JSS MAHAVIDYAPEETHA
JSS SCIENCE AND TECHNOLOGY UNIVERSITY
(Formerly Sri Jayachamarajendra College of Engineering)
JSS TECHNICAL INSTITUTIONS CAMPUS

*Digital Communication (EC610)*

***Event 2***

***Simulation Report on***

***"Speech Signal Encryption and Decryption using DES"***

**Submitted by**



| Sl. No. | USN | Name |
|---|---|---|
| 1 | 01JST16EC043 | Kevin Tom |
| 2 | 01JST16EC044 | Kuhoo Tiwari |
| 3 | 01JST16EC048 | Mohammad Safeel |



**Submitted to**

**Gayathri H M**
Associate Professor
Department of Electronics and Communication

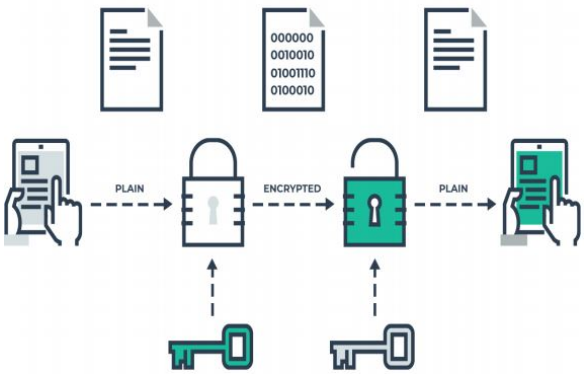
DEPARTMENT OF ELECTRONICS AND COMMUNICATION
JSS SCIENCE AND TECHNOLOGY UNIVERSITY
JSS TECHNICAL INSTITUTIONS CAMPUS
MYSURU 570006
(2018-2019)

# Contents

# 1 Introduction

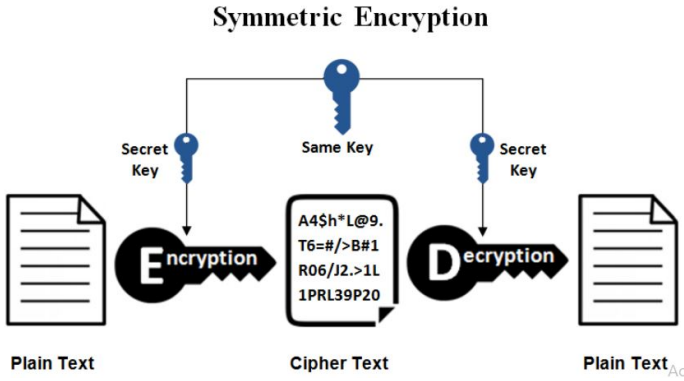
## 1.1 Encryption

It is a process whereby a message is encoded in a format that cannot be read or understood by an eavesdropper. It is the process of locking up information using cryptography. Involves a plain-text and a key. Two types of Encryption




### Symmetric Key

In symmetric encryption, you use the same key for both encryption and decryption of your data or message. Taking the example I gave above, sending a secure message to your granny, both of vou need to have the same kev in order to encrypt and decrypt the mess.




### Asymmetric Key

You use one to encrypt your data, which is called public key, and the other to decrypt the encrypted message, which is called the private key.
When you encrypt your message using, lets say, your grannys public key, that same message can only be decrypted using her private key.

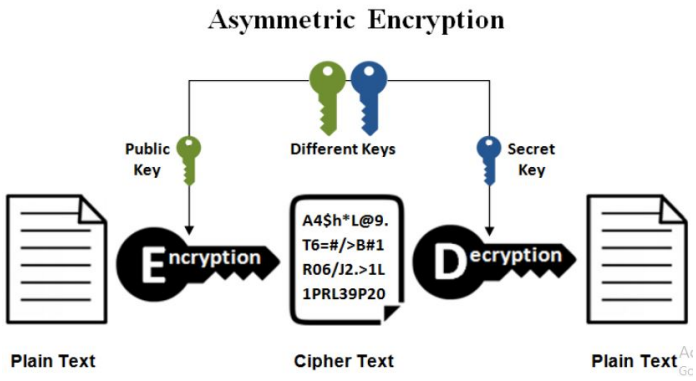
**Private keys**

Your private key, as the name states, is yours and it must be kept private, as its the only key that can decrypt any messaged that was encrypted with your public key.

**Public keys**

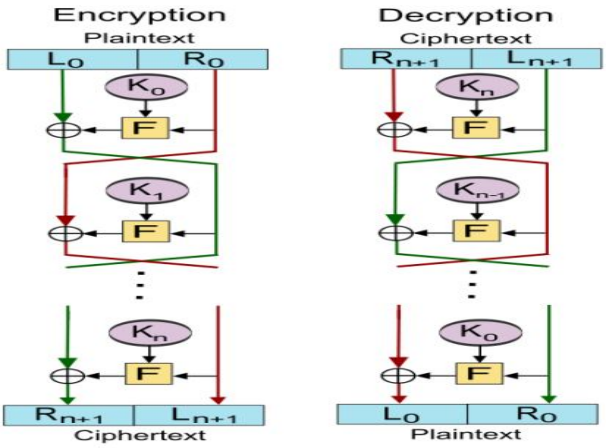
Public keys as, yet again, the name states, are public and thus no security is required because of it should publicly available and can be passed over the internet.

The public key is used to encrypt a message that can only be decrypted using, as I written above, its private counterpart.




## 1.2 DES Encryption

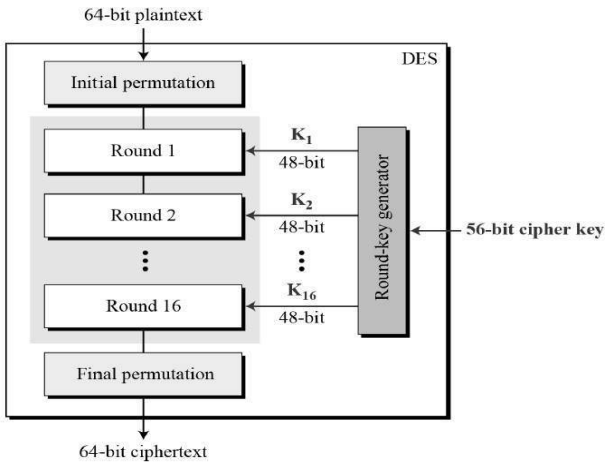
The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).




DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration.

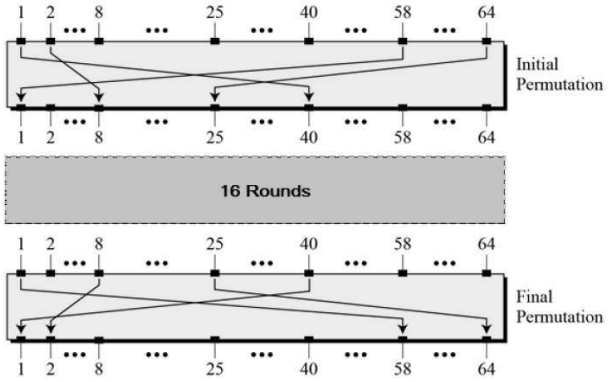
Since DES is based on the Feistel Cipher, all that is required to specify DES is

- Round function
- Key schedule
- Any additional processing  Initial and final permutation



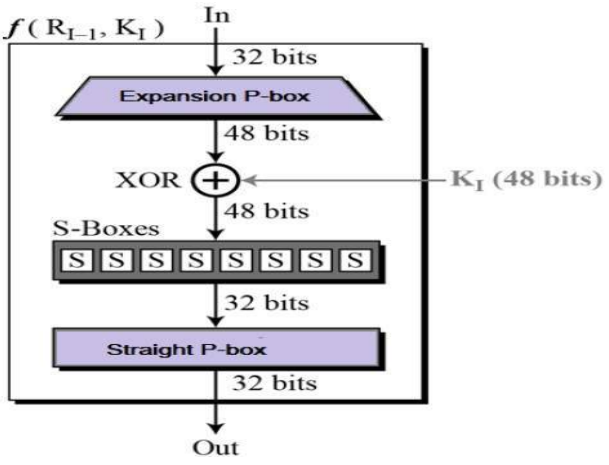

### Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as in figure.

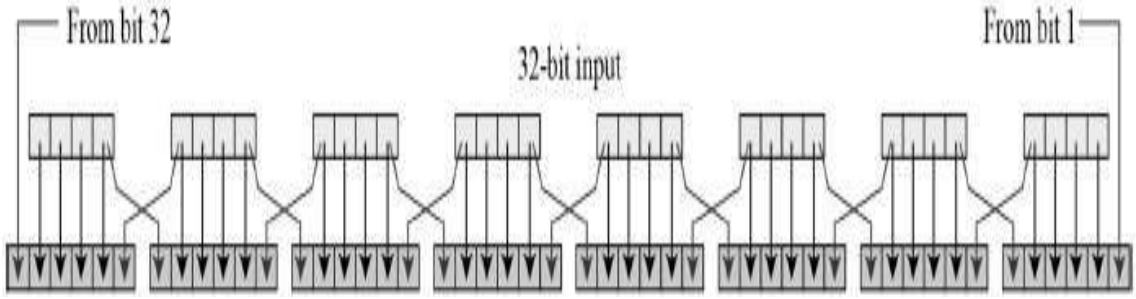



### Round Function

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



- Expansion Permutation Box Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration

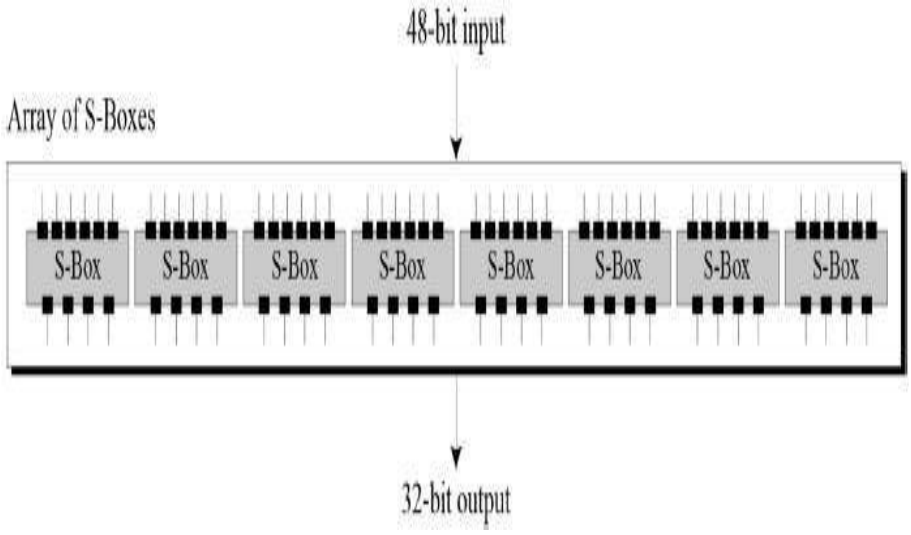


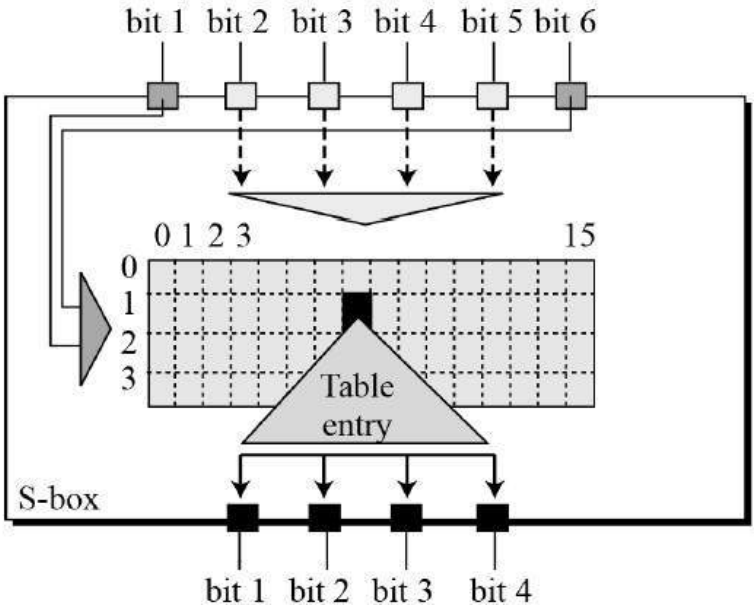

- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown

| | | | | | |
|---|---|---|---|---|---|
| 32 | 01 | 02 | 03 | 04 | 05 |
| 04 | 05 | 06 | 07 | 08 | 09 |
| 08 | 09 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 31 | 31 | 32 | 01 |

- XOR (Whitener). After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

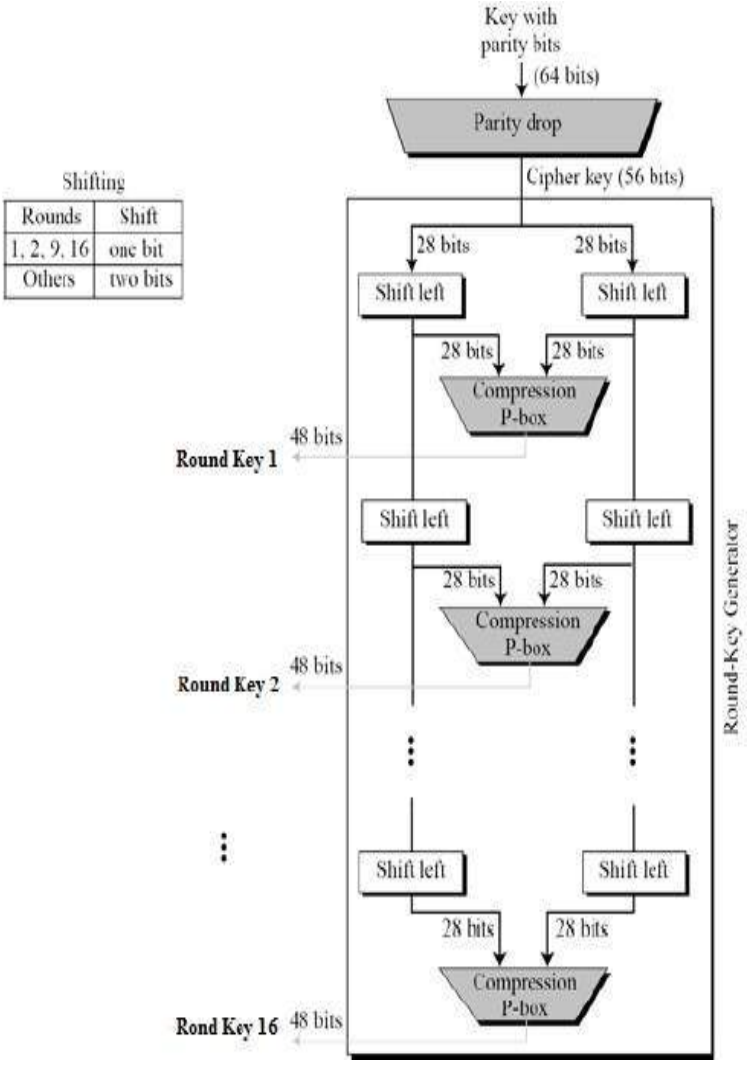
- Substitution Boxes. The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration





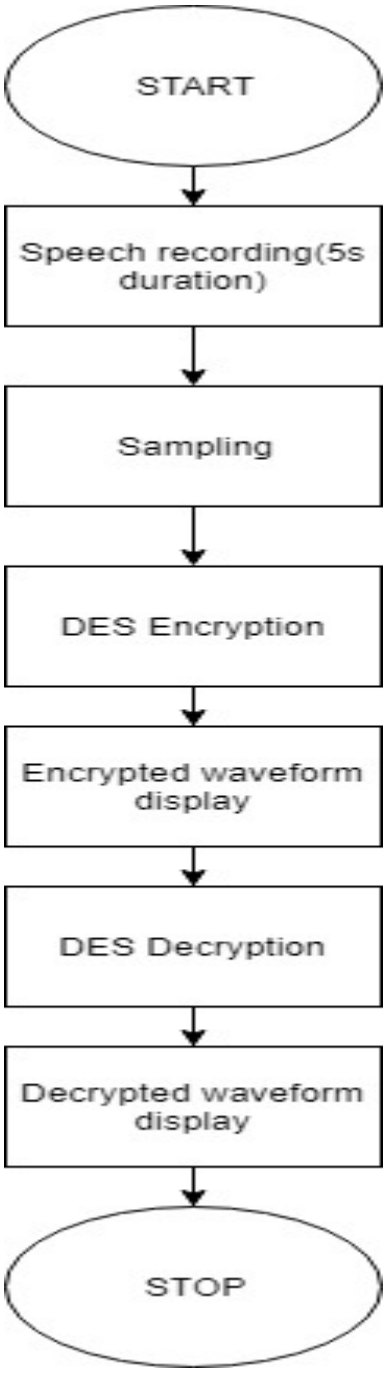

**Key Generation**

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration



# 2 FlowChart

The flow chart of our project and steps of how data flow is done in the program is given below. The recorded signal is sampled and applied to DES algorithm, then we give an encryption key, the encrypted wave is given as input to decryption algorithm and decryption key is given. If both keys are same we will get similar waves, Else we will get different waves.



# 3 Results

The resulting graphs given as output by the program is show below.

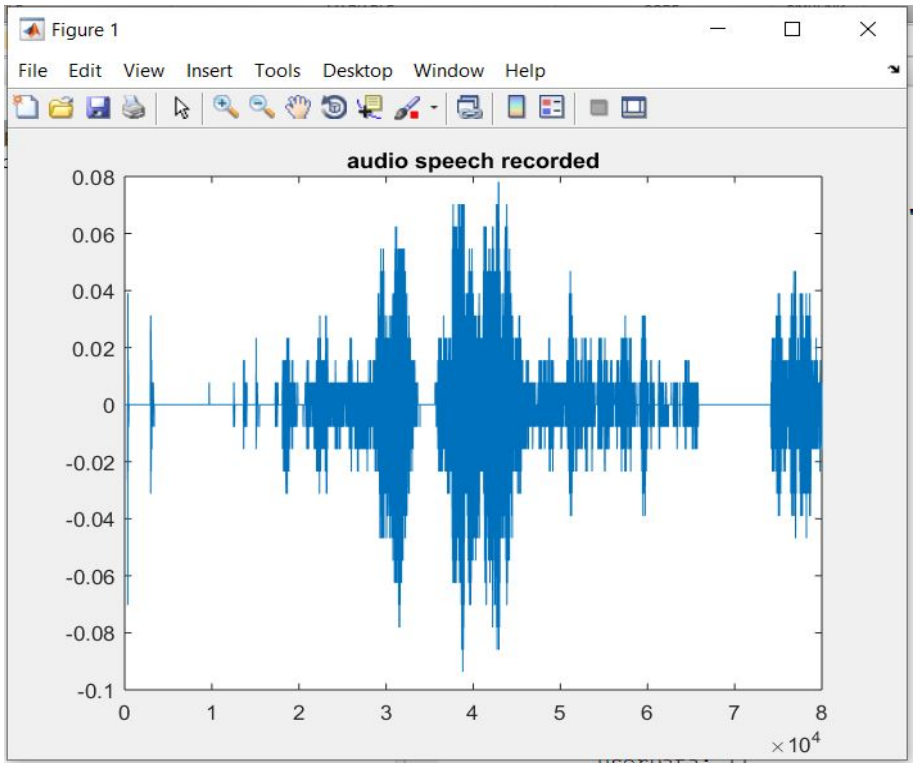



Figure 1: Recorded voice signal

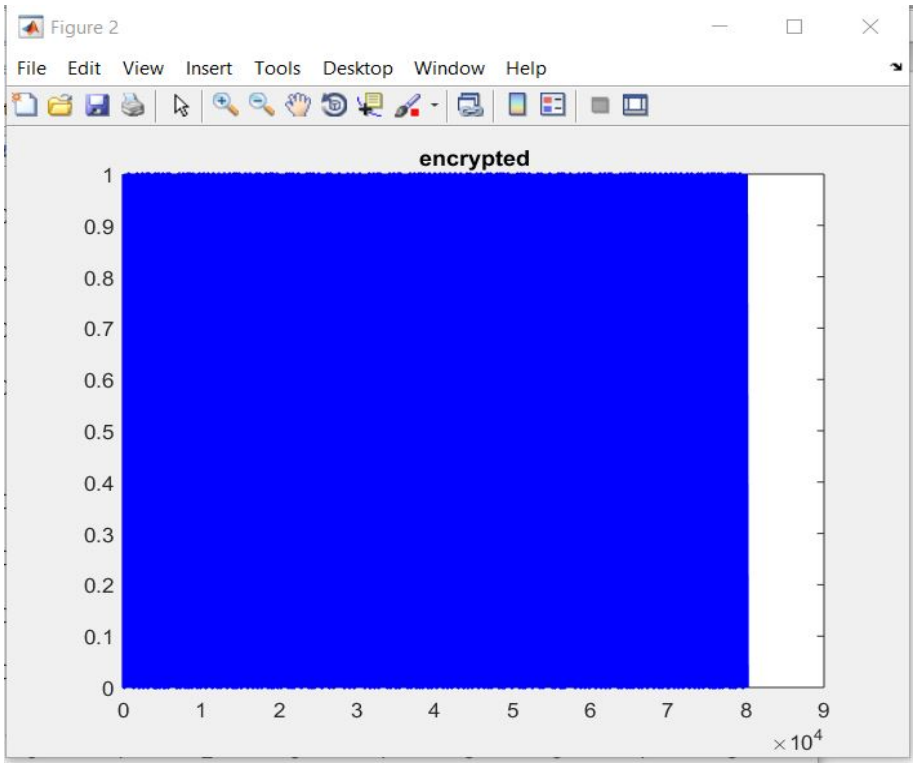



Figure 2: Encrypted voice signal

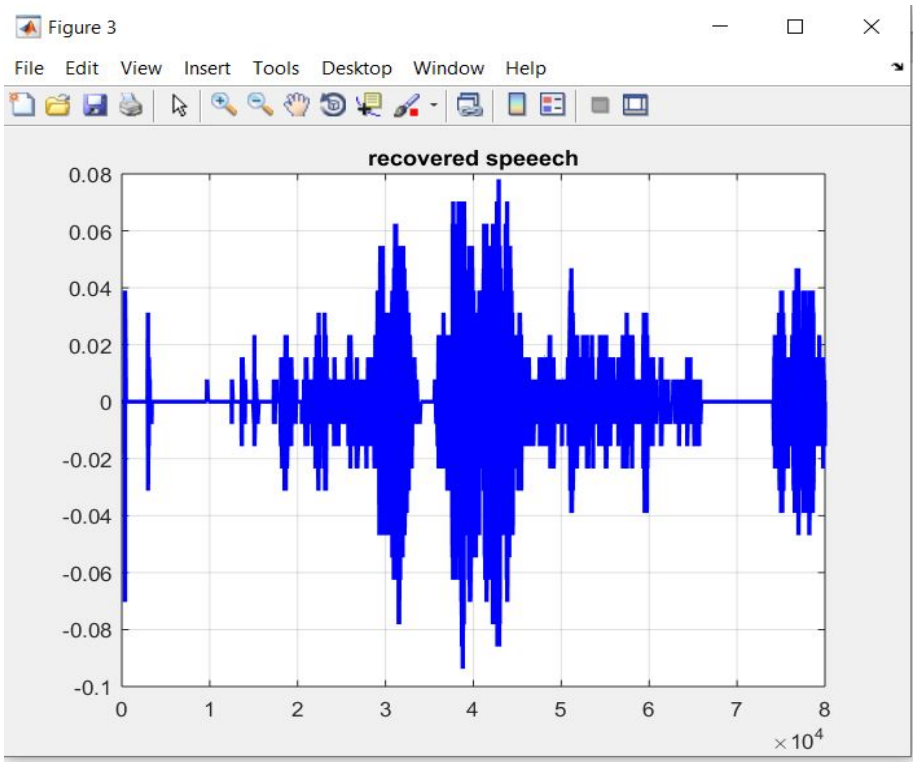



Figure 3: Recovered voice signal

# 4 Advantages

- Waveform is fully encrypted.
- It cannot be easily recognized by any speech recognition software.
- Decryption on possible using key
- Any coding techniques can be used since the output is in binary terms.

# 5 Disadvantages

- Symmetric key encryption-Less secure compared to asymmetric
- Key needs to be safely transmitted, any corruption in key will lead to wrong decryption.
- Complex implementation.
- Need for high computing power.
- Key can be found using Brut force attacks(Needs high computing power)

# 6 Applications

- Military applications
- Police radio
- End to end encryption
- Basis for higher encryption standards like Triple-DES.
- Used in different protocols

# 7 Scope for Future Work

The encryption of data is very important for security application. The terms of privacy are very strict and this necessities the use of data encryption techniques, the safe and secured transfer of data. The usage of DES Encryption enables to use any further encoding technique at d further stages which improves d data transmission quality.

# 8 Conclusion

Symmetric encryption algorithms are easy to implement and easy to use compared to asymmetric algorithms. They can be made secure by using a strong encryption key using a combination of letters and numbers. The longer the key, the more immune to Brut force attacks.
Decryption leads to some error, which are not recognizable to ears.The clarity of sound remains same, but some small parts may be lost(these are not recognizable). Hence DES algorithms can be used for short distance voice communication, unlike telephones, which can be tapped.

# 9 References


1. https://www.tutorialspoint.com/cryptography/dataencryptionstandard.htm
2. https://en.wikipedia.org/wiki/Sampling(signalprocessing)
3. https://en.wikipedia.org/wiki/Encryption
4. https://www.techopedia.com/definition/18091/brute-force-attack
5. https://docs.microsoft.com/en-us/windows/desktop/seccrypto/data-encryption-and-decryption