Sheet 3
Computer/Information/Network Security
For CS , IS , IT 4th Year ,3rd Year IT

---

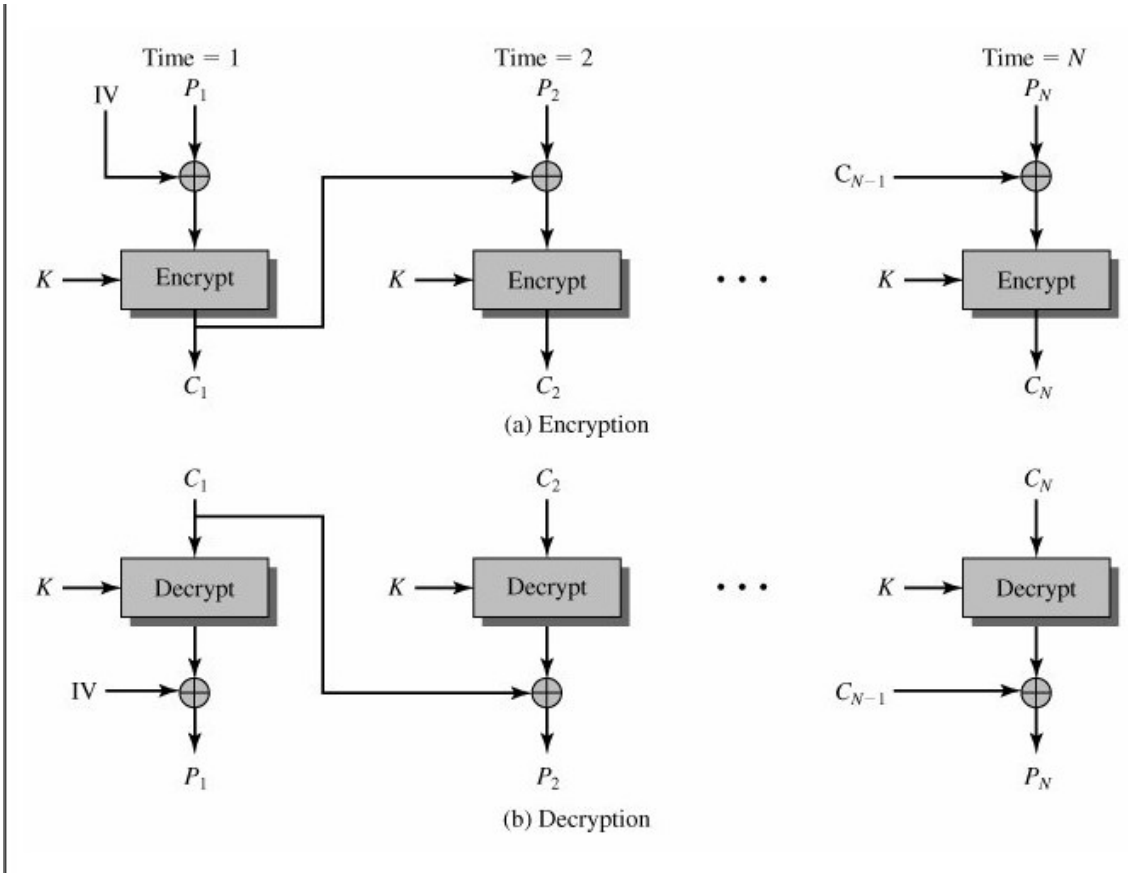
1. **If we have a computer that can test 2^{40} keys each second, what is the expected time to find a key by exhaustive key search if the keyspace is of size 2^{128}? Give your answer in years**.

   ¿ $\frac{2^{128}}{2^{40}} * 60^{-2} * 24^{-1} * 365^{-1}\ Year$

2. **Draw diagrams to illustrate encryption and decryption in CBC mode.**

   $Ci = E(P_i \oplus C_{i-1}, K)$ for $i = 0, 1, 2, \ldots$

   $Pi = D(C_i, K) \oplus C_{i-1}$ for $i = 0, 1, 2, \ldots$



3. **Compare between DES Block cipher modes in terms of operation and applications**

Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed j bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

4. **Describe the meet-in-middle attack.**
   It is used for double DES
   $C = E(E(P, K1), K2)$.
   - This attack is a chosen plaintext attack.

- We select a particular plaintext *P* and obtain the corresponding ciphertext *C*.
- Our goal is to find the keys K_1 and K_2 in *the previous equation.*
- First we precompute a table of size 2^{56} containing the pairs *E(P, K)* and *K* for all possible key values *K*.
- We sort this table on the values *E(P,K)*. Now given this table and the ciphertext value *C* corresponding to the chosen *P*, we decrypt *C* with keys $K\tilde{}$ until we find a value $D(C, K\tilde{})$ that is in table.
- The value that we find in the table will be *E(P,K)* for some *K* and we have
  $D(C, K)\tilde{} = E(P,K)$
  where $K\tilde{}$ and *K* are known.
- That we have found the 112-bit key can be seen by encrypting
  both sides with $K\tilde{}$, which gives
  $C = E(E(P,K), K\tilde{})$ that is, $K_1 = K$ and $K_2 = K\tilde{}$.

5. **For the DES highlight the operations that supports confusion and the other that supports diffusion.**

   S-box Confusion

   P-box Diffusion

   Expansion Permutation Confusion (Permutations) and Diffusion (Expansion)

   Usage of round key Confusion and Diffusion

6. **Consider a Feistel cipher with four rounds and *P = (L0,R0)*. What is the ciphertext *C* if the round function is**
   a. *F(Ri−1,Ki)* = 0.
   b. *F(Ri−1,Ki)* = *Ri−1* .
   c. *F(Ri−1,Ki)* = *Ki* .
   d. *F(Ri−1,Ki)* = *Ri−1* ⊕ *Ki* .

Solution

For feistel

$Li = Ri-1$
$Ri = Li-1 \oplus F(Ri-1, Ki)$

L1 = R0 , R1 = L0⊕0=L0

L2 = R1 , R2 = L1⊕0=L1

L3 = R2 , R3 = L2⊕0=L2

L4 = R3=L2=R1=L0 , R4 = L3⊕0=L3=R2=L1=R0

The same Procedure will be used for parts b , c ,d.

7. **For the following image and its cipher (ECB block mode) discuss the problem and suggest a solution**

Problem is : ECB same plain gives same cipher

Solution : use CBC

8. **Draw a wire diagram illustrates the operation of a DES round.**

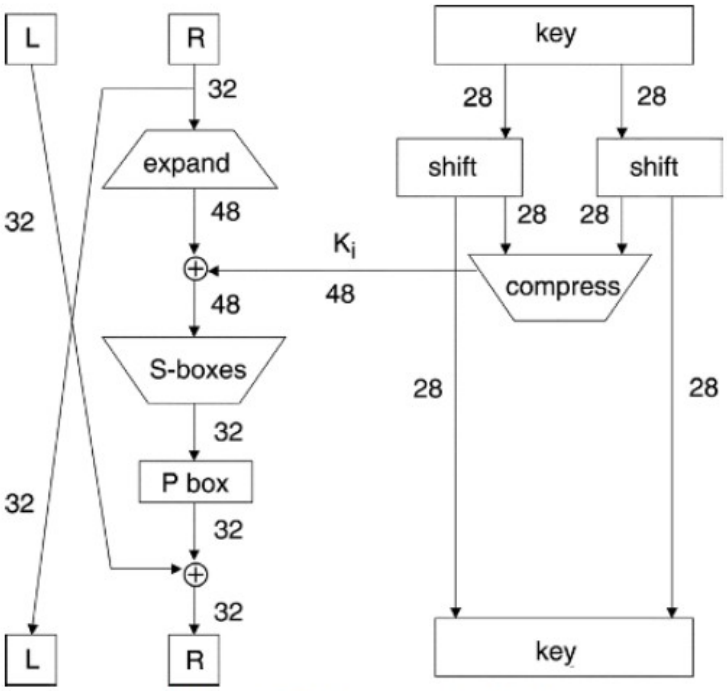


Figure 3.2. One round of DES.

9. **DES swaps the output of the final round, that is, the ciphertext is not $C = (L_{16}, R_{16})$ but instead is $C = (R_{16}, L_{16})$. What is the purpose of this swap?**
Hint: The swap serves no security purpose.

From the figure below the last swap aims to sustain reversibility in case of decryption and making the algorithm suitable for encrypt and decrypt.