PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

APPLIED CRYPTOGRAPHY

Private key systems

Lecture 7

Cryptanalysis

Linear and differential

DES Weaknesses

- ***Weaknesses in Cipher Design***
    1. ***Weaknesses in S-boxes***
    2. ***Weaknesses in P-boxes***
    3. ***Weaknesses in Key***

Security of DES

- DES, as the first important block cipher, has gone through much scrutiny.
- The size of the key space, 64, is “too small” to be secure. Brute-Force Attack: Combining short cipher key in DES with the key complement weakness.
- Security of DES mainly relies on the nonlinearity of the function f

Security of DES

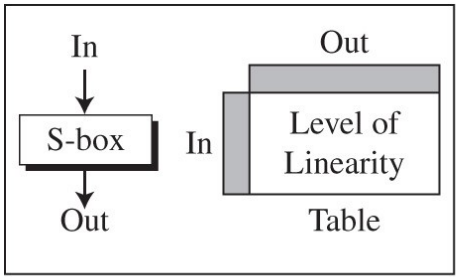
- Differential cryptanalysis: Designed S-boxes and 16 rounds aim to make DES specifically resistant to this type of attack.
- Linear cryptanalysis: DES is more vulnerable to linear cryptanalysis than to differential cryptanalysis. S-boxes are not very resistant to linear cryptanalysis. It has been shown that DES can be broken using ***243*** pairs of known plaintexts.

Linear Cryptanalysis

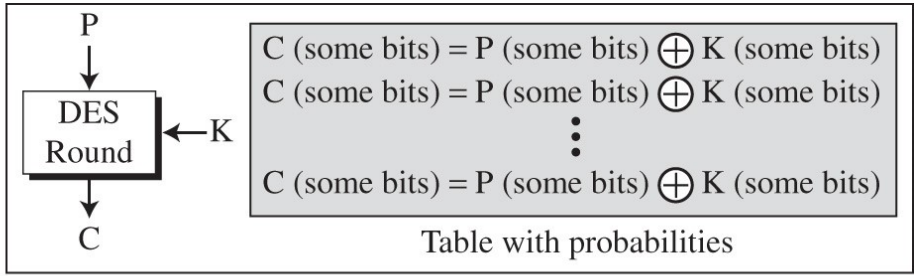
- Linear cryptanalysis first defined by Matsui and Yamagishi in 1992. It was extended Matsui later in 1993 published a linear attack on DES.
- Linear cryptanalysis is a known plaintext attack in which cryptanalyst access larger plaintext and ciphertext messages along with an encrypted unknown key.

Reference 1: section 6.2.6 Differential and Linear Cryptanalysis

Linear Cryptanalysis



a. Linearity Profile

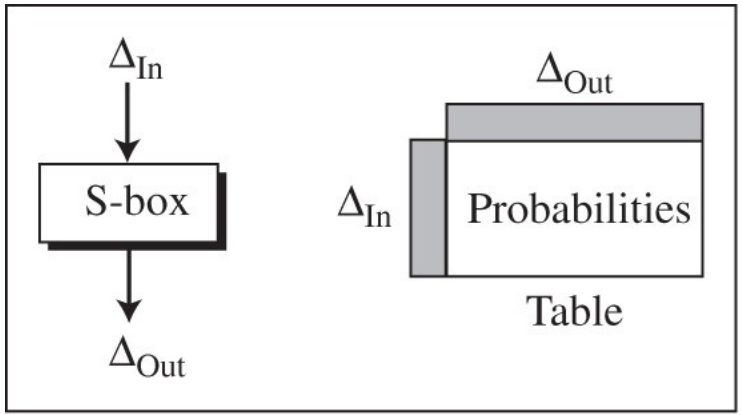


b. Round Characteristic

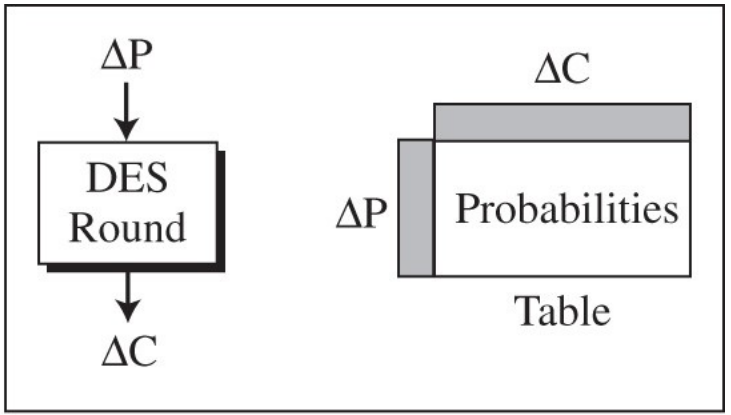
Differential Cryptanalysis

- is a method for breaking certain classes of cryptosystems. It was invented in 1990 by Israeli researchers Eli Biham and Adi Shamir.
- is available to obtain clues about some bits of the key, thereby shortening an exhaustive search. By analyzing the changes in some chosen plaintexts, and the difference in the outputs resulting from encrypting each one, it is possible to recover some properties of the key.

Differential Cryptanalysis



a. Differential Profile



b. Round Characteristic

For example, assume that the ciphertext obtained from one exclusive-or operation of plain text and key.

Without knowing the value of the key, the cryptanalyst can easily find the differences between plaintext and ciphertext. Plaintext difference is represented by P1⊕P2.

Whereas the ciphertext difference represented by C1⊕C2. The following proves that C1⊕C2 =P1⊕P2 First ciphertext C1 obtained = First plaintext P1 ⊕ Key K

Second ciphertext C2 obtained = Second plaintext P2 ⊕ Key K, if C1 and C2 obtained from XORing P1 and P2 and using Key K, can be represented by,

C1⊕C2=P1⊕K⊕P2⊕K=P1⊕P2

Difference between Linear and differential cryptanalysis

- Linear cryptanalysis
  first defined by Matsui and Yamagishi in 1992.
- The cryptanalyst decrypts each cipher text using all possible sub keys for one round of encryption and studies the resulting intermediate cipher text to analyze the random result

- Differential cryptanalysis is a method for breaking certain classes of crypto systemsis invented in 1990 by Israeli researchers Eli Biham and Adi Shamir.
- Cryptanalyst studies changes to the intermediate cipher text obtained between multiple rounds of encryption. The attacks can be combined, which is called differential-linear cryptanalysis.

Difference between Linear and differential cryptanalysis

- In linear cryptanalysis, the role of cryptanalyst is to identify the linear relation between some bits of the plaintext, some bits of the ciphertext and some bits of the unknown key
- Linear cryptanalysis focus on statistical analysis against one round of decrypted cipher text

- By analyzing the changes in some chosen plaintexts, and the difference in the outputs resulting from encrypting each one, it is possible to recover some of the key.
- Differential analysis focuses on statistical analysis of two inputs an two outputs of a cryptographic algorithm.

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT PESU Center for Internet of Things