[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Rathva Kaushikkumar Sanjaybhai (202051156) — Week : 2 (4nd lecture #)

1 Kirchhoff's Rule :

Design of cryptographic algorithm needs to be public in order of it to be :

1. Widely adapted by people.
2. For the algorithm to improve.

2 The perfect Secrecy : Shonno's notion

Encryption algo E
Message M
Cipher text C

E(M) = C
Here C might transmitted through public domain where people read it.

Definition 1 ***Perfect Secrecy*** *: E will be providing perfect secrecy if the cipher text doesn't reveal any information regarding the plain text/message.*
When we have the cipher text.

For the perfect secrecy the reader shouldn't have any advantage over the situation where they doesn't have it.

$P_r[M = m|C = c] = P_r[M = m]$

$P_r[message|Ciphertext] = P_r[message]$

If probability of us guessing the answer right without cipher text is p_g and with cipher text is $p_c = p_g + \epsilon$. Then p_c should be less or equal to p_g.
So, $p_c \leq p_g$
$p_g + \epsilon \leq p_g$
[1]

[1]OTP - One Time Padding.

3 Symmetric Key Cipher :

Symmetric Key Cipher has two categories :

3.1 Block cipher :

M message is devided in n blocks of fixed length l.

$M = m_0 \mid\mid m_1 \mid\mid m_2 \mid\mid \ldots \mid\mid m_n \rightarrow$ Blocks

3.1.1 Encryption :

Enc is encryption function.

$C = Enc(m_0, k) \mid\mid Enc(m_1, k) \mid\mid \ldots Enc(m_n, k)$

$C = (c_0 \mid\mid c_1 \mid\mid c_2 \ldots \mid\mid c_n)$

3.1.2 Decryption :

Dec is encryption function.

$C = Dec(c_0, k) \mid\mid Dec(c_1, k) \mid\mid \ldots Dec(c_n, k)$

$Plain\ text = (p_0 \mid\mid p_1 \mid\mid p_2 \ldots \mid\mid p_n)$

Block cipher is not very efficient for long strings.

3.2 Stream Cipher :

Stream cipher is used in places where the length of the message to be encrypted is either too long or length is not determined just yet.

For example, Mobile telephony and easy hardware implementation.

$M = (m_0 \ldots m_n)$ where $m_n \epsilon 0, 1$

3.2.1 Encryption :

$C = (m_0 \oplus z_0, m_1 \oplus z_1 \ldots m_n \oplus z_n)$

Here, $z_0, z_1 \ldots z_n$ are generated using function $F(k) \rightarrow z_i \epsilon 0, 1$

3.2.2 Decryption :

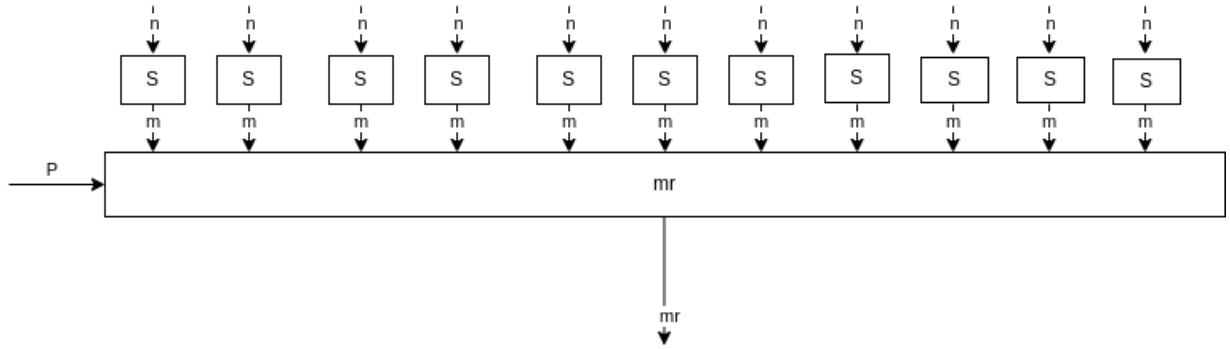
$Plaintext = (c_0 \oplus z_0, c_1 \oplus c_1 \ldots c_n \oplus z_n)$

4 Product Cipher :

A product cipher **combines two or more transformations** in a manner intending that the **resulting cipher is more secure** then the individual transformations.

5 Substitution Permutation Network (SPN):

It is a product cipher based substitution box and permutation box, SPN is based on block cipher and AES is based on SPN.



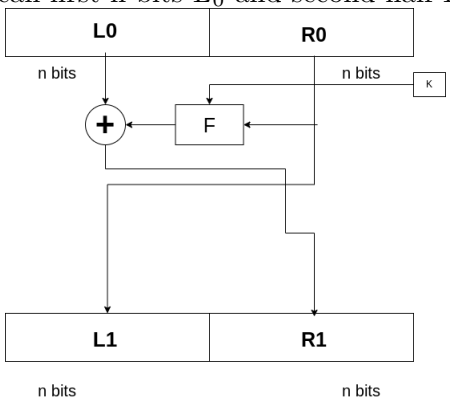
$S : \{0,1\}^n \rightarrow \{0,1\}^m$,
$p : \{0, \ldots m_{r-1} \rightarrow \{0, \ldots m_{r-1}\}$

6 Feistel Network(FN) :

FN is based also based on block cipher.Also DES is based on FN.

6.1 Encryption :

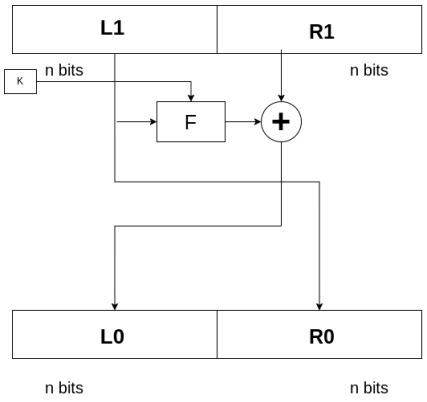
$P \rightarrow$ plain text of size 2n-bits. Out of that let's call first n bits L_0 and second half R_0.



If Cipher text $C = L_1||R_1$.
$L_! = R_0$
$R1 = L_1 \oplus f(R_0, k)$

6.2 Decryption :

Plain text



$L_0 = R_1 \oplus f(R_0, k) \rightarrow L_0 = R_1 \oplus f(L_1, k)$
$R_0 = L_1$

7 Iterated block cipher :

One computation will be iterated for number of rounds.the computation is called round fuunction.

Parameters of such functions are :
number of rounds r,
block size n,
round key k_i of length l.[2]

7.1 Characteristics of iterative block cipher:

1. no. of rounds n
2. round function F
3. Plain text block P
4. Secret key K

Let's take a 3 round block cipher. It has 3 rounds and relative keys and we have a key scheduling function

$G(n) = k_1, k_2, k_3$

and those are our round keys.
key scheduling functions gives distinct round keys for the secret key as input.

8 OTP(One time padding):

OTP provides perfect secrecy under some condition.

8.1 Encryption :

$P \rightarrow$ plain text
$K \rightarrow$ Secret key

$Enc(P, k) = p \oplus k = C$

8.2 decryption :

$Dec(C, k) = C \oplus k = CP$

$P_r[message|Ciphertext] = P_r[message]$

[2]It is generated from the original seceret key k