JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

"बेटी बचाओ, बेटी पढ़ाओ"

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name – Cryptography and Network Security

Session no.: 12

Session Name- Data Encryption Standard

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

Review of previous Session **– Block Cipher Techniques**

Topic to be discussed today- Today We will discuss about **Data Encryption Standard**

Lesson deliverance (ICT, Diagrams & Live Example)-

- ➢ Diagrams

Introduction & Brief Discussion about the Topic **– Data Encryption Standard**

Data Encryption Standard

In May 1973, and again in Aug 1974 the NBS (now NIST) called for possible encryption algorithms for use in unclassified government applications response was mostly disappointing, however IBM submitted their Lucifer design following a period of redesign and comment it became the Data Encryption Standard (DES)

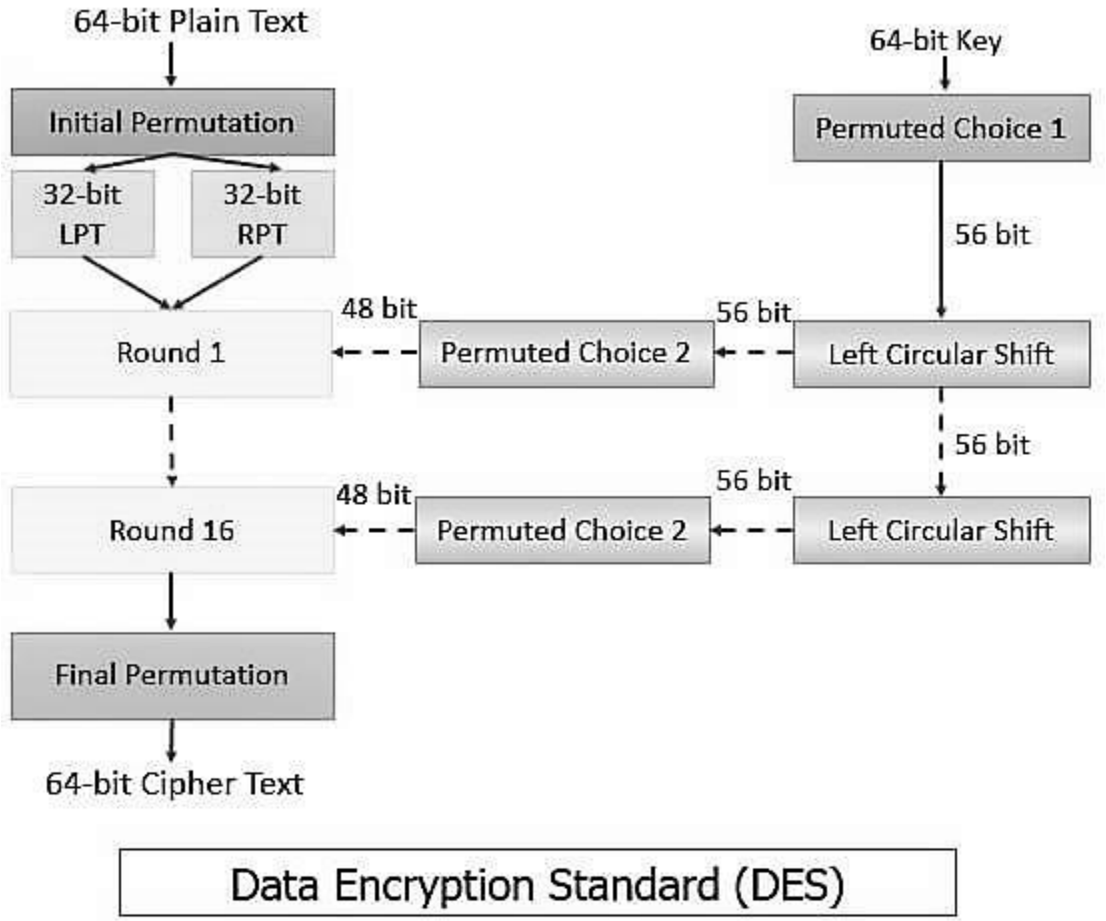
it was adopted as a (US) federal standard in Nov 76, published by NBS as a hardware only scheme in Jan 77 and by ANSI for both hardware and software standards in ANSI X3.92-1981 (also X3.106-1983 modes of use) subsequently it has been widely adopted and is now published in many standards around the world of Australian Standard AS2805.5-1985

one of the largest users of the DES is the banking industry, particularly with EFT, and EFTPOS

it is for this use that the DES has primarily been standardized, with ANSI having twice reconfirmed its recommended use for 5-year periods - a further extension is not expected however although the standard is public, the design criteria used are classified and have yet to be released there has been considerable controversy over the design, particularly in the choice of a 56-bit key

- Recent analysis has shown despite this that the choice was appropriate, and that DES is well designed
- Rapid advances in computing speed though have rendered the 56-bit key susceptible to exhaustive key search, as predicted by Diffie & Hellman
- The DES has also been theoretically broken using a method called Differential Cryptanalysis, however in practice this is unlikely to be a problem (yet)

Overview of the DES Encryption Algorithm



- the basic process in enciphering a 64-bit data block using the DES consists of:
    - an initial permutation (IP)
    - 16 rounds of a complex key dependent calculation f
    - a final permutation, being the inverse of IP
- In more detail, one of the 16 rounds of f consist of:

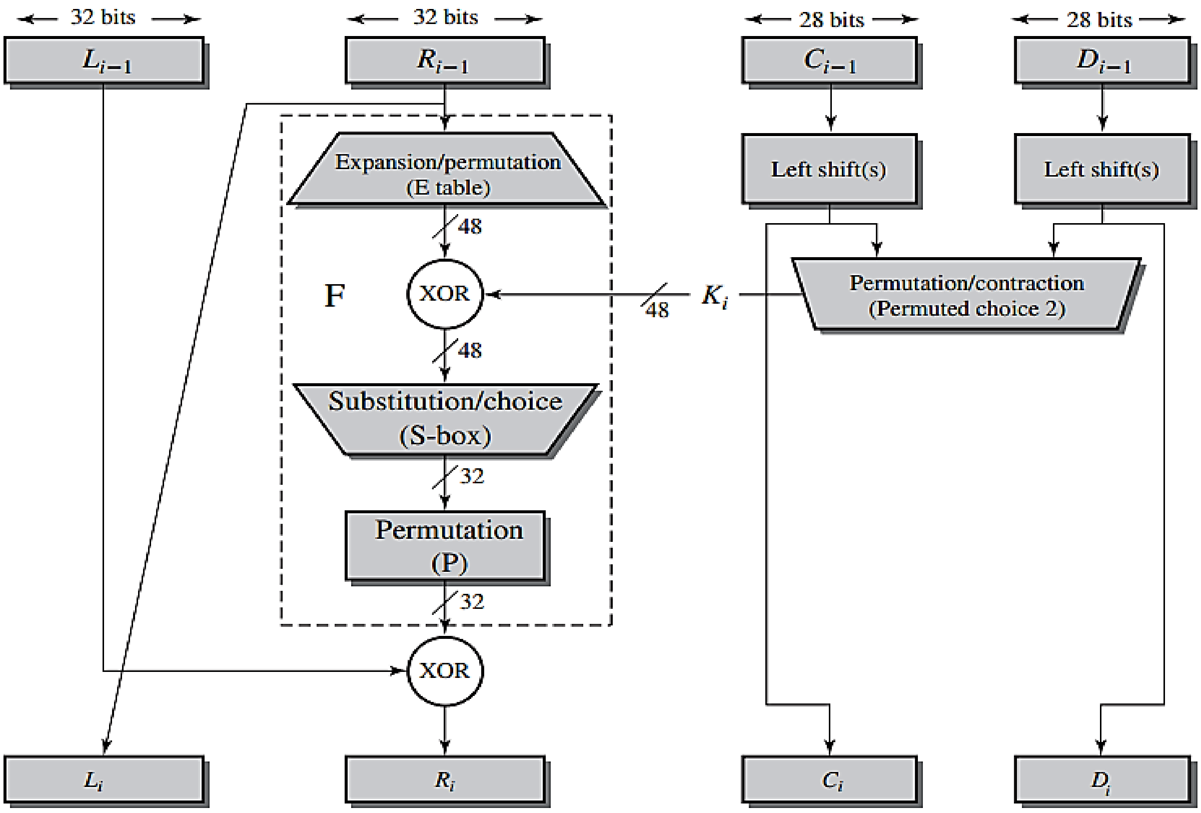


Fig. 2 Single Round of DES Algorithm

- this can be described functionally as

L(i) = R(i-1)

R(i) = L(i-1) (+) P (S(E(R(i-1)) (+) K(i)))

and forms one round in an S-P network

- the subkeys used by the 16 rounds are formed by the **key schedule** which consists of:
  - an initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves
  - 16 stages consisting of
  - selecting 24-bits from each half and permuting them by PC2 for use in function f,
  - rotating each half either 1 or 2 places depending on the **key rotation schedule** KS

- This can be described functionally as: K(i) = PC2(KS(PC1(K),i))

The key rotation schedule KS is specified as:																
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
KS	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
Total Rot	1	2	4	6	8	10	12	14	15	17	19	21	23	25	27	28

Reference-

1. **Book:** William Stallings, “Cryptography & Network Security”, Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. What is the sub-key size of DES?

Q2. What are two algorithms are used in DES?

Q3. Explain the data encryption standard algorithm.

Next, we will discuss about Data Encryption Standard modes of use.

- Academic Day ends with-
  National song ‘Vande Mataram’