# Scribe: Cryptography and Network Security

Akash Singh Sant (20CS60R40)

October 1, 2020

## 1 Symmetric Key Cipher

In symmetric Key Cipher system the key used for encryption and decryption are same.
Before moving forward certain assumptions are made:
1.Two entities : Sender and Receiver
2.Only sender and receiver knows the secret keys
3.Attacker doesn't have any knowledge about the key used for encryption and decryption but have information about the algorithm and communication channel.

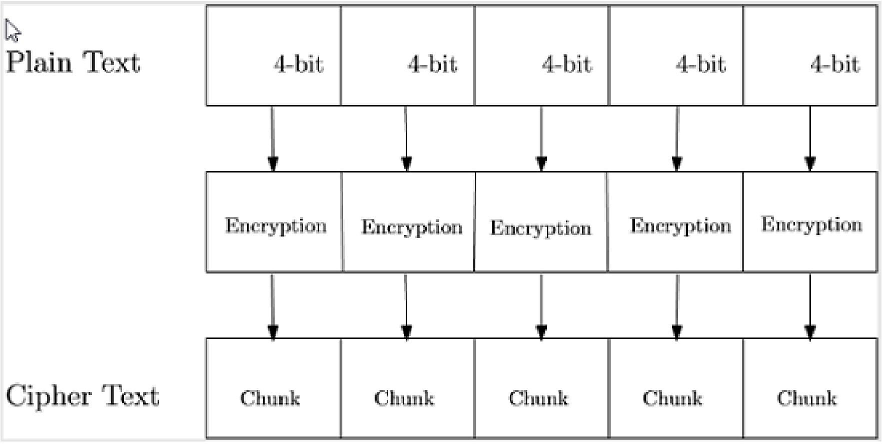
### 1.1 Types of Symmetric Key Ciphers

1.**Block Cipher**: In this block of data is encrypted ,Block Size currently being used in modern cipher >=128 bits.
Example :AES is 128 bits

2.**Stream Ciphers**: Block size <128 bits and can be in 1 bit as well. We operate on bits of info.
It is extremely fast.

#### 1.1.1 Block Ciphers

A symmetric key modern cipher encrypts an n bit block of plain text or decrypts an b bit block of cipher text. Typically we assume size of plain text =size of Cipher text .However there may be case the plain text might be lesser than multiple of n then padding is done to make it a multiple of n then encryption is done.
For better understanding the normal working of a block cipher is shown in the figure below.

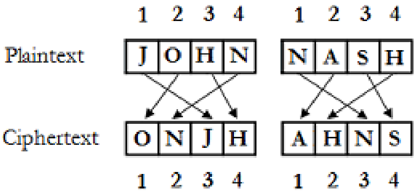


In the figure above we are assuming n=4.
So in this this 4 bit chunk is then encrypted to some b bit chunk cipher text and this process repeats for the coming n bits as well.So just like the plain text the cipher text also contains blocks. This type of code create is called electronic code block. In the decryption process this b bit chunk is decrypted to get the corresponding n bit plain text chunk.

## 1.2 Full Key cipher

### 1.2.1 Transposition Ciphers

The class of block cipher in which bits are rearranged in a different manner keeping the integrity of input intact is called Transposition ciphers.It is generally obtained by rearranging of wiring.
Consider a n bit cipher
Number of arrangement possible = n!
To make the permutation done secret we will kind of encode the permutation using a key.
Key will tell us the the corresponding permutation to be applied. Since no of permutation = n!
Suppose length of key= t bits
To provide unique encoding for all n! permutation then $2^t$ >=n!
No of bits required in key = ceil($log_2$(n!))



### 1.2.2 Substitution Ciphers

In this rearranging is not done but Substitution. So in this n bit block is replaced by another n bit of data.
Note: Since the encryption has to be reversal so as to get the original plain text.So there has to be 1:1 mapping (bijective).
However this can be modelled as a Transposition as well :
Each block of n bit can be replaced by $2^n$ values Substitution just takes one value out $2^n$ and maps it to different space of $2^n$ values keeping 1:1 mapping intact.
So for the 1st chunk we get $2^n$ values
for second input we get $2^n$ -1 possibilities
Hence in this way we have total $2^n$ ! permutation.
To make this mapping secret a key will be used and size of key = ceil[$log_2(2^n!)$] bits

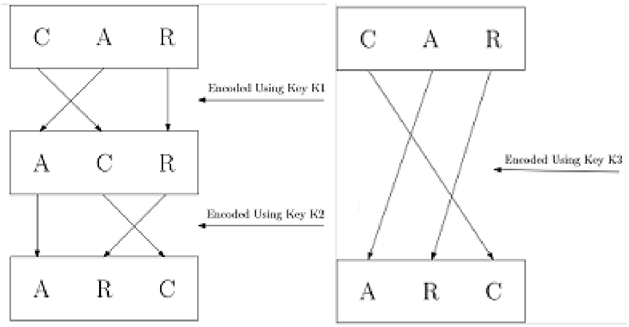
Both the transposition and substitution Cipher are the kind of Full Size Key Ciphers.
However in modern world we don't normally use full size key ciphers .There are some disadvantages of using full size key ciphers :

**1. Unused keys:**
Consider a 3-bit block ciphers. How many bits are needed for the full-size key?

Transposition cipher: ceil($log_2 6$)= 3 bits.
No of unused keys=8-6=2

Substitution cipher: There are 8!=40,320 possible substitutions
Thus there are ceil($log_2 40320$)=16 bits
No of Unused keys=$2^{16}$-40320=25216

**2.Permutation group:**
In both the transposition and substitution cipher permutation shows cascading but it is of no use because the permutation forms a group under the composition operation which means that different iteration of transformation can just be achieved by a single transformation.A clear representation is shown in the figure given below.



However Substitution and Transposition Ciphers are used in a partial manner in modern day ciphers.

### 1.3 Partial Size Key ciphers

Actual ciphers cannot use full size keys, as the size is large. Consider DES as instance of substitutions cipher with 64 bit block cipher
Size of full keys= ceil($log_2(log_2 64!)$=$log_2 70$
Much large compared to 56 bits which is actually used.
Also the partial key cipher used does not form a group under composition

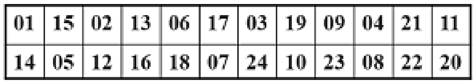
## 2 Components of Modern Block Ciphers

### 2.1 P-Box

P-Box stands for permutation box. It is a key-less fixed transposition cipher.It provides diffusion

**Diffusion**: It hides the relationship between the cipher text and the plain text. let us consider the input is changed by only 1 bit. Now because of the number of round transformation the number of output bits which are affected should approximately equal to half of the output cipher. Then the cipher has achieved diffusion.
**Diffusion P boxes :**

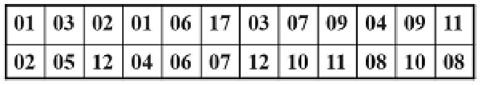
**1.Straight Boxes**:
In this single input bit is mapped to single bit of output.There is no repeatation involved. Eg.24*24 Box



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

In the above figure it can be seen that the $1^{st}$ input bit is mapped to $1^{st}$ bit of output.$2^{nd}$ bit is mapped to $15^{th}$ bit of output and so on.

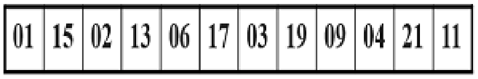
**2.Expansion Boxes**:
In this a smaller number of input bits are mapped to larger number of bit of output.There is repeatation involved. Eg.12*24 Box



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 03 | 02 | 01 | 06 | 17 | 03 | 07 | 09 | 04 | 09 | 11 |
| 02 | 05 | 12 | 04 | 06 | 07 | 12 | 10 | 11 | 08 | 10 | 08 |

In the above figure it can be seen that the $1^{st}$ input bit is mapped to $1^{st}$ and $4^{th}$ ,also $4^{th}$ bit of input is mapped to $10^{th}$ and $16^{th}$ bit of output.Hence there is repeatation

**3.Compression Boxes**:
In this a larger number of input bits are mapped to smaller number of output bits. Eg.24*12 Box



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 15 | 02 | 13 | 06 | 17 | 03 | 19 | 09 | 04 | 21 | 11 |

## 2.2 S-Box

S-Box stands for substitution box. It is a key-less fixed substitution cipher.An SBox (substitution box) is an mxn substitution box, where m and n are not necessarily same.
Each output bit is a Boolean function of the inputs It is dependent on the unknown key and it is used to provide confusion.

**Confusion**: It hides the relationship between the cipher text and the key let us consider the key is changed by only 1 bit. Now because of the number of transformation the number of output bits which are affected should approximately equal to half of the output cipher. Then the cipher has achieved Confusion.

Confusion and Diffusion are the two properties necessary for a good block cipher.

# 3 Conclusion

In this lecture we discussed the symmetric key cipher and their types and also about the components of modern day ciphers.

# 4 References

1.Lecture slides
2.Cryptography: Theory and Practice - Douglas Robert Stinson