Differential Cryptanalysis -DES

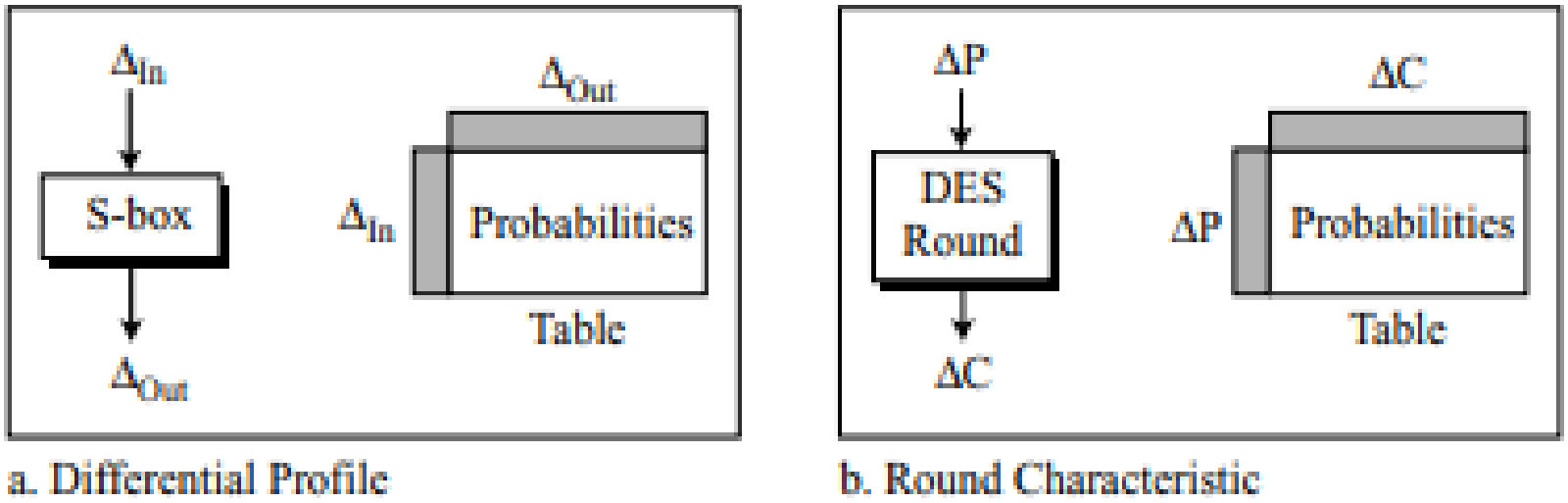
- The intruder concentrates on chosen-plaintext attacks.
- The analysis uses the propagation of input differences through the cipher.
- The term ‘difference’ here refers to exclusive-OR of two different inputs(plain texts).
- Intruder analyzes how P $\oplus$ P’ is propagated through rounds.

Differential Cryptanalysis

Probabilistic Relations

- The idea of differential cryptanalysis is based on the probabilistic relations between input and output differences.
- Two relations are of particular interest in the analysis: Differential profiles and round characteristics

Differential Profile



a. Differential Profile

b. Round Characteristic

Fig1

Differential Cryptanalysis

- Differential Profile

  A differential profile (or XOR profile) shows the probabilistic relation between the input differences and output differences of an S-box.

Differential Cryptanalysis

- Round Characteristic

  A round characteristic is similar to a differential profile but calculated for the whole round.

  The characteristic shows the probability that one input difference would create one output difference.

  Note: The characteristic is same for each round because any relation that involves differences is independent of the round key.

Differential Cryptanalysis

- Round characteristic

  There are many round characteristics for a round but figure below shows only 4 of them.

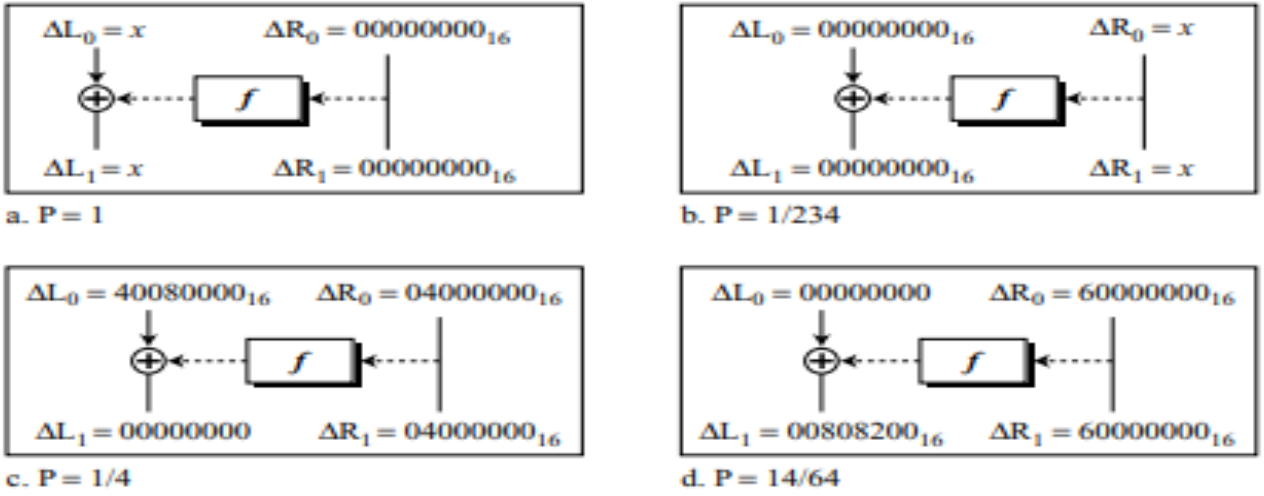


Fig 2

Differential Cryptanalysis

- In each characteristic there is division of input differences and output differences into left and right sections.
- Each left or right difference is made of 32 bits or 8 hexadecimal digits.
- Fig a shows that the input difference of $(x,00000000_{16})$ produces the output difference of $(x,00000000_{16})$ with probability 1.

Differential Cryptanalysis

- Fig b shows the same characteristic as Fig a except that the left and right inputs and outputs are swapped; the probability will change tremendously.
- Fig c shows that the input difference of (40080000_{16},04000000_{16}) produces the output difference (00000000_{16},04000000_{16}) with probability ¼.
- Fig d shows that the input difference (00000000_{16},60000000_{16}) produces the output difference (00808200_{16},60000000_{16}) with probability 14/64.

Differential Cryptanalysis

- A Three-Round Characteristic

  The analyzer can combine different rounds to create a multiple-round characteristic.

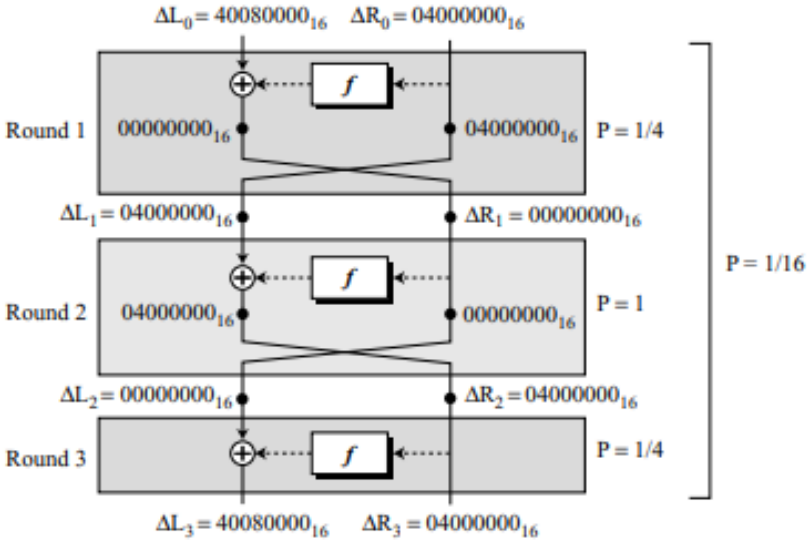


Fig 3

Differential Cryptanalysis

- In this Fig there are 3 mixers and only 2 swappers because the last round needs no swapper.
- The characteristics shown in the mixers of the 1st and 3rd rounds is same as of Fig 2.
- The characteristic of the mixer in 2nd round is same as the one in Fig 1.
- In this particular case the input and output differences are the same($\Delta L_3 = \Delta L_0$ and $\Delta R_3 = \Delta R_0$)

Differential Cryptanalysis

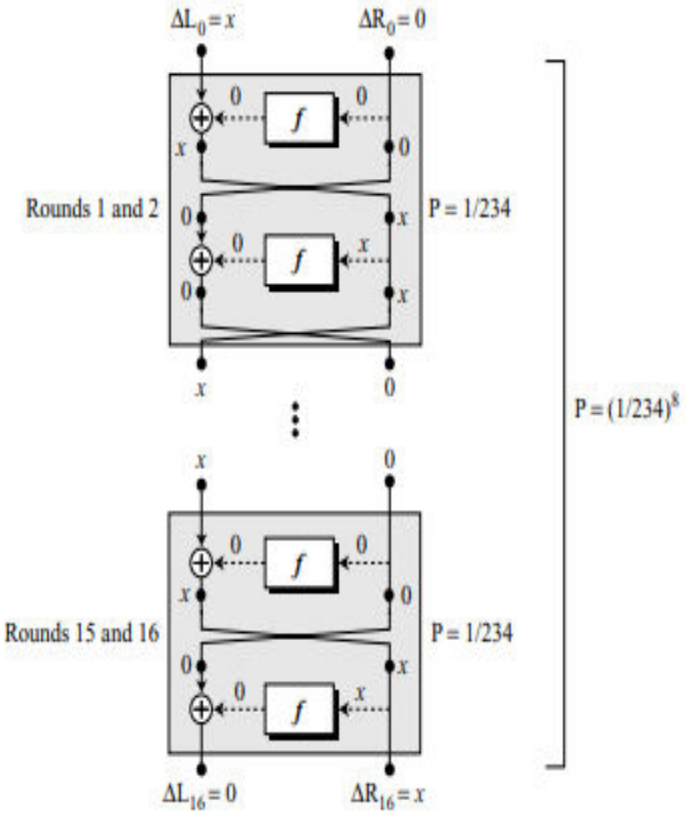


Fig 4

Differential Cryptanalysis

- Attack

  Assume that Eve uses the characteristic of Fig 4 to attack a 16- round DES. Eve somehow lures Alice to encrypt a lot of plaintexts in the form (x,0), in which the left half is x(different values) and right half is 0. Eve then keeps all cipher texts received from Alice in the form (0,x).

  Note: 0 means 00000000_{16}

Differential Cryptanalysis

- Finding the Cipher Key

  By finding the round keys from the bottom to the top(K_{16} to K_1)

  Finding the last Round key: If the intruder has enough plaintext/ciphertext pairs she can use the relationship in the last round, $0=f(K_{16},x)$ to find some of the bits in K_{16} .This can be done by finding the most probable values that make this relation more likely.

Differential Cryptanalysis

Finding other round keys

Can be found using other characteristics or brute-force attacks.

- Security

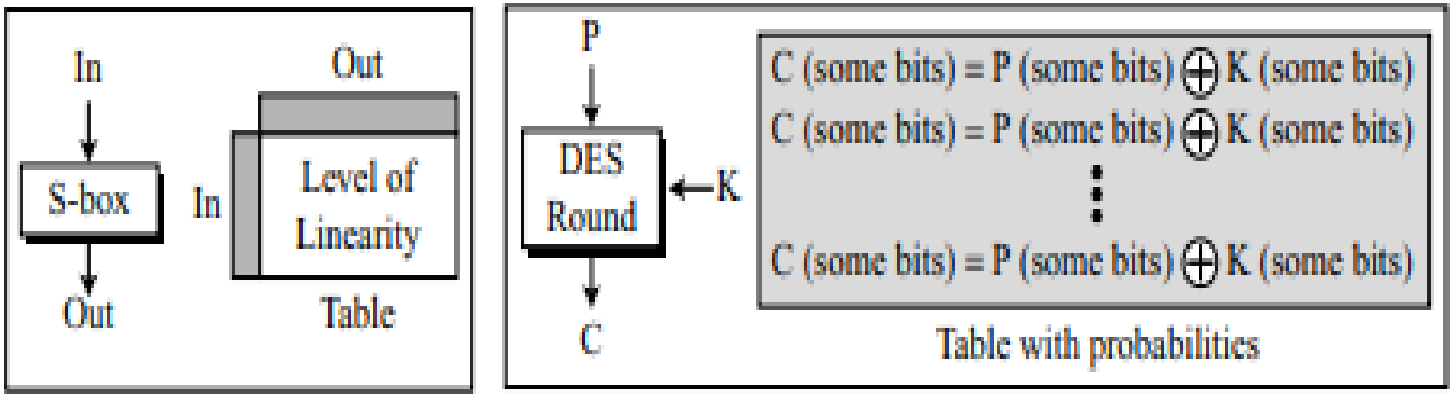
  2^{47} Chosen plaintext/ciphertext pairs are needed to attack a 16-round DES. Finding such a huge no. of pairs is difficult so DES is not vulnerable to this type of attack.

Linear Cryptanalysis

- It is a known-plaintext attack
- The analysis uses the propagation of a particular set of bits through the cipher.
- Linearity Relations

  Linear Cryptanalysis is based on linearity relations. Two set of relations particularly: linear profile and round characteristics.

Linear Cryptanalysis



a. Linearity Profile

b. Round Characteristic

Fig 5

Linear Cryptanalysis

- Linear Profile

  A linear profile shows the level of linearity between input and output of an S-box. In an S-box, each output bit is a function of all input bits.

  The ideal case in an S-box is if each output bit is a non-linear function of all input bits. Unfortunately some output bits are linear function of some combinations of input bits.

Linear Cryptanalysis

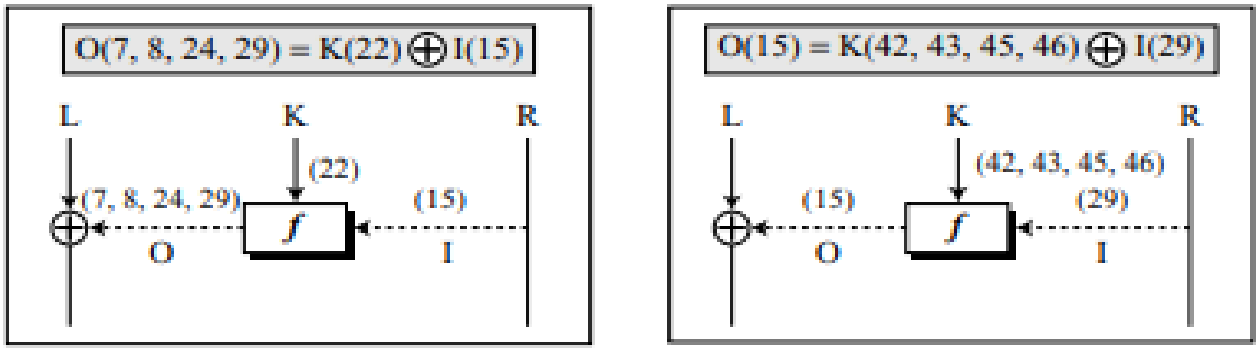
The cryptanalysis can create 8 different tables, one for each S-box, in which the 1st column shows the possible combination of 6-bit inputs, 00_{16} to $3F_{16}$ and the 1st row shows the possible combinations of 4-bit inputs, 0_{16} to F_{16} . The entries show the level of linearity.

Linear Cryptanalysis

- Round Characteristic

Shows the combination of input bits, round key bits, and output bits that show a linear relation.

Fig 6 shows two different round characteristics.



a. P = 52/64

b. P = 42/64

Fig 6

Linear Cryptanalysis

- The notation used for each case defines the bits that must be exclusive-ored together.
- For example, O(7, 8, 24, 29) means the exclusive-or of 7th, 8th, 24th, and 29th bits coming out of the function;
- K(22) means the 22nd bit in the round key; I(15) means the 15th bit going into the function.

Linear Cryptanalysis

- The relations using individual bits :
- Part a: $O(7) \oplus O(8) \oplus O(24) \oplus O(29) = I(15) \oplus K(22)$
- Part b: $F(15) = I(29) \oplus K(42) \oplus K(43) \oplus K(45) \oplus K(46)$

Linear Cryptanalysis

- A Three-Round Characteristic

Fig 7 shows a case of a three-round DES in which rounds 1 and 3 use the same characteristic as shown in Fig 6, but round 2 uses an arbitrary characteristic.

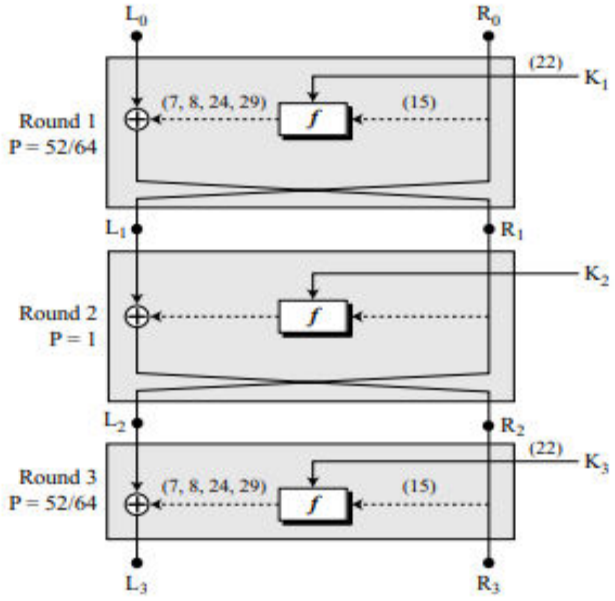


Fig 7

Linear Cryptanalysis

- The goal of linear cryptanalysis is to find a linear relation between some bits in the plaintext, the ciphertext, and the key
- For Fig 7

Round 1: $R_1(7, 8, 24, 29) = L_0(7, 8, 24, 29) \oplus R_0(15) \oplus K_1(22)$

Round 3: $L_3(7, 8, 24, 29) = L_2(7, 8, 24, 29) \oplus R_2(15) \oplus K_3(22)$

Linear Cryptanalysis

- But L_2 is the same as R_1, and R_2 is the same as R_3. After replacing L_2 with R_1 and R_2 with R_3 in the second relation, we have:
- $L_3(7, 8, 24, 29) = R_1(7, 8, 24, 29) \oplus R_3 (15) \oplus K_3(22)$
- Substitute R_1 with its equivalent value in round 1, resulting in:
- $L_3(7, 8, 24, 29) = L_0(7, 8, 24, 29) \oplus R_0(15) \oplus K_1(22) \oplus R_3 (15) \oplus K_3(22)$

Linear Cryptanalysis

- This is a relationship between input and output bits for the whole three rounds after being reordered:
- $L_3(7, 8, 24, 29) \oplus R_3(15) = L_0(7, 8, 24, 29) \oplus R_0(15) \oplus K_1(22) \oplus K_3(22)$
- In other words, we have:
- $C(7, 8, 15, 24, 29) = P(7, 8, 15, 24, 29) \oplus K_1(22) \oplus K_3(22)$

Linear Cryptanalysis

- A Sixteen-Round Characteristic

A 16-round characteristic can also be compiled to provide a linear relationship between some plaintext bits, some ciphertext bits, and some bits in the round keys.

C(some bits) = P(some bits) $\oplus$ K_1(some bits) $\oplus$ … $\oplus$ K_{16}(some bits)

Linear Cryptanalysis

- Attack

After finding and storing many relationship between some plaintext bits, ciphertext bits, and round-key bits. Eve can access some plaintext/ciphertext pairs (known-plaintext attack) and use the corresponding bits in the stored characteristics to find bits in the round keys.

Linear Cryptanalysis

- Security

243 known plaintext/ciphertext pairs are needed to attack a 16-round DES.

Linear cryptanalysis looks more probable than differential cryptanalysis for two reasons.

First, the number of steps is smaller.

Second it is easier to launch a known plaintext attack than a chosen-plaintext attack.