byte key

    tdes_key = DES3.adjust_key_parity(key_hash)
```



```
    cipher = DES3.new(tdes_key, DES3.MODE_EAX, nonce=b'0')

    with open('Audio_1.wav', 'rb') as input_file:
        file_bytes = input_file.read()


  decrypted = cipher.decrypt(file_bytes)

    with open('Audio_1.wav', 'wb') as dec_file:
        dec_file.write(decrypted)

    print("Audio file decripted with DES3 Algorithm :")

    print("\nDecoding Starts.. Stegnography ")
    audio = wave.open("Audio_1.wav", mode='rb')
    frame_bytes = bytearray(list(audio.readframes(audio.getnframes())))
    extracted = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
    string = "".join(chr(
        int("".join(map(str, extracted[i:i+8])), 2)) for i in range(0,
len(extracted), 8))
    decoded = string.split("###")[0]
    print("Sucessfully decoded: "+decoded)
    audio.close()



def main():
    while (1):
        print("\nSelect an option: \n1)Encode\n2)Decode\n3)exit")
        val = int(input("\nChoice:"))
        case(val)


if __name___== "__main__":
    main()
```

# Using Steganography and Fernet Algorithm

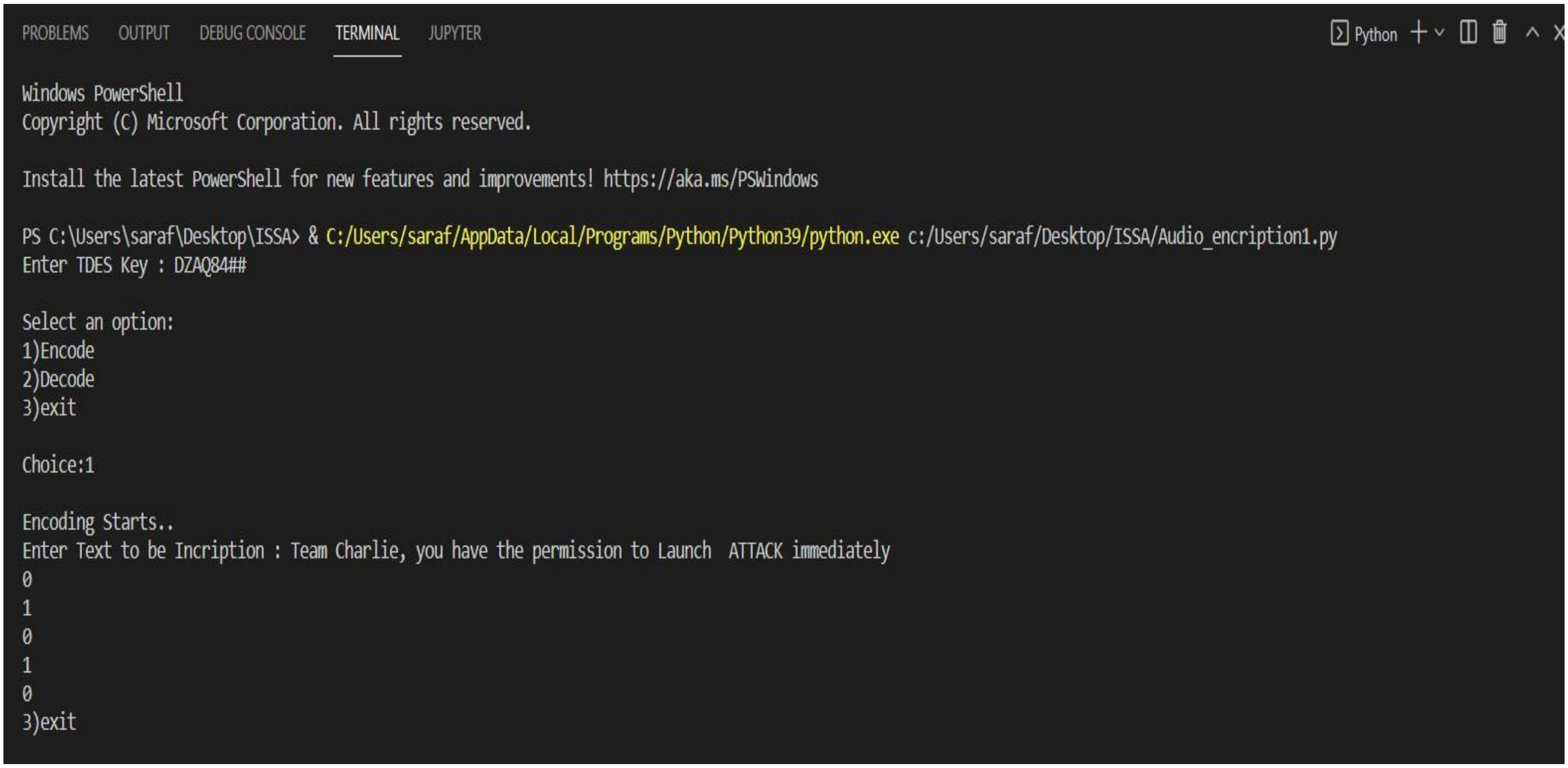
```
import wave
# import required module
from cryptography.fernet import Fernet
from cryptography.fernet import Fernet


# key generation
key = Fernet.generate_key()

# string the key in a file
with open('filekey.key', 'wb') as filekey:
    filekey.write(key)


def case(a):
    if a == 1:
        encode()
    elif a == 2:
        decode()
    elif a == 3:
        quit()
    else:
        print("\nEnter valid Choice!")


def encode():
    print("\nEncoding Starts..")
    audio = wave.open("pink.wav", mode="rb")
    frame_bytes = bytearray(list(audio.readframes(audio.getnframes())))

    string = str(input("Enter Text to be Encripted : "))

    string = string + int((len(frame_bytes)-(len(string)*8*8))/8) * '#'
    bits = list(
        map(int, ''.join([bin(ord(i)).lstrip('0b').rjust(8, '0') for i in
string])))
    for i, bit in enumerate(bits):
        frame_bytes[i] = (frame_bytes[i] & 254) | bit
    frame_modified = bytes(frame_bytes)
    for i in range(0, 10):
        print(frame_bytes[i])
    newAudio = wave.open('Audio_1.wav', 'wb')
    newAudio.setparams(audio.getparams())
    newAudio.writeframes(frame_modified)

    newAudio.close()
    audio.close()
    print(" |----> Succesfully encoded inside Audio_1.wav")

    print("Applying Fernet Algorithm to Encript  Audio 1 file ")

    # opening the key
    with open('filekey.key', 'rb') as filekey:
        key = filekey.read()

    # using the generated key
    fernet = Fernet(key)

    # opening the original file to encrypt
    with open('Audio_1.wav', 'rb') as file:
        original = file.read()

    # encrypting the file
    encrypted = fernet.encrypt(original)

    # opening the file in write mode and
    # writing the encrypted data
    with open('Audio_1.wav', 'wb') as encrypted_file:
        encrypted_file.write(encrypted)

    print("Audio file encripted with Fernet Algorithm Successful ")

def decode():
```



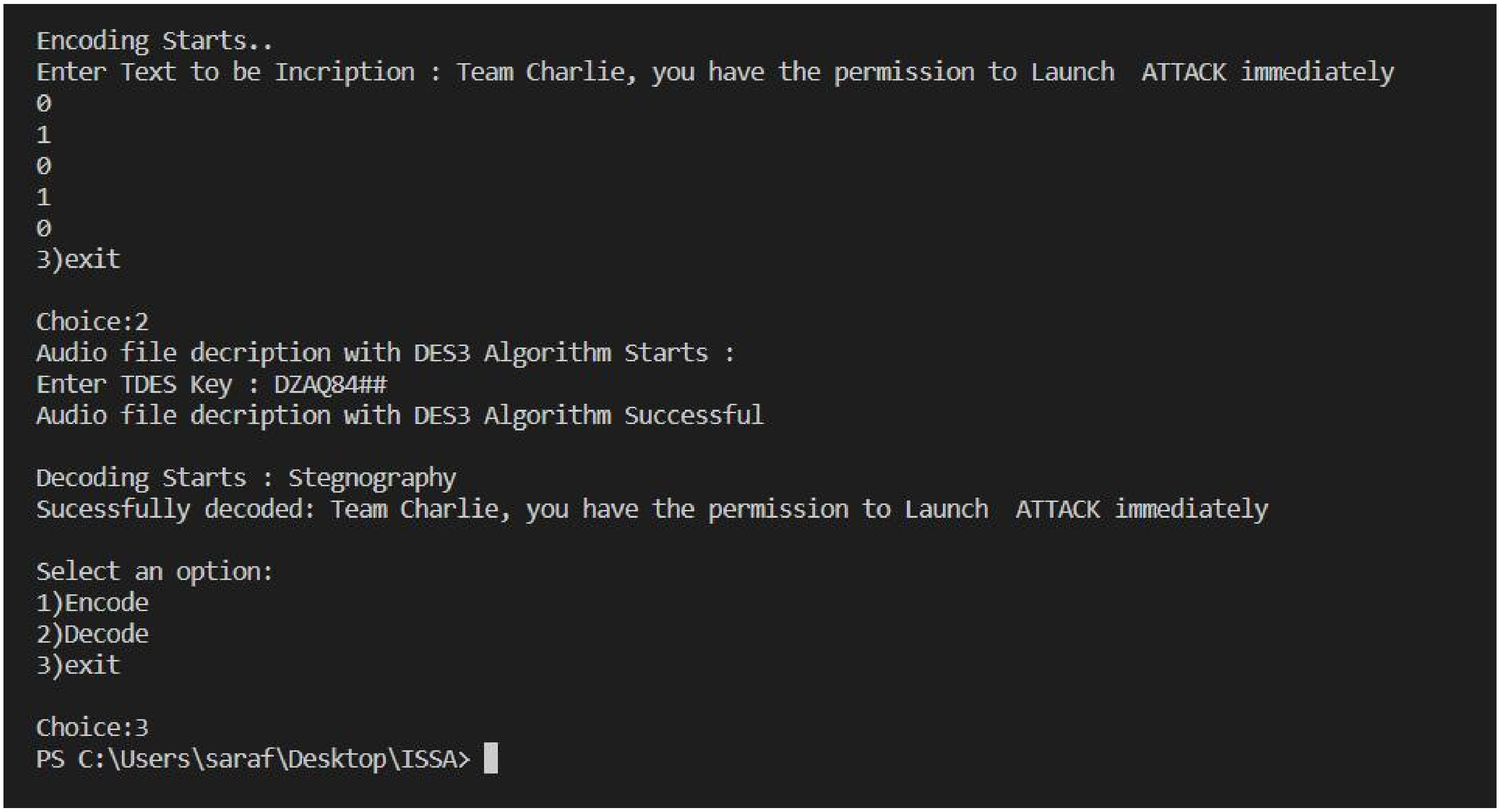
```
    print("Audio file decription with Fernet Algorithm Starts :")
    # using the key
    fernet = Fernet(key)

    # opening the encrypted file
    with open('Audio_1.wav', 'rb') as enc_file:
        encrypted = enc_file.read()

    # decrypting the file
    decrypted = fernet.decrypt(encrypted)

    # opening the file in write mode and
    # writing the decrypted data
    with open('Audio_1.wav', 'wb') as dec_file:
        dec_file.write(decrypted)

    print("Audio file decription with Fernet Algorithm Successful ")

    print("\nDecoding Starts : Stegnography ")
    audio = wave.open("Audio_1.wav", mode='rb')
    frame_bytes = bytearray(list(audio.readframes(audio.getnframes())))
    extracted = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
    string = "".join(chr(
        int("".join(map(str, extracted[i:i+8])), 2)) for i in range(0,
len(extracted), 8))
    decoded = string.split("###")[0]
    print("Sucessfully decoded: "+decoded)
    audio.close()



def main():
    while (1):
        print("\nSelect an option: \n1)Encode\n2)Decode\n3)exit")
        val = int(input("\nChoice:"))
        case(val)

if __name___ == "__main__":
    main()
```

# Output

# Steganography and Triple DES Algorithm



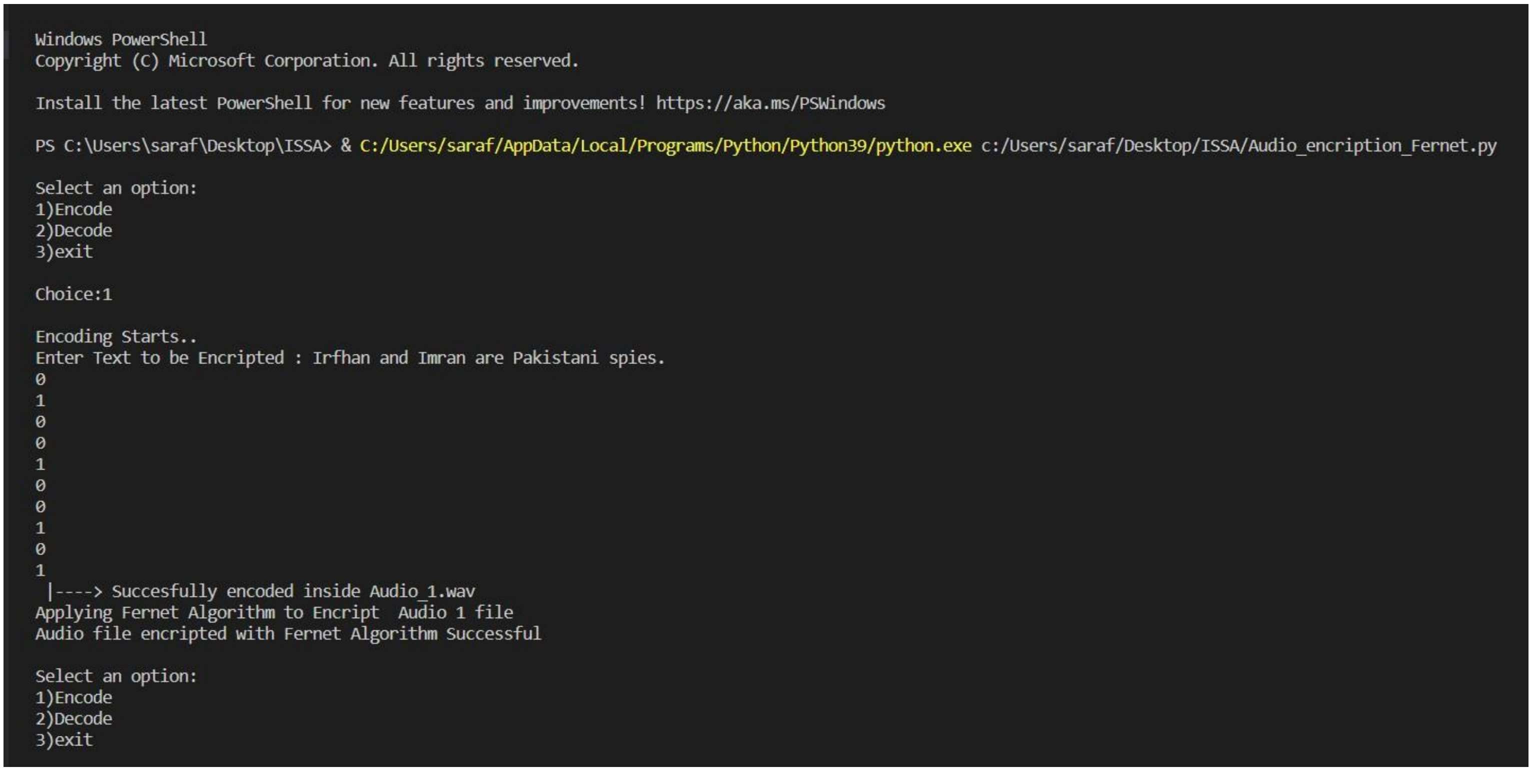
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\saraf\Desktop\ISSA> & C:/Users/saraf/AppData/Local/Programs/Python/Python39/python.exe c:/Users/saraf/Desktop/ISSA/Audio_encription1.py
Enter TDES Key : DZAQ84##

Select an option:
1)Encode
2)Decode
3)exit

Choice:1

Encoding Starts..
Enter Text to be Incription : Team Charlie, you have the permission to Launch  ATTACK immediately
0
1
0
1
0
3)exit
```



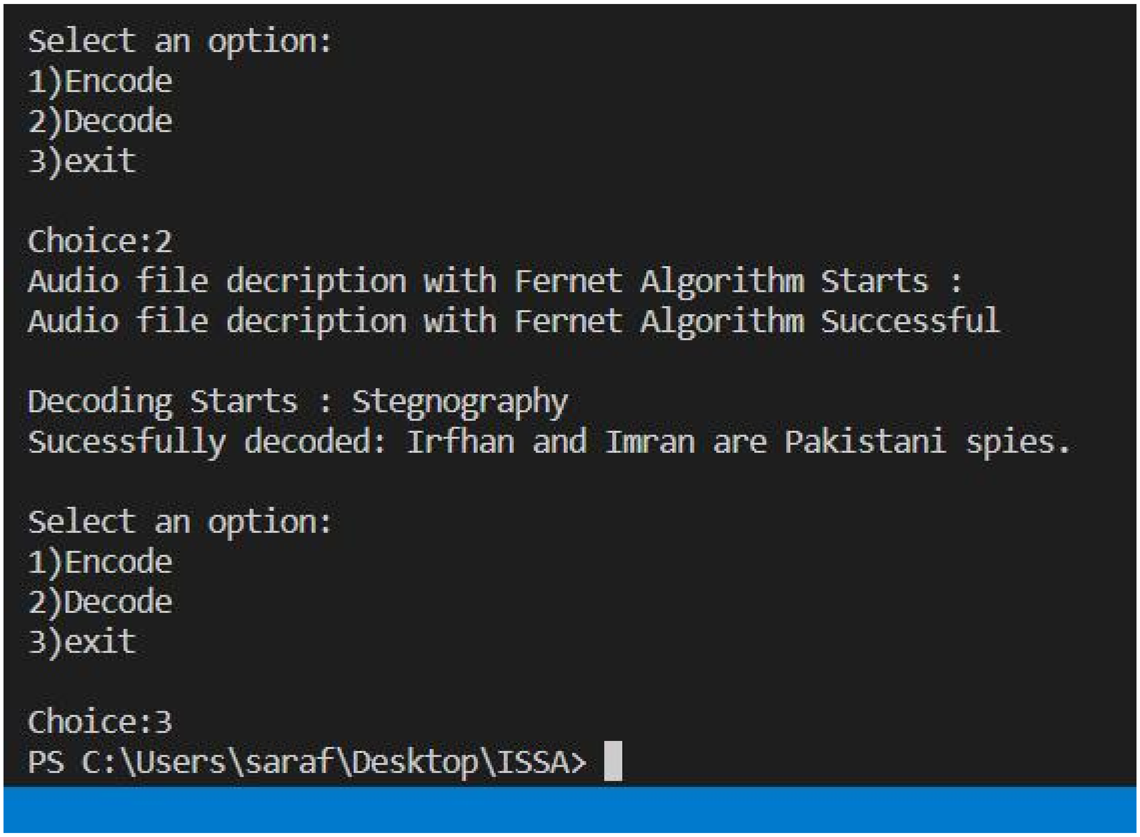
```
Encoding Starts..
Enter Text to be Incription : Team Charlie, you have the permission to Launch  ATTACK immediately
0
1
0
1
0
3)exit

Choice:2
Audio file decription with DES3 Algorithm Starts :
Enter TDES Key : DZAQ84##
Audio file decription with DES3 Algorithm Successful

Decoding Starts : Stegnography
Sucessfully decoded: Team Charlie, you have the permission to Launch  ATTACK immediately

Select an option:
1)Encode
2)Decode
3)exit

Choice:3
PS C:\Users\saraf\Desktop\ISSA> █
```

# Output

# Steganography and Fernet Algorithm



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\saraf\Desktop\ISSA> & C:/Users/saraf/AppData/Local/Programs/Python/Python39/python.exe c:/Users/saraf/Desktop/ISSA/Audio_encription_Fernet.py

Select an option:
1)Encode
2)Decode
3)exit

Choice:1

Encoding Starts..
Enter Text to be Encripted : Irfhan and Imran are Pakistani spies.
0
1
0
0
1
0
0
1
0
1
 |----> Succesfully encoded inside Audio_1.wav
Applying Fernet Algorithm to Encript  Audio 1 file
Audio file encripted with Fernet Algorithm Successful

Select an option:
1)Encode
2)Decode
3)exit
```



```
Select an option:
1)Encode
2)Decode
3)exit

Choice:2
Audio file decription with Fernet Algorithm Starts :
Audio file decription with Fernet Algorithm Successful

Decoding Starts : Stegnography
Sucessfully decoded: Irfhan and Imran are Pakistani spies.

Select an option:
1)Encode
2)Decode
3)exit

Choice:3
PS C:\Users\saraf\Desktop\ISSA>
```

# Conclusion

The main methods for data concealing in audio files have been thoroughly examined in this model.

In particular, the idea of Audio Steganography was discussed in this report of Steganography. Different audio steganography methods, including LSB Coding and Triple DES, were thoroughly discussed.

Finally, the viability of audio steganography was assessed by weighing its advantages and disadvantages. In conclusion, many of the data concealing techniques discussed above could be effective tools for the transmission of safe and untraceable communication if used properly and in conjunction with cryptographic techniques to secure the embedded data before insertion to a cover media.

**References:**

**[1]** Jayaram, & Ranganatha, & Anupama,. (2011). Information Hiding Using Audio Steganography - A Survey. The International journal of Multimedia & Its Applications. 3. 86-96. 10.5121/ijma.2011.3308.

**[2]** Kamred Udham Singh. Article: A Survey on Audio Steganography Approaches. *International Journal of Computer Applications* 95(14):7-14, June 2014.

**[3]** Shi, C. and B. Bhargava. Light-weight MPEG Video Encryption Algorithm. In Proceedings of the International Multimedia Conference on Multimedia,(Multimedia98, Shaping The Future) January 23-25, 1998, pages 55-61, New Delhi, India. IETE, Tata Mcgraw-Hill Publishing Company.

**[4]** Zheng Liu, Xue Li. Motion Vector Encryption in Multimedia Streaming. Proceedings of the 10th International Multimedia Modeling Conference. IEEE 2004.

**[5]** T. Vino, E. Logashanmugam. A Modelbased Multimedia Encryption Scheme for Real Time Videos. IEEE 2010.

**[6]** Wenjun Zeng and Shawmin Lei. Efficient frequency domain selective scrambling of digital video. In Proc. of the IEEE Transactions on Multimedia, 2002, pp. 118–129.

**[7]** Raphael Horvath, D. N. (2015). A Literature Review on Challenges and Effects of Software Defined Networking. Conference on ENTERprise Information Systems / International Conference on Project. Elsevier ScienceDirect Procedia Computer Science. doi:10.1016/j.procs.2015.08.563

**[8]** A discussion with Amin Vahdat, D. C. (2016, March). A Purpose-Built Global Network: Google's move to SDN. Communications of the ACM , 59(3), 46-54. doi:DOI:10.1145/2814326

**[9]** H. Li, P. L. (2014 ). Byzantine-resilient secure software defined networks with multiple controllers. Communications (ICC), IEEE International Conference, 695-700.

**[10]** Aditya Kotkar, Shreyas Khadapkar, Aniket Gupta, Smita Jangale, "Multiple layered Security using combination of Cryptography with Rotational, Flipping Steganography and Message Authentication", 2022 IEEE International Conference on Data Science and Information System (ICDSIS), pp.1-5, 2022.

**[11]** Putta Bharathi, Gayathri Annam, Jaya Bindu Kandi, Vamsi Krishna Duggana, Anjali T., "Secure File Storage using Hybrid Cryptography", 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp.1-6, 2021.

**[12]** Yue Zhao, Leyu Lin, Yiru Niu, Kaijun Wu, Yao Hao, Hong Su, Yarang Yang, "The Secure Computing Architecture for Dual Hard Disk and Dual System Switching", 2022 IEEE 5th International Conference on Big Data and Artificial Intelligence (BDAI), pp.125-129, 2022.

**[13]** Rini Indrayani, "Modified LSB on Audio Steganography using WAV Format", 2020 3rd International Conference on Information and Communications Technology (ICOIACT), pp.466-470, 2020.

**[14]** Artz, D. (2001). Digital Steganography: Hiding Data within Data. IEEE Internet Computing Journal, (June).

**[15]** Moerland, T.(2001). Steganography and Steganalysis. Leiden Institute of Advanced Computing Science. Accessed September 12, 2012. Available from www.liacs.nl/home/ tmoerl/privtech.pdf

**[16]** Chandramouli, R., Kharrazi, M. & Memon, N.(2003). Image steganography and steganalysis: Concepts and Practice. Proceedings of the 2nd International Workshop on Digital Watermarking, October.

**[17]** Sumartono, Isnar & Siahaan, Andysah Putera Utama & Arpan, Arpan. (2016). Base64 Character Encoding and Decoding Modeling. International Journal of Recent Trends in Engineering & Research. 2. 63-68.

**[18]** Dhany, Hanna & Izhari, Fahmi & Fahmi, Hasanul & Tulus, Tulus & Sutarman, Mr. (2018). Encryption and Decryption using Password Based Encryption, MD5, and DES. 10.2991/icoposdev-17.2018.57.

Fernet (symmetric encryption) using Cryptography module in Python - GeeksforGeeks

Comparative study of digital audio steganography techniques

What is Triple DES? - Definition from Techopedia

Symmetric Key Encryption - why, where and how it’s used in banking