Diff b/w Differential and Linear

Differential

→ role of cryptanalysis is to identify the linear relation b/w some bit of plain text.

→ They changes the intermediate ciphertext obtained b/w each 16 rounds.

→ uses chosen plain text to get all possible key combination to recover keys

→ uses statistical analysis against one round of decrypted cipher text

→

Linear

Identifies clues about the keys.

They decrypts each ciphertext using all possible values to get random result.

→ Identifies linear relation b/w some bits.

uses statistical analysis against one round for two i/p's and two o/p's.

Keys obtained intermediate is called candidate key.

Avalanche effect in DES

Even a slight change in an input string should cause the hash value to change drastically. In particular, change in one bit of the plaintext or one bit of the key, should produce a change in many bits of the ciphertext. This is called as the "Avalanche effect".

BLOCK CIPHER DESIGN PRINCIPLES

-> A block cipher operates on blocks on data.
-> Here DES breaks plaintext into blocks and operates independently on each block.
-> There is 2^n size of block.
-> Here the security depends on design functions
-> software implementation of block cipher depends on function, it is faster than the stream cipher.
-> Errors in transmitting one block doesn't affect the other blocks.
-> Example:. plaintext = 227 bytes long.
16 rounds. each round 16 byte blocks.

$$\text{Block size} = 16 \text{ bytes} = \frac{227}{16} = 14 \text{ blocks}, 3 \text{ bytes}.$$

14 blocks are encrypted with 14 rounds and remaining to encrypt the last three bytes, padding is used. whoever does the decryption, recognize the padding bits in the last block.

But one issue is same block of plaintext occurs means then same cipherText block is created.

To avoid these kind of problem, feedback mode is used.

in one bit of the plaintext or one bit of the key. In particular, a change in one bit of the plaintext or one bit of the key will produce a change in many bits of the ciphertext. This is called as the "Avalanche effect".

BLOCK CIPHER DESIGN PRINCIPLES

-> A block cipher operates on blocks on data.
-> Here DES breaks plaintext into blocks and operates independently on each block.
-> There is 2^n size of block.
-> Here the security depends on design functions
-> software implementation of block cipher depends on function, it is faster than the stream cipher.
-> Errors in transmitting one block doesn't affect other blocks.
-> Example:. plaintext = 227 bytes. long.
16 rounds. each round 16 byte blocks.

$$\text{Block size} = 16 \text{ bytes} = \frac{227}{16} = 14 \text{ blocks}, 3 \text{ bytes}.$$

14 blocks are encrypted with 14 rounds and remaining to encrypt the last three bytes, padding is used. whoever does the decryption, recognize the padding bits in the last block.

But one issue is same block of plaintext occurs means then same ciphertext block is created.

Advantages
-> High diff
-> Immunit

Disadvanta
->Slowness
->Errors

STREAM

Stream
Key a
Ciphe

Avalanche effect in DES

Even a sight change in an input string should cause the hash value to change drastically. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is called as the "Avalanche effect".

BLOCK CIPHER DESIGN PRINCIPLES

-> A block cipher operates on blocks of data.

-> Here DES breaks plaintext into blocks and operates independently on each block.

-> There is 2^n size of block.

-> Here the security depends on design functions.

-> software implementation of block cipher depends on function, it is faster than the stream cipher.

-> Errors in transmitting one block doesn't affect other blocks.

-> Example: plaintext = 227 bytes long.

16 rounds. each round 16 byte blocks.

Block size = 16 bytes = $\frac{227}{16}$ = 14 blocks, 3 bytes.

14 blocks are encrypted with 14 rounds and remaining to encrypt the last three bytes, padding is used. whoever does the decryption, recognize the padding bit in the last block.

But one issue is same block of plaintext occurs means then same cipherText block is created.

To avoid these kind of problem, feedback mode is used.