Goa College Of Engineering

Expt No: 8 **Perform Cryptanalysis On A Ciphertext** Date:

Aim:

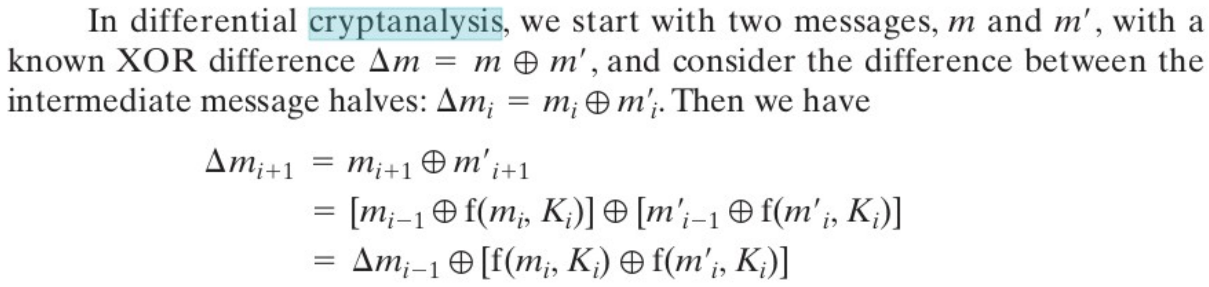
Theory:

- For most of its life, the prime concern with DES has been its vulnerability to brute-force attack because of its relatively short (56 bits) key length.
- However, there has also been interest in finding cryptanalytic attacks on DES. With the increasing popularity of block ciphers with longer key lengths, including triple DES, brute-force attacks have become increasingly impractical.
- Thus, there has been increased emphasis on cryptanalytic attacks on DES and other symmetric block ciphers.

- Differential Cryptanalysis
  - One of the most significant advances in cryptanalysis in recent years is differential cryptanalysis.
  - Differential cryptanalysis was not reported in the open literature until 1990.
  - The first published effort appears to have been the cryptanalysis of a block cipher called FEAL by Murphy. This was followed by a number of papers by Biham and Shamir, who demonstrated this form of attack on a variety of encryption algorithms and hash functions; their results are summarized in.
  - Differential cryptanalysis is the first published attack that is capable of breaking DES in less than 2^{55} encryptions. The scheme, as reported in, can successfully cryptanalyze DES with an effort on the order of 2^{47} encryptions, requiring 2^{47} chosen plaintexts. Although 2^{47} is certainly significantly less than 2^{55} , the need for the adversary to find 2^{47} chosen plaintexts makes this attack of only theoretical interest.

- DIFFERENTIAL CRYPTANALYSIS ATTACK
  - The differential cryptanalysis attack is complex; provides a complete description. The rationale behind differential cryptanalysis is to observe the behavior of pairs of text blocks evolving along each round of the cipher, instead of observing the evolution of a single text block. Here, we provide a brief overview so that you can get the flavor of the attack.
  - We begin with a change in notation for DES. Consider the original plaintext block m to consist of two halves m 0 , m 1 . Each round of DES maps the right-hand input into the left-hand output and sets the right-hand output to be a function of the left-hand input and the subkey for this round. So, at each round, only one new 32-bit block is created. If we label each new block m_i (2 <= i <= 17) , then the intermediate message halves are related as follows:

$$m_{i+1} = m_{i-1} \oplus \mathrm{f}(m_i, K_i), \qquad i = 1, 2, \ldots, 16$$



In differential cryptanalysis, we start with two messages, m and m', with a known XOR difference $\Delta m = m \oplus m'$, and consider the difference between the intermediate message halves: $\Delta m_i = m_i \oplus m'_i$. Then we have

$$\begin{aligned}\Delta m_{i+1} &= m_{i+1} \oplus m'_{i+1} \\ &= [m_{i-1} \oplus \mathrm{f}(m_i, K_i)] \oplus [m'_{i-1} \oplus \mathrm{f}(m'_i, K_i)] \\ &= \Delta m_{i-1} \oplus [\mathrm{f}(m_i, K_i) \oplus \mathrm{f}(m'_i, K_i)]\end{aligned}$$

  - Now, suppose that many pairs of inputs to f with the same difference yield the same output difference if the same subkey is used.
  - To put this more precisely, let us say that X may cause Y with probability p , if for a fraction p of the pairs in which the input XOR is X , the output XOR equals Y .
  - We want to suppose that there are a number of values of X that have high probability of causing a particular output difference. Therefore, if we know Δm_{i-1} and Δm_i with high probability, then we know Δm_{i-1} with high probability. Furthermore, if a number of such differences are determined, it is feasible to determine the subkey used in the function f.
  - The overall strategy of differential cryptanalysis is based on these considerations for a single round. The procedure is to begin with two plaintext messages m and m’ with a given difference and trace through a probable pattern of differences after each round to yield a probable difference for the ciphertext.
  - Actually, there are two probable patterns of differences for the two 32-bit halves: $(\Delta m_{17} \| \Delta m_{16})$.
  - Next, we submit m and m’ for encryption to determine the actual difference under the unknown key and compare the result to the probable difference. If there is a match,

    $$\mathrm{E}(K, m) \oplus \mathrm{E}(K, m') = (\Delta m_{17} \| \Delta m_{16})$$

    then we suspect that all the probable patterns at all the intermediate rounds are correct. With that assumption, we can make some deductions about the key bits. This procedure must be repeated many times to determine all the key bits.
  - Figure below, illustrates the propagation of differences through three rounds of DES. The probabilities shown on the right refer to the probability that a given set of intermediate differences will appear as a function of the input differences. Overall, after three rounds, the probability that the output difference is as shown is equal to 0.25 * 1 * 0.25 = 0.0625 .
- Linear Cryptanalysis
  - A more recent development is linear cryptanalysis.This attack is based on finding linear approximations to describe the transformations performed in DES.
  - This method can find a DES key given 2^{43} known plaintexts, as compared to 2^{47} chosen plaintexts for differential cryptanalysis. Although this is a minor improvement, because it may be easier to acquire known plaintext rather than chosen plaintext, it still leaves linear cryptanalysis infeasible as an attack on DES.
  - So far, little work has been done by other groups to validate the linear cryptanalytic approach. We now give a brief summary of the principle on which linear cryptanalysis is

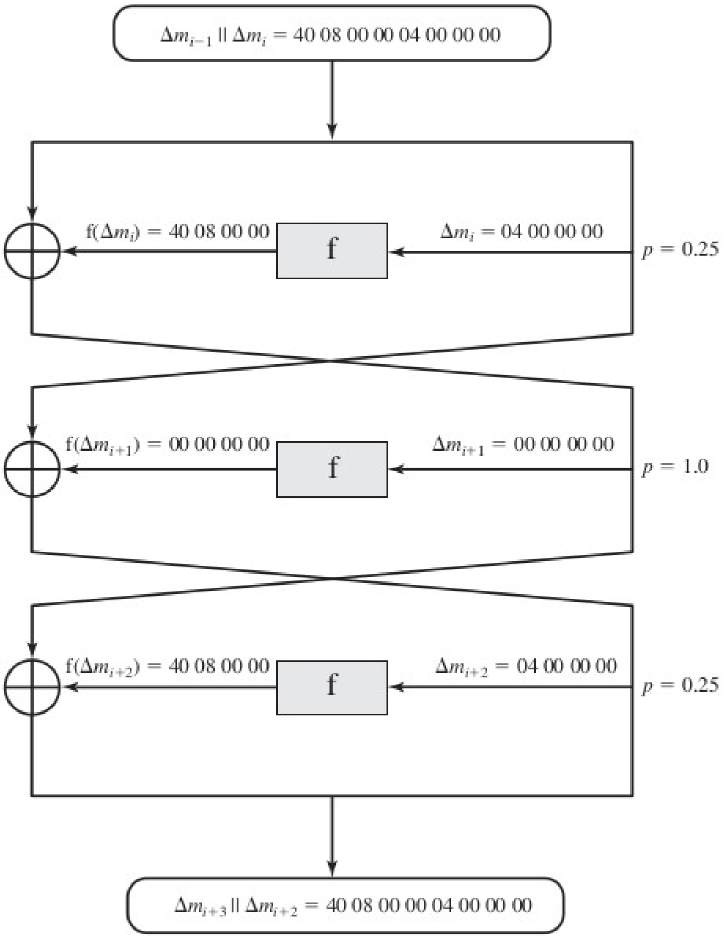
based. For a cipher with n -bit plaintext and ciphertext blocks and an m -bit key, let the plaintext block be labeled P[1],...P[n] , the cipher text block C[1],...C[n] , and the key K[1],...K[m] . Then define

$$\mathrm{A}[i, j, \ldots, k] = \mathrm{A}[i] \oplus \mathrm{A}[j] \oplus \ldots \oplus \mathrm{A}[k]$$

- The objective of linear cryptanalysis is to find an effective linear equation of the form:

$$\mathrm{P}[\alpha_1, \alpha_2, \ldots, \alpha_a] \oplus \mathrm{C}[\beta_1, \beta_2, \ldots, \beta_b] = \mathrm{K}[\gamma_1, \gamma_2, \ldots, \gamma_c]$$

- (where x = 0 or 1; 1 <= a; b <= n; c <= m ; and where the a, b, and g terms represent fixed, unique bit locations) that holds with probability p Z 0.5 . The further p is from 0.5, the more effective the equation.


$\Delta m_{i-1} \| \Delta m_i$ = 40 08 00 00 04 00 00 00
$f(\Delta m_i)$ = 40 08 00 00
f
Δm_i = 04 00 00 00
$p = 0.25$
$f(\Delta m_{i+1})$ = 00 00 00 00
f
Δm_{i+1} = 00 00 00 00
$p = 1.0$
$f(\Delta m_{i+2})$ = 40 08 00 00
f
Δm_{i+2} = 04 00 00 00
$p = 0.25$
$\Delta m_{i+3} \| \Delta m_{i+2}$ = 40 08 00 00 04 00 00 00

Algorithm: