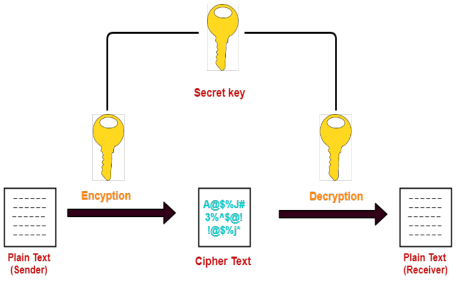
Scribe: Cryptography and Network Security (Week 4 Class 3)

Venu Gopal Bandhakavi

1-October-2020

1 Symmetric Key Cryptography

Symmetric Key cryptography involves encryption and decryption with a single key known as secret key which is shared by both Alice and Bob. Here the attacker Eve has access to the encrypted cipher text and the communication channel but do not know about the secret key used by Alice and Bob. Here Alice and Bob decide about a secret key which is used for their communication.



Symmetric Key Cryptography

Some symmetric key Ciphers are:

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Diffie Hellman (DH) key exchange algorithm

2 Types of Symmetric Key Ciphers

2.1 Block Ciphers

Symmetric key ciphers where a block of plaintext is encrypted at once or a block of ciphertext is decrypted at once are called as block ciphers. It can encrypt n bits of plaintext at once or it can decrypt m bits of ciphertext at once.

2.1.1 Electronic Code Book(ECB)

Electronic Code Book (ECB) is a mode of operation for a block cipher, with the characteristic that each possible block of plaintext has a defined corresponding ciphertext value and vice versa. Which means that each plaintext value will always result to same ciphertext value.

2.1.2 Padding

If the block cipher encrypts with a block size of n then the plaintext length should be divisible by n. When it is not divisible by n , then the last block of plaintext is padded to make it the size of n.

2.2 Stream Ciphers

Stream ciphers are block ciphers with block size of 1. At once only one bit of plaintext is encrypted or decrypted.

3 Block Ciphers

3.1 Transposition Ciphers

In transposition cipher we map the bits of the input to another position without changing the bit value. We rearrange the bits of the input to obtain the output.

B_1	B_2	B_3	B_4	B_5	B_6	B_7
B_5	B_4	B_1	B_3	B_2	B_7	B_6

As we know for a n length sequence we have $n!$ different permutations of that given sequence. In the same way for a n bit input we have $n!$ different permutations of it , which means $n!$ different keys possible to encrypt that given input. The transposition cipher key length is $\lceil \log(n!) \rceil$, as the number of keys possible is $n!$ it takes $\lceil \log(n!) \rceil$ bits to encode a specific key.

3.2 Substitution Cipher

The substitution cipher instead of rearranging or permuting the bits it substitutes values into the bit. When we are given with a n bit input then the substitution cipher replaces it with another n bit output. For a n bit input we have the input space of 2^n which is when given to a substitution cipher it then maps it into the 2^n output space. This mapping by the substitution cipher should be bijective as the cipher should be invertible for decryption. For this reason the key space is $\lceil \log(2^n!) \rceil$.

3.3 Permutation Groups

The Transposition and Substitution ciphers are a permutatinos of the plaintext. We also know that a permutation of a permutation is another permutation. This means that permutations form a group under the composition operator.

$$\pi_i \circ \pi_j = \pi_z$$

This means that applying the transposition or substitution cipher twice will give us the same effect as applying a different transposition or substitution cipher once. This is an unwanted property for a cipher.

3.4 Full Size Key Ciphers

Full size keys ciphers are the ciphers which operate over all the n bits of the input. Transposition and Substitution ciphers are Full size key ciphers. The full size key ciphers have a very huge key space and many of the keys are wasted as they are not used.

For transposition cipher of a 3-bit block we need a key size of $\lceil \log(3!) \rceil$ that is 3 bits. For substitution cipher of a 3-bit block we need a key size of $\lceil \log(2^3!) \rceil$ that is 16 bits. But for a 3 bit block we do not need that big of a key size and it leads to wastage of a lot of keys.

3.5 Partial Size Keys

Actual ciphers which are used in real world cannot use full size keys as the key size is very large and it is not practical. Which is why we use partial size keys. For Data Encryption Standard (DES) with block size 64 we have $\lceil \log(2^{64}!) \rceil \approx 2^{70}$ which is very huge. But DES uses 56 bit key.

3.5.1 Do Partial Key Cipher form a Group?

If the partial key ciphers forms a group over composition then multiple applications of the cipher is useless. We have to make sure that the partial key cipher does not form a group. A partial key cipher forms a group if it is a subgroup of the corresponding full key cipher.

It has been proven that multistaged DES of 56 bit does not form a group as no subgroup of 2^{56} mappings can be formed from the corresponding group with $2^{64}!$ mappings.

4 Modern Day Block Ciphers

Modern day block ciphers make use of :

1. **PBox** : PBox also known as Permutation Box is a keyless and fixed transposition cipher.

2. **SBox** : SBox also known as Substitution Box is a keyless and fixed substitution cipher.

4.1 Principles of Confusion and Diffusion:

Confusion and Diffusion are techniques used in the modern day block ciphers. Confusion and Diffusion are achieved using the Sbox and Pbox respectively.

- **Confusion** : It is used to make the relation between plaintext and secret key as complex and involved as possible.
- **Diffusion** : It is used to dissipate the statistical structure of plaintext over the bulk of ciphertext. It hides the relationship between ciphertext and the plaintext.

Proper combination of confusion and diffusion is necessary.

4.2 PBox

Pbox is a keyless and fixed transposition cipher.PBoxes are used to achieve Diffusion. Although the for a n bit input $n!$ different keys are possible but there is only one mapping possible for a given PBox as it is keyless and fixed. Here there is no computation being done only rewiring of the bits is being done. There are three types of PBoxes:

1. **Straight PBox** : A PBox with n input bits and n output bits is called as a straight PBox. Each input bit is mapped to a output bit according to the wiring of the PBox. Straight PBoxes are invertible in nature.

01	15	02	13	06	17	03	19	09	04	21	11
14	05	12	16	18	07	24	10	23	08	22	20

24×24 Straight PBox

2. **Compression Box** : A PBox with n bit input and m bit output with $n>m$ is called a compression PBox. Some inputs are blocked and do not reach the output. The permutation table for these PBoxes have some missing values. These boxes are used when we need to rearrange the bits and same time we want to decrease the number of bits.

01	15	02	03	06	17	03	19	09	04	21	11

24×12 Compression PBox

3. **Expansion PBox** : A PBox with n bit input and m bit output where $n<m$ is called an expansion PBox. In this box some entries are repeated $(m-n)$. These boxes are used when we need to rearrange the bits and at the same time also want to increase the number of bits.

01	03	02	01	06	17	03	19	09	04	09	11
14	05	12	16	18	07	24	10	23	08	22	20

12×24 Expansion PBox

4.3 SBox

Sbox is a substitution cipher which is mapping n bit input to m bits output. Where each output bit is output of a boolean function of the inputs. SBox is used to provide confusion and it is dependent on an unknown key which provides the confusion. In the SBox some computation is done not as PBox where the bits are reqired.

$$\begin{aligned} y_1 &= f_1(x_1, x_2, x_3, ..., x_n) \\ y_2 &= f_2(x_1, x_2, x_3, ..., x_n) \\ y_3 &= f_3(x_1, x_2, x_3, ..., x_n) \\ .... \\ y_m &= f_m(x_1, x_2, x_3, ..., x_n) \end{aligned}$$

There are two types of Sboxes:

1. **Linear SBoxes** : When the function can be described in a linear way then the SBox is said to be a linear relation.

$$\begin{aligned} y &= x_1 \oplus x_2 \oplus x_3 .... \oplus x_n \\ y &= x_1 + x_2 \oplus x_3 + x_4 .... \oplus x_n \end{aligned}$$

2. **Non-Linear SBoxes** : When the function cannot be described in a linear way then the SBox is said to be a non-Linear relation.

$$\begin{aligned} y &= x_1 x_2 + x_3 x_4 \\ y &= x_1^2 + x_2^2 + ... + x_n^2 \end{aligned}$$

5 Conclusion

In this class we have discussed about the block ciphers. We have discussed about full size keys and partial size keys. In full size keys we have discussed about transposition and substitution ciphers. We have also discussed about PBox and SBox.