Linear and Differential Cryptanalysis

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.
- In a linear Cryptanalysis, the role of the 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. This relation helps cryptanalysts to understand the logic used during encryption and decryption. the decryption of messages and to find how many bits of messages undergo encryption.
- There are two basic approaches. The first is to use an approximation that relates some way as mentioned earlier. bits of plain text with some bits ciphertext messages and user-defined key in a linear.
- The second focuses on statistical analysis against one round of decrypted ciphertext. The cryptanalyst each ciphertext using all possible subkeys for one round of encryption and studies the resulting intermediate ciphertext to analyze the random result.
- The subkey obtained during this pro and dec g this process called as candidate key used during encryption of a large amount of data.

Differential Cryptanalysis

- Differential cryptanalysis is a method for breaking certain classes of cryptosystems. It was invented in 1990 by Israeli researchers Eli Biham and Adi Shamir.
- Differential cryptanalysis 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 is a chosen-plaintext attack that identifies a relationship between ciphertexts produced by the same plaintexts.
- The differential analysis focuses on a statistical analysis of two inputs and two outputs of a cryptographic algorithm. *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,

$$C1 \oplus C2 = P1 \oplus K \oplus P2 \oplus K = P1 \oplus P2$$

- Differential cryptanalysis and linear cryptanalysis attacks are related to each other basically used in symmetric key cryptography. Whatever ciphertext produced from the same plain text the multiple rounds of encryption applied using for each round.
- Subkey Cryptanalyst studies changes to the intermediate ciphertext obtained between multiple rounds of encryption. The attacks can be combined, which is called differential-linear cryptanalysis.

Difference Between Linear and Differential Cryptanalysis

- In cryptography, Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.
- Whereas Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior and exploiting such properties to recover the secret key (cryptography key)

Linear Cryptanalysis	**Differential Cryptanalysis**
Linear cryptanalysis first defined by Matsui and Yamagishi in 1992.	Differential cryptanalysis is a method for breaking certain classes of cryptosystems is invented in 1990 by Israeli researchers Eli Biham and Adi Shamir.
In linear cryptanalysis, the role of the 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.	Differential cryptanalysis is available to obtain clues about some bits of the key, thereby shortening an exhaustive search
The cryptanalyst decrypts each ciphertext using all possible subkeys for one round of encryption and studies the resulting intermediate ciphertext to analyze the random result.	Cryptanalyst studies changes to the intermediate ciphertext obtained between multiple rounds of encryption. The attacks can be combined, which is called differential linear cryptanalysis.
In linear cryptanalysis, the role of the 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	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 keys.
Linear cryptanalyses focus on statistical analysis against one round of decrypted ciphertext	Differential analysis focuses on the statistical analysis of two inputs and two outputs of a cryptographic algorithm.