SPEECH SIGNAL ENCRYPTION & DECRYPTION USING DES

Prepared by,

Kevin Tom

Kuhoo Tiwari

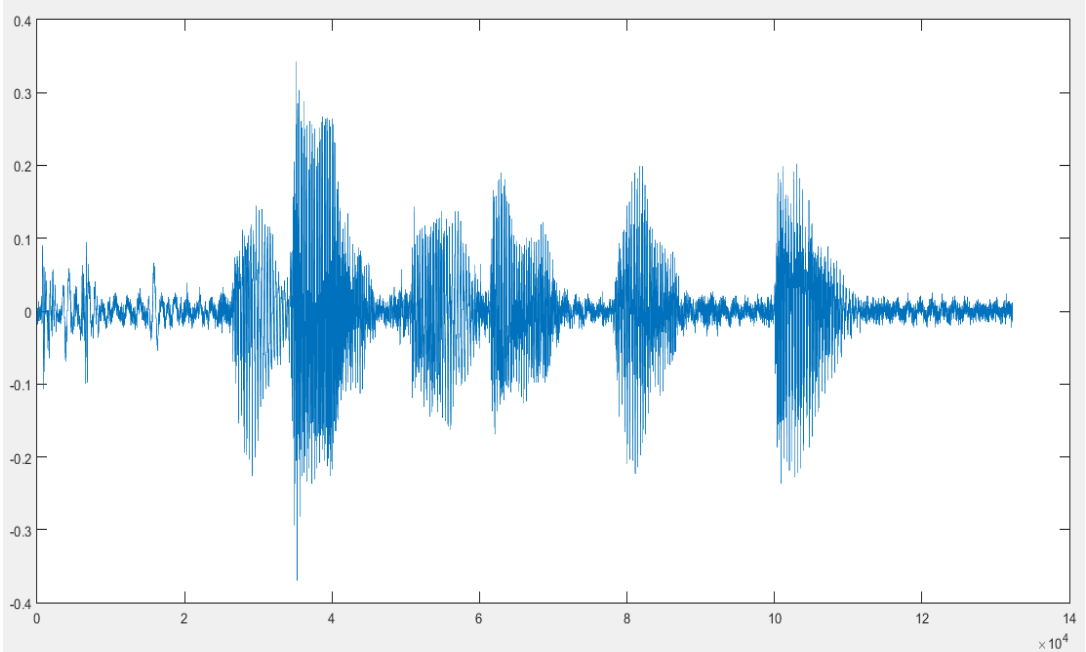
Mohammed Safeel

INTRODUCTION

- Our project is having 5 main steps:
  - **Speech recording(5s duration)**
  - **Sampling**
  - **DES Encryption**
  - **Encrypted waveform display**
  - **DES Decryption**
  - **Decrypted waveform display**

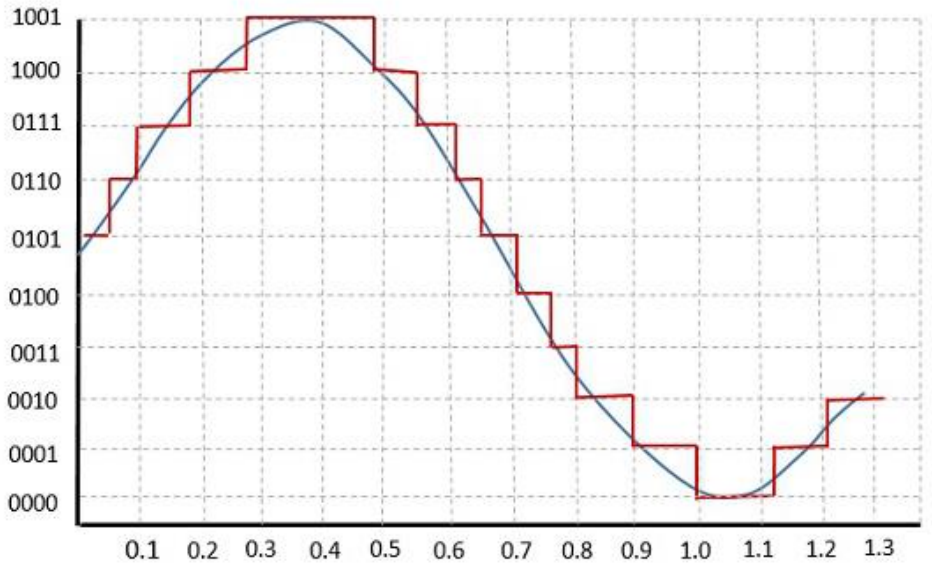
Speech sampling

- Speech signals, i.e., signals intended to carry only human speech, can usually be sampled at a much lower rate. For most phonemes, almost all of the energy is contained in the 100 Hz–4 kHz range, allowing a sampling rate of 8 kHz. This is the sampling rate used by nearly all systems, which use the G.711 sampling and quantization specifications.
- Our project also uses 8kHz of sampling rate for discretizing the speech signal.



Quantization

- **Quantization**, in mathematics and digital signal processing, is the process of mapping input values from a large set (often a continuous set) to output values in a (countable) smaller set, often with a finite number of elements.
- The difference between an input value and its quantized value (such as round-off error) is referred to as **quantization error**. A device or algorithmic function that performs quantization is called a **quantizer**.

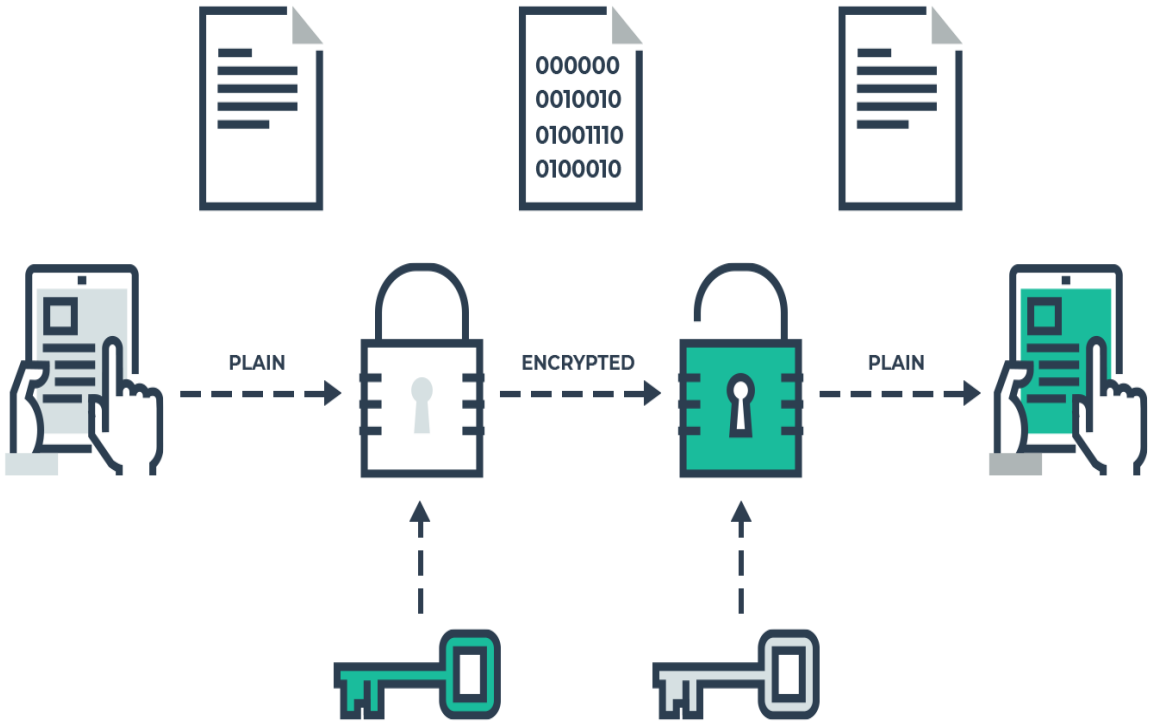


ENCRYPTION

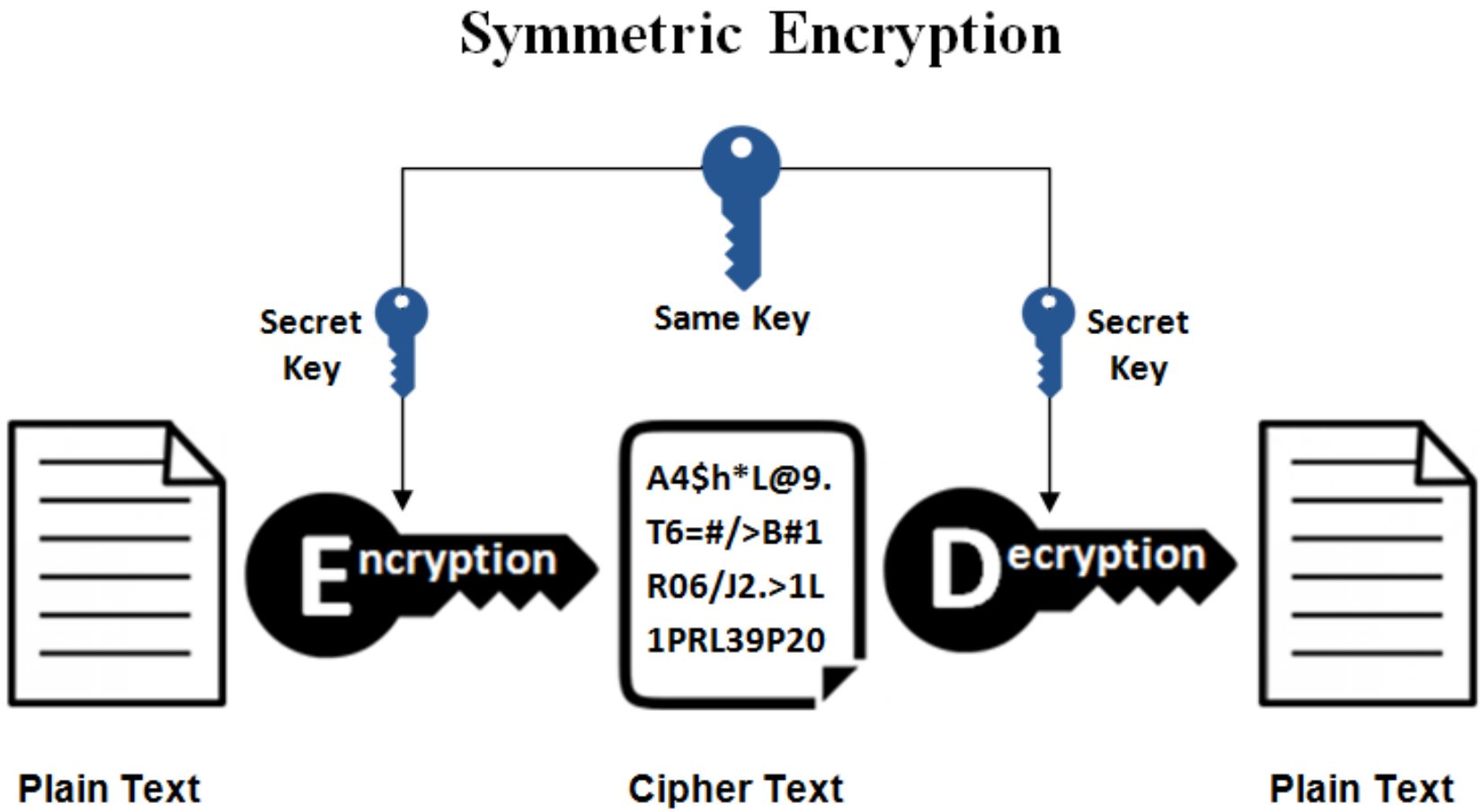
- It is a process whereby a message is encoded in a format that cannot be read or understood by an eavesdropper.
- It is the process of locking up information using cryptography.
- Two types of Encryption

  Symmetric Key

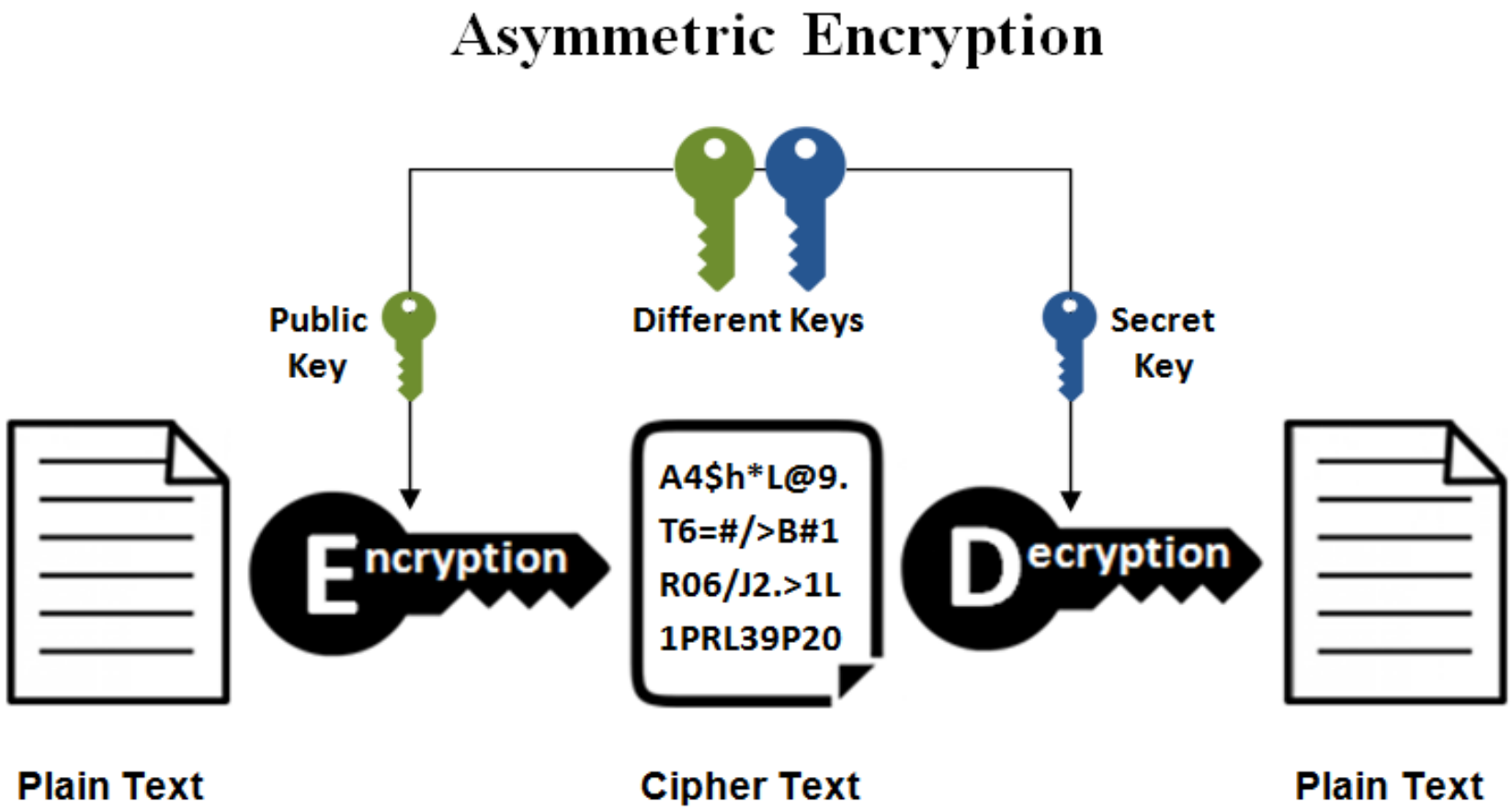
  Asymmetric Key
- Involves a plain-text and a key.



Symmetric-Key Encryption

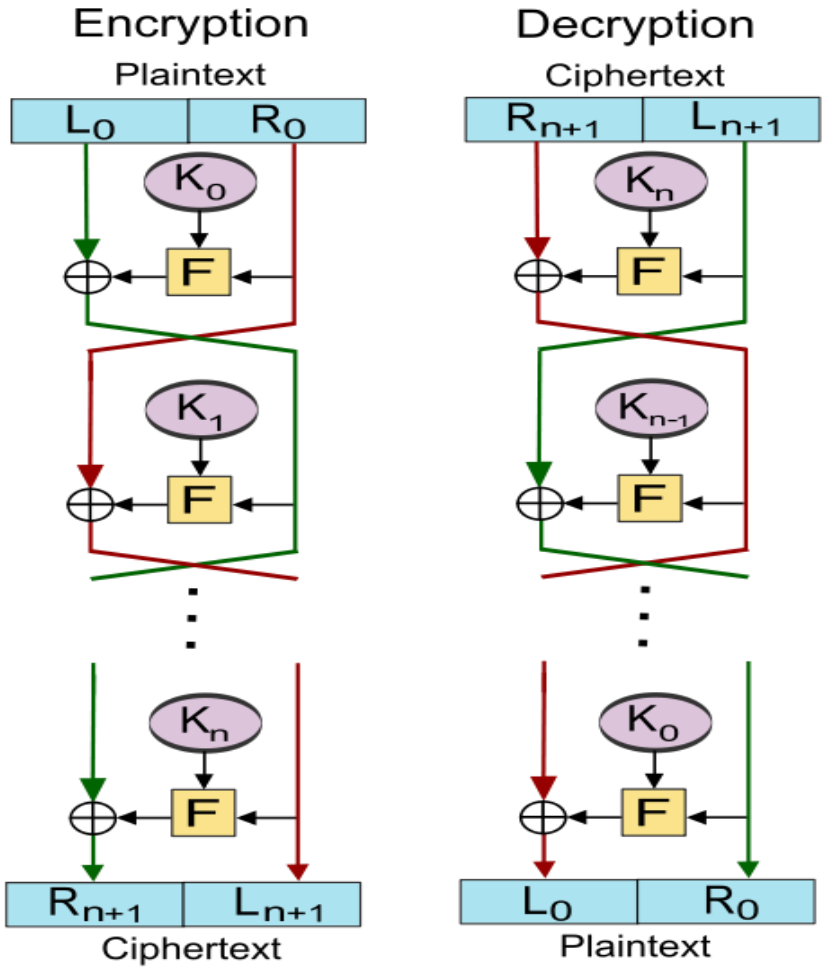


Asymmetric-Key Encryption

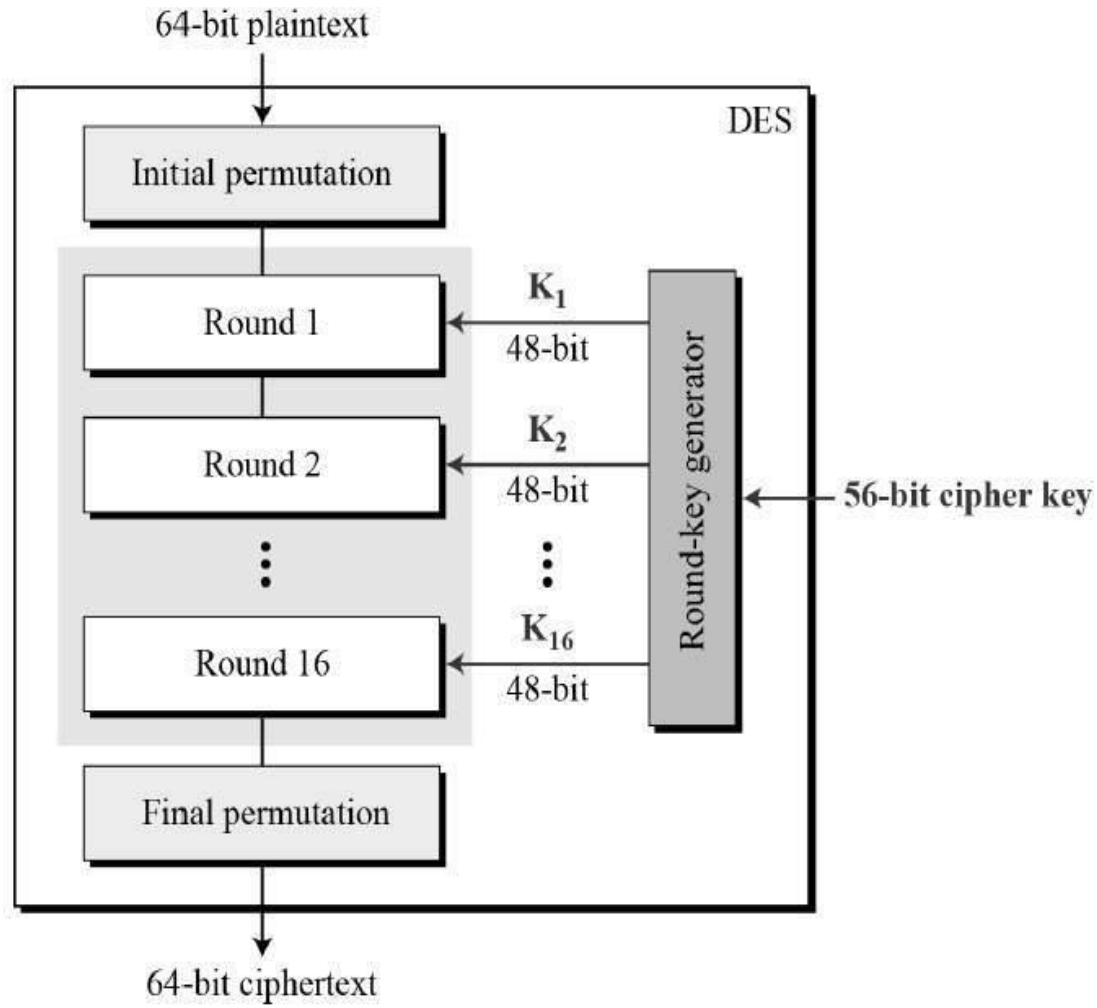


DES Encryption

- 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 next slide.



Flow diagram of DES

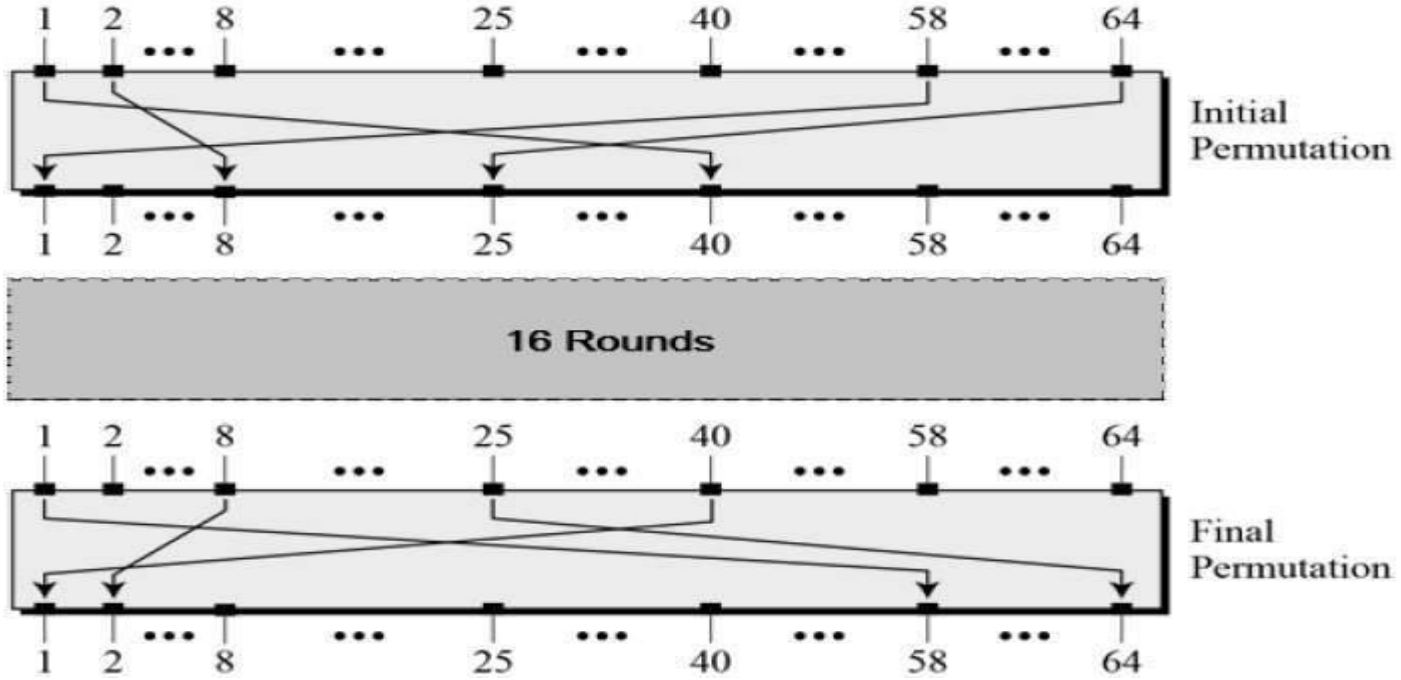


Since DES is based on the Feistel Cipher, all that is required to specify DES is −

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

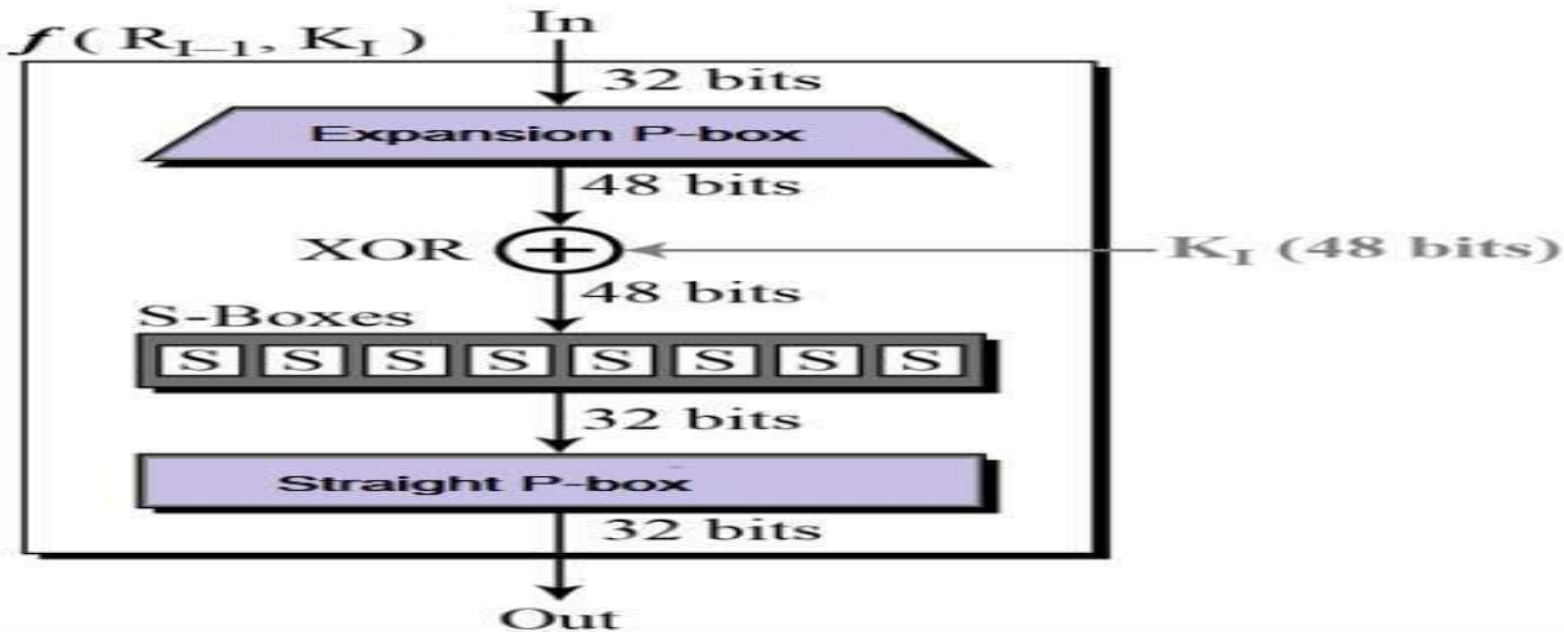
Initial and Final Permutation

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 follows −



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.

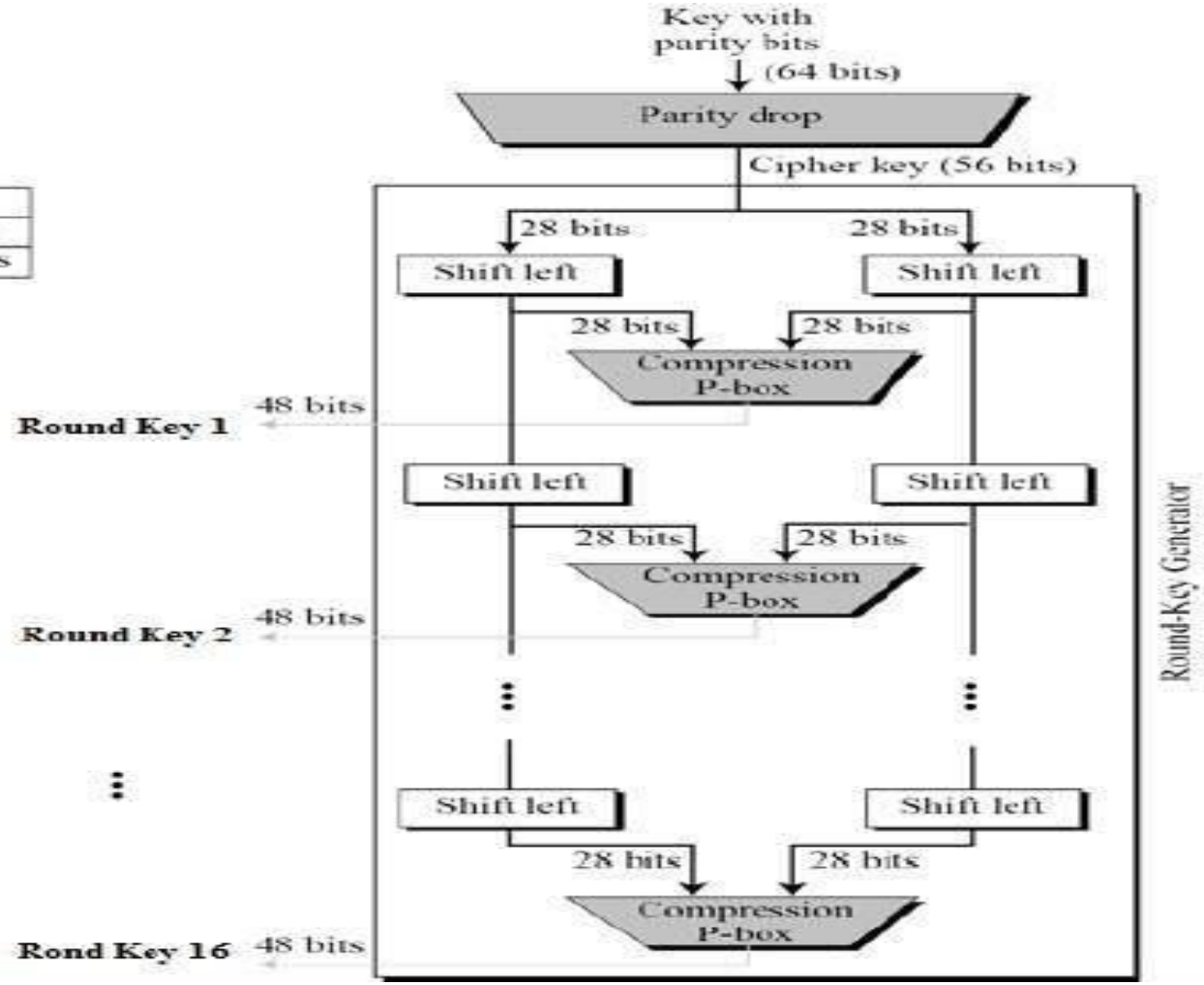


Key Generation

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 −

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



Simplified DES

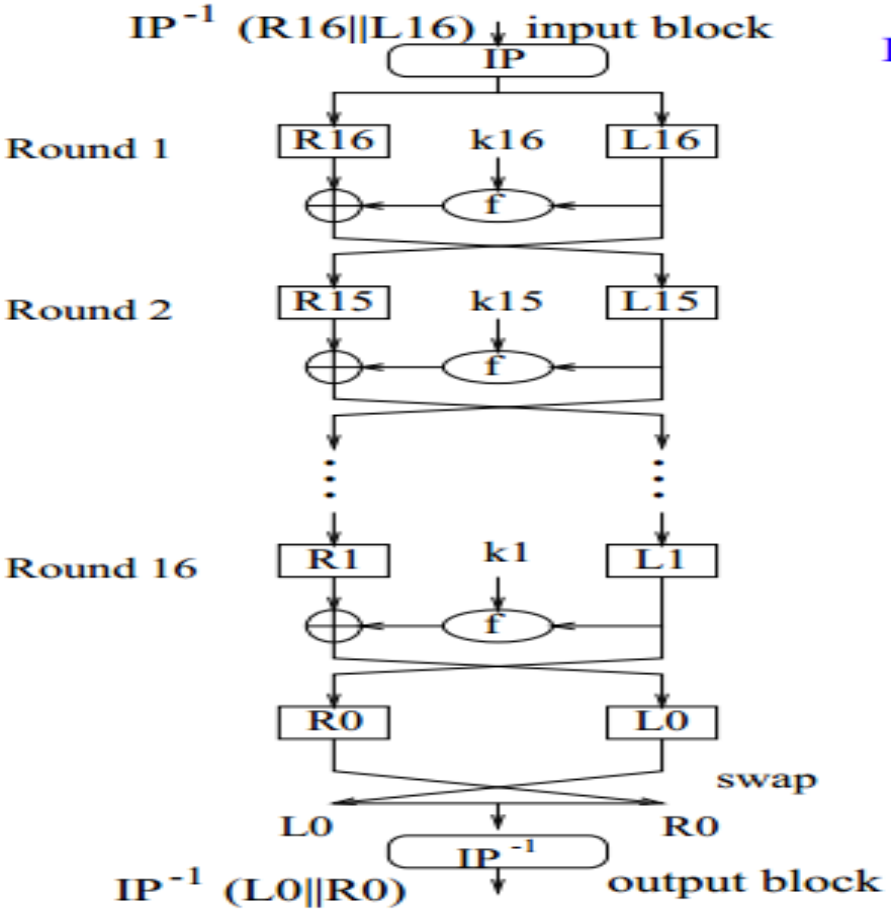
- Plaintext is broken into blocks of length 64 bits. Encryption is block wise.
- A message block is first gone through an initial permutation IP,then divided into two parts L_0,where L_0 is the left part of 32 bits and R_0 is the right part of the 32 bits
- Round i has input L_{i-1},R_{i-1} and output L_i,R_i $L_i = R_{i-1}$,$R_i = L_{i-1} \oplus f(R_{i-1},K_i)$ and K_i is the sub key for the 'i'th where $1 \le i \le 16$

$L_1 = R_0$, $R_1 = L_0 \oplus f(R_0,K_1)$
$L_2 = R_1$, $R_2 = L_1 \oplus f(R_1,K_2)$
$L_3 = R_2$, $R_3 = L_2 \oplus f(R_2,K_3)$
....
....
....
$L_{16} = R_{15}$, $R_{16} = L_{15} \oplus f(R_{15},K_{16})$

- After round 16,L_{16} and R_{16} are swapped, so that the decryption algorithm has the same structure as the encryption algorithm.
- Finally, the block is gone through the inverse the permutation IP^{-1} and then output

DES DECRYPTION

- Observation : In encryption, we have $L_i = R_{i-1}, R_i = R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
- and K_i is the sub key for the 'i'th round. Hence $R_{i-1} = L_i, L_{i-1} = R_i \oplus f(L_i, K_i)$ for each 'i'



- Due to swap operation after the 16th round encryption,the output of encryption is $IP^{-1}(R_{16},L_{16})$
- Equation(1) as follows:

$$\mathbf{R_{15} = L_{16},\quad L_{15} = R_{16} \oplus f(L_{16},K_{16})}$$
$$\mathbf{R_{14} = L_{15},\quad L_{14} = R_{15} \oplus f(L_{15},K_{15})}$$
$$\mathbf{R_{13} = L_{14},\quad L_{13} = R_{14} \oplus f(L_{14},K_{14})}$$
$$\mathbf{.....\qquad .....}$$
$$\mathbf{.....\qquad .....}$$
$$\mathbf{.....\qquad .....}$$
$$\mathbf{R_1 = L_2,\quad L_1 = R_2 \oplus f(L_2,K_2)}$$

- If we give $IP^{-1}(R_{16},L_{16})$ as the input for the same algorithm with round subkeys($K_{16},K_{15},.....K_1$), then the output is $IP^{-1}(L_0,R_0)$,the original message block
- Decryption is performed using the same algorithm, except the K_{16} is used as the first round,K_{15} in the second, and so on, with K_1 used in the 16th round

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.

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).

Applications

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

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.