Scribe: Cryptography and Network Security (Class.2.B)

Ritik Kumar

8-Oct-2020

1 Introduction

In this class, we started with the discussion on Fiestel Permutation which was discussed in Last class. And later on, we discussed DES which is a type of Feistal Cipher.

2 Fiestel Permutation

Feistel permutation divides the input plaintext block into two halves, each half passes through different number of rounds for encryption and then combines to produce the cipher text block.
So, in this input is divided into 2 parts L_0 and R_0.
Plainttext - (L_0, R_0)
For each round i=1,2, .. n-1, n
$L_i = R_{i-1}$
$R_i = L_{i-1}$ xor $F(R_{i-1}, K_i)$
Here, F is a round function and K_i is sub-key for the round i.

Fiestel permutation is invertible irrespective what we choose function for F but is secure only for certain functions F (when it is bijective).
Since this is invertible, so it can be decrypted for each cipher value.
For Decryption
$R_{i-1} =L_i$
$L_{i-1} = R_i$ xor $F(L_i, K_i)$.

3 Non-Feistel Ciphers

Non-feistel cipher uses only invertible components. There is no need to divide the block into two halves. Input of each round consists of key and the output of previous round. Also, these functions are obtained by the repeated application of Subsitution (invertible SBoxes) and Premutation. And so, they are called **Substitution Permutation Networks (SPN)**

4 Data Encryption Standard(DES)

Data Encryption Standard (DES) is a symmetric-key block cipher and is an implementation of a Feistel Cipher.

It is based on IBM Lucifer cipher. But the design process was not open, so people were suspicious that hidden trapdoors that would have allowed NSA to decrypt without the keys. Other disadvantage was that key length was small (56 bits). So, people started looking for alternatives such as AES.

4.1 Implementation of DES

DES is a Feistal Cipher in which block length is 64 bit block length, Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

16 rounds is applied since it is a product cipher. Each round uses 48 bits of key used each round (subkey). Each round is simple because blocks are easy to calculate and security depends primarily on "S-boxes" where each S-boxes maps 6 bits to 4 bits (so S-boxes are not bijective).

Initial and Final Permutation
DES has initial permutation and a final one after 16 rounds. And these permutations are inverse of each other and operate on 64 bits, since plain text is of 64 bits. This permutations has no cryptographic significance as the specification is open and the layer is fixed.

4.2 DES S-box(Substitution Box)

Each S-box maps 6 bits to 4-bits.
In S-Box, Rows are permutations. Each output are non-linear combination of the inputs.
S-box satisfy the **Avalanche Effect** which says change of one bit in the input and half of the output bits change.
Each output bit is dependent on all the input bits.

It is hard to design of S-Box. Individually boolean functions (y0, y1, y2 ...) should satisfy the above properties but also their combination should satisfy these properties. If it is not, it may be exploited later on.

4.3 Advantages of DES

Decryption in DES can be done by applying the encryption algorithm to the ciphertext, with the key schedule reversed. So, the same code and hardware could be used for decryption as well as encryption.
And due to the use of S-boxes, it satisfies **Avalanche effect** and **Completeness**.

4.4 Weak and semi-weak keys

A weak key is the one which after parity drop operation, consists either of all 0's, all 1's or half 0's and half 1's.For DES, it is found out that out of power(2,56) keys possible, four keys are weak.
Consequence of weak keys is that the round keys created from any of these weak keys are same. Lets understand this from the eample: For one weak key, all the round keys are 0, second key leads to half 0's and half 1's. So a block which is encrypted with a weak key and subsequently encrypt the result with the same weak key, we get the original block.

$\mathrm{E_k(E_k(P)) = P}$

So, they are 8 equal round keys in each semi-weak keys. So, the round key in the first set is the same as the 16^{th} key in the second set. So this means that the keys are inverse of each other.

$\mathrm{E_{k2}(E_{k1}(P)) = P}$

So, these keys can easily be exploited.

5 Conclusion

From this class, we understood that DES has proved to be a very well designed block cipher.