Network & Information Security:

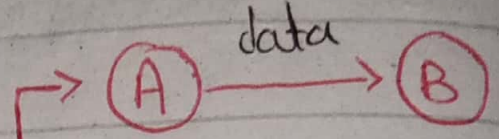
- Security: Degree of protection against danger, damage, loss, and crime.

- Information Security: Protecting information and information systems from unauthorized:
  - access
  - use
  - disclosure
  - disruption
  - modification
  - perusal
  - inspection
  - recording
  - destruction

- Network Security: consists of the provisions and policies adopted by the network administrator to prevent and monitor
  - Unauthorized access
  - misuse
  - modification
  - denial

of computer network & network-accessible resources.

Security Concerns:



- Data Manipulation
- Data loss
- Delay
- Denial of Service
- Confidentiality
- Unauthorized Access

} Cryptography deals with all this

To handle all these security concerns, we have:

C (Confidentiality) I (Integrity) A (Availability)

Cryptographic Techniques:

1) Encryption: $E(d, K) = C$
   - Achieve Confidentiality

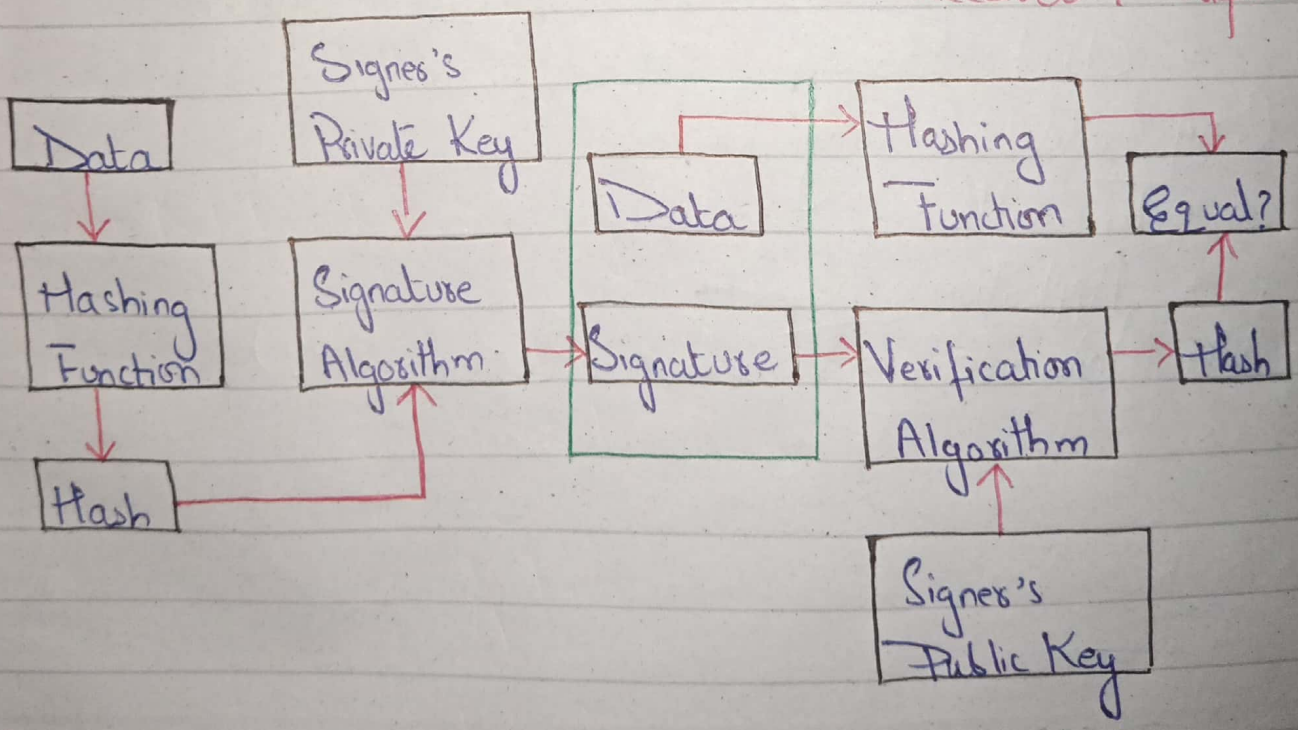
2) Digital Signatures: Detect Modification
using digital signatures
   - Achieve Integrity

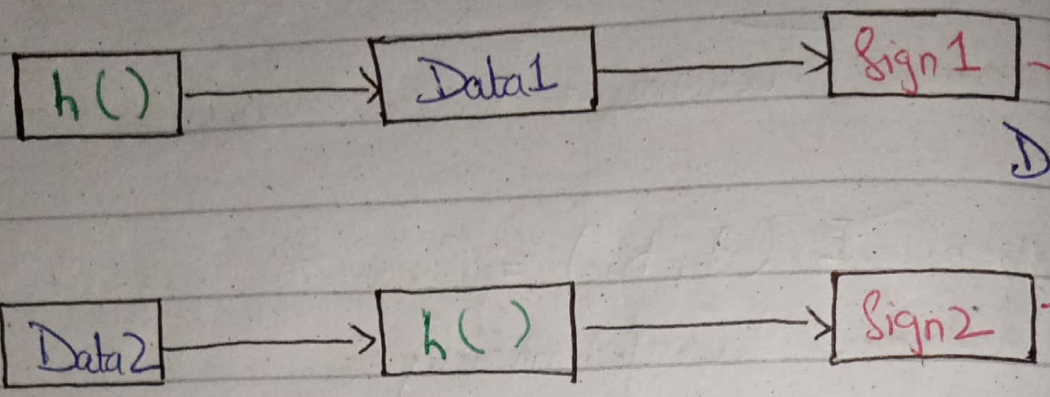
$f(C, K) = d$

Digital Signature -> Unique Association
e.g. Biometric

Signer / Sender

Receiver / Verifier





h( ) → hash function

If sing1 ≠ sign2, Data Modification has been detected.

5) Network Security Controls:

- Achieve Availability

+ Access Control
+ Antivirus and Anti-Malware Software
+ Cloud Security
+ Email Security
+ Firewalls
+ Application Security
+ Intrusion Prevention System (IPS)

4) Hashing: Process of generating a fixed-size output from an input of variable size using the mathematical formulas known as hash functions.

5) Zero-Knowledge Proof: (ZKP)

Cryptographic protocol that enables one person (the prover) to convince another (the verifier) that a particular claim is true without disclosing any details about the claim itself.

You have knowledge but not transferring the knowledge to other person but convincing him/her that you have knowledge.

CRYPTOGRAPHY:

- Practice & study of techniques for secure communication in the presence of third parties called adversaries.

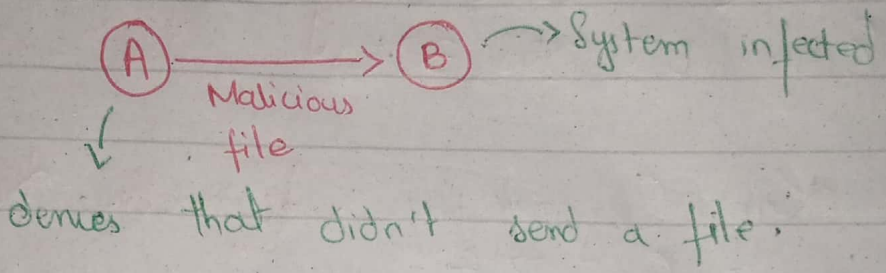
Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

- Act of making code for secure data transmission through network.

FEATURES OF CRYPTOGRAPHY:

- Confidentiality: Hides the contents of a message from unauthorized parties
- Integrity: Ensures that a message has not been altered during transmission.
- Authentication: Verifies the identity of the sender and receiver of a message.

- Non-repudiation: Prevents the sender from denying having sent a message.



CRYPTANALYSIS: Art of breaking the Cryptographic mechanisms.

Cryptology = Cryptography + Cryptanalysis

- Actual information (Plaintext) is transformed (encrypted) by a method (Encryption algorithm) in an unintelligible format (Ciphertext).

- Ciphertext can be transformed (decrypted) into the Plaintext by using some secret information (key) or/and a secret cryptographic algorithm.

Types Of Cryptography:

1) Classical (Symmetric Key Cryptography)
E.g: AES, DES, 3DES

2) Public Key Cryptography (Asymmetric Key Cryptography) E.g: RSA

3) Quantum Cryptography E.g: BB84, B92, SARG04, KMB09

Symmetric Key Cryptography (Same Encryption & Decryption Key)

Asymmetric Key Cryptography (Private & Public Keys)

Symmetric Key is better than Asymmetric Key Cryptography.

Symmetric Key Cryptography: $Y = E_K(X)$ $X = D_K(Y)$

- Basic Encryption Techniques:

1) Substitution (Letters replaced by other letters)
2) Transposition (Rearranging the letter order)
3) Product (Substitution followed by Transposition)

- Types of Cipher Schemes:

1) Stream Cipher (RC4, A5/1, A5/2 etc)
2) Block Cipher (AES, DES etc)

- Possible Attacks:

1) Cryptanalytic attack
2) Brute-force attack

+ Cryptanalytic Attacks:

1) Ciphertext-only attack
   Given: Ciphertext to Cipher analyst

2) Known-plaintext attack
   Given: Ciphertext + samples (P_1, C_1)
   (P_2, C_2)...
   Plaintext & Ciphertext are given

3) Chosen-plaintext attack
   Given: samples (P_1, C_1) (P_2, C_2), ...
   where P_1, P_2, ... chosen by adversary +
   Ciphertext

4) Chosen-Ciphertext attack
   Ciphertext chosen by cryptanalyst / adversary,
   together with its corresponding decrypted
   Plaintext generated with the secret key.

+ Brute-Force Attack Vs Key length:

- Also called Exhaustive Key Search.
- We apply all possible keys.

Key Size (bits)	No. of Alternative Keys	Time required at 1 decryption / μs	Time required at 10^6 decryption / μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 min	2.15 milliseconds
56 DES	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128 AES	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168 3DES	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^{6} years

Computationally Secure but not Unconditionally Secure

Computational Security: No one is going to spend that much time to break the scheme that's why the scheme is secure.

Example : AES, 3DES

Unconditional Security: No concern with computing power

Computing power >> No effect on Scheme Security

Basic Encryption Techniques:

- Substitution Ciphers:

  - Simplest Substitution:
    1) Caesar Cipher

  - Monoalphabetic Substitution:
    1) Playfair Cipher
    2) Hill Cipher

  - Polyalphabetic Substitution:
    1) Vigenère Cipher
    2) Autokey Cipher
    3) One-time Pad

1) Caesar Cipher:

- Trivial & Insecure
- Key: 1 - 25

$E(P, K) = C$

P → Plaintext

K → no of shifts

Encryption: $E_K(X) = (X + K) \bmod 26$

Decryption: $D_K(X) = (X - K) \bmod 26$

C → Ciphertext

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7

I	J	K	L	M	N	O	P
8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X
16	17	18	19	20	21	22	23

Y	Z
24	25

Plaintext: S E C R E T

Ciphertext: T F D S F U

Plaintext: C A R Key: ?

2 0 17

+ 9 9 9

11 9 26

L J A

$E_K(P) = (P+K) \bmod 26$

$D_K(C) = (C-K) \bmod 26$

How to Encrypt Numerical Values in Caesar Cipher?

A	B	C	...	Z	0	1	2	3	4
0				25	26	27	28	29	30

5	6	7	8	9
31	32	33	34	35

Encryption: $E(K)(P) = (P+K) \bmod 36$

Decryption: $D_K(C) = (C-K) \bmod 36$

Weakness Of Caesar Cipher:

1) Small Key Space. Total Keys: 25 or 35
2) Uniformity in encryption

Improvement in Caesar Cipher (Monoalphabetic Cipher)

- Jumble the letters arbitrarily.
- Each plaintext letter maps to a different random ciphertext.
- You make your own Key Table.

Advantage: Key space is increased

Total Keys: 35! or 26!

Possible Attack: (Frequency Analysis)

Language characteristics can be used to unveil the original message. E.g: The frequency of some letters like (a, e, i, o, t) is very high.

Therefore, Frequency Analysis of Individual Alphabets of a Particular language may be used to break Caesar Cipher.

Frequency Analysis is only Applicable for uniform Substitution.

First introduced by Muslim Scientist Abu Al-Kindi in 9th Century.

2) PLAY-FAIR CIPHER:

Charles Wheatstone - 1854

- But named after his friend Baron Playfair
- 5x5 matrix of letters based on a keyword
- Fill in letters of Keyword
- Fill rest of matrix with other letters.

Keyword: MONARCHY

Plaintext: NED UNIVERSITY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

NE → MG
DU → CZ
NI → AG
VE → UF
RS → AT
IT → KS
YX → BW

The letter we want to replace should be considered as row

Plaintext: PHONE

PH → VF
ON → NA
EX → IU

RULES:

+ Plaintext is encrypted two letters at a time.

+ If a pair is a repeated letter, insert filler like 'X'. E.g:

FLOOR → FL OX OR

+ If both letters fall in the same row, replace each with letter to right (wrapping back to start from end) E.g:

AR encrypts as RM

+ If both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom) E.g:

MU encrypts to CM

+ Otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair. E.g

HS encrypts to BP

Security of Playfair Cipher:

- Better security than Monoalphabetic Cipher
- Since have 26x26 = 676 digrams.
- Would need a 676 entry frequency table to analyse (versus 26 for a Monoalphabetic) and correspondingly more ciphertext.

Calculate the Cipher text for the word "NED UNIVERSITY" given the secret keyword "FACTOR".

F	A	C	T	O
R	B	D	E	G
H	I/J	K	L	M
N	P	Q	S	U
V	W	X	Y	Z

NE ⟶ SR
DU ⟶ GQ
NI ⟶ PH
VE ⟶ YR
RS ⟶ EN
IT ⟶ LA
YX ⟶ ZX

Ciphertext: SRG QPHYRENLAZ

Hill Cipher: (Lester S. Hill, 1929)

- A substitution cipher based on Linear Algebra.

- Encryption: A block of n letters from plaintext is considered as a vector of n dimensions, and multiplied by an invertible n×n key matrix, modulo 26.

Plaintext: ACT

Key Matrix: $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

ACT => 0 2 19

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \begin{matrix} A \\ C \\ T \end{matrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \begin{matrix} P \\ O \\ H \end{matrix} \pmod{26}$$

15 14 7 => POH

Ciphertext: POH

- DECRYPTION: A block of n letters from Ciphertext is considered as a vector of n dimensions and multiplied by the inverse of key matrix, modulo 26

Inverse of key matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

!! Not all matrices are invertible.

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \begin{matrix} A \\ C \\ T \end{matrix} \pmod{26}$$

Decrypted text: ACT

Finding The Modular Inverse Matrix:

- Modulus Theorem:

For an integer a and modulus m, let:

$$R = \text{remainder of } \frac{|a|}{m}$$

Then the residue r of a modulus m is given by:

$$r = \begin{cases} R & \text{if } a \geq 0 \\ m - R & \text{if } a < 0 \text{ and } R \neq 0 \\ 0 & \text{if } a < 0 \text{ and } R = 0 \end{cases}$$

- Example:

1. 80 Mod 26

$\frac{|80|}{26} = 3$ R 2 => $80 \geq 0$ => 80 Mod 26 = 2

2. $-80 \text{ Mod } 26$

$\frac{|-80|}{26} = 3R\,2 \Rightarrow -80 < 0$ and $2 \neq 0$

$\Rightarrow -80 \text{ Mod } 26 = 26 - 2 = 24$

3. $-52 \text{ Mod } 26$

$\frac{|-52|}{26} = 2R\,0 \Rightarrow -52 < 0$ and $0 = 0$

$\Rightarrow -52 \text{ Mod } 26 = 0$

VIGENÈRE CIPHER: Uniformity in Key

- Encryption involves adding k mod 26 to the numerical equivalent of each letter.
- The keystream is simply a keyword repeated as necessary.

Key: SECRET

Plaintext: NED UNIVERSITY

Ciphertext:

N	E	D	U	N	I	V	E	R	S	I	T	Y
13	4	3	20	13	8	21	4	17	18	8	19	24
S	E	C	R	E	T	S	E	C	R	E	T	S
18	4	2	17	4	19	18	4	2	17	4	19	18
31	8	5	37	17	27	39	8	19	35	12	38	42
mod 26												
5	8	5	11	17	1	13	8	19	9	12	12	16
F	I	F	L	R	B	N	I	T	J	M	M	Q

Cipher: FIF LRBNITJMMQ

Advantage: Same letters are substituted differently.

Security: Identifying the no. of translation alphabets, and then attack each separately can break the Vigenére Cipher.

AUTOKEY CIPHER: (by Vigenère)

No Uniformity in Key

- Key is as long as the message.
- Keyword is prefixed to message as key.
- Knowing keyword can recover the first few letters which become the basis to guess rest of the message.
- Still have frequency characteristics to attack.

Example #1

Keyword: DECEPTIVE

~~Key: deceptive~~

Plaintext: wearediscoveredsaveyourself

Key: deceptive we are discovered sav

Add k mod 26

Ciphertext: zicvtwqngkzeiigasxstslvvwla

Example # 2:

Keyword: SECRET

Plaintext: NED UNIVERSITY

Key: SECRETNEDUNIV

Transposition Ciphers:

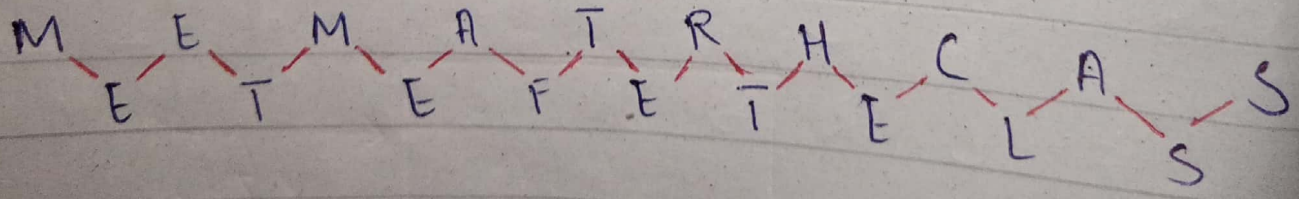
1) Rail Fence Cipher
2) Row Transposition Cipher

Rail Fence Cipher:

- Write message letters out diagonally over a number of rows then read off cipher row by row.
- No alphabet Substitution
- Jumble / Shuffle the letters

Plaintext: MEET ME AFTER THE CLASS
Key: 2 (Pattern)

Ciphertext:



MEMATRHCASSETEFETELS

Row Transposition Cipher:

- A more Complex Transposition.

Steps:

1. Write letters of message out in rows over a specified no. of columns.

2. Then reorder the columns a/c to some key.

3. Write the columns (top to bottom) from start.

Plaintext: ATTACK AT THREE PM

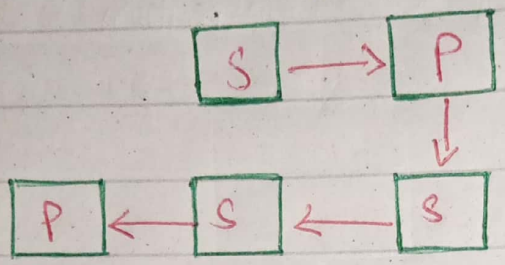
2	4	3	6	1	5
A	T	T	A	C	K
A	T	T	H	R	E
E	P	M	X	Y	Z

This reordering is Key

↳ Row Major Or Column Major

Ciphertext : CRYAAETTMTTPKEZAHX

SP - NETWORK: Applying permutation & substitution repeatedly in a specific patte



DES / AES Scheme

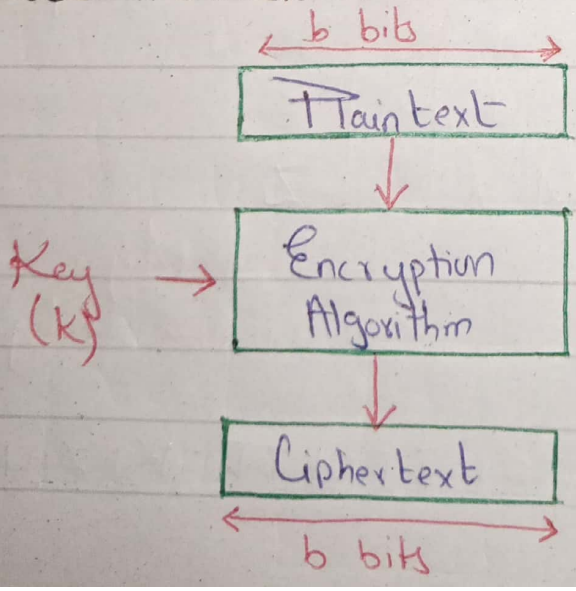
DES / AES Schemes work on binary string.

BINARY STRING:

In modern world, we do encryption using binary string. There are two schemes:

- Block Ciphers
- Stream Ciphers

- BLOCK CIPHER:



- A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

- Typically, a fixed block size of 64 or 128 bits is used.

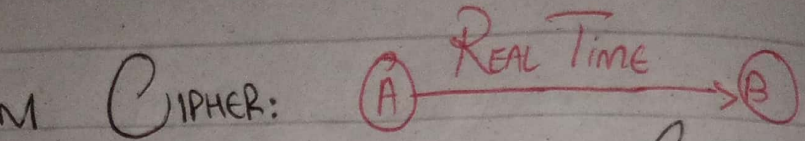
For DES (64 bits)
For AES (128 bits)

- Limitation of block cipher is if you donot have complete block (i.e bits) of data, you cannot encrypt data, you have to wait.

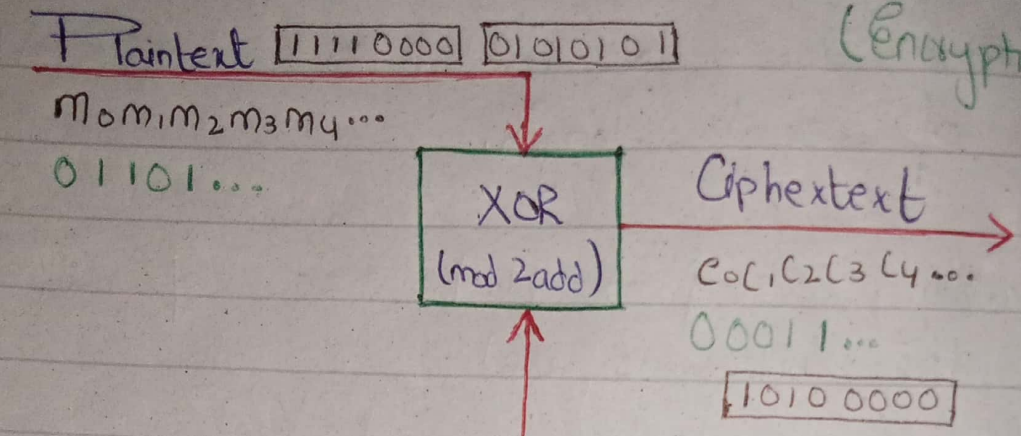
- There will be delay in block cipher due to wait for block to complete.

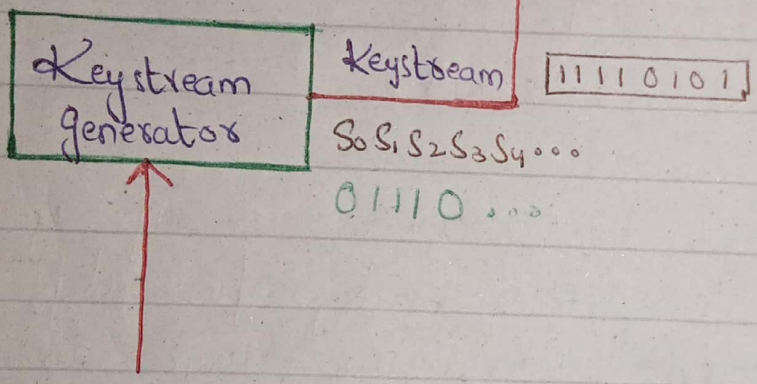
- Block cipher scheme is not ideal for real time communication.

- Stream Cipher:



Sender (Encryption)





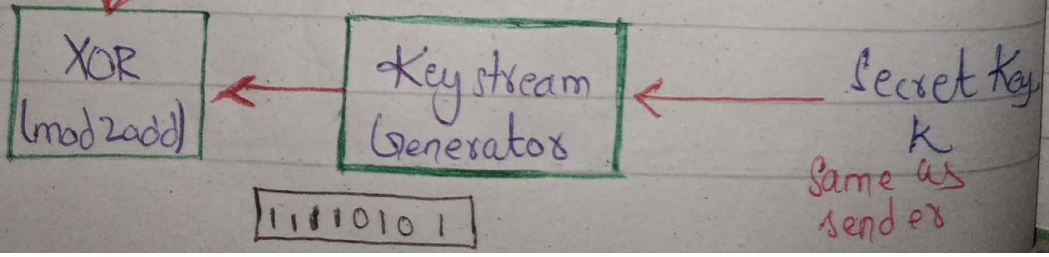
Secret key, k (will make the generator generate the same sequence of bytes)

Plaintext: 0 1 0 1 0 1 0 1

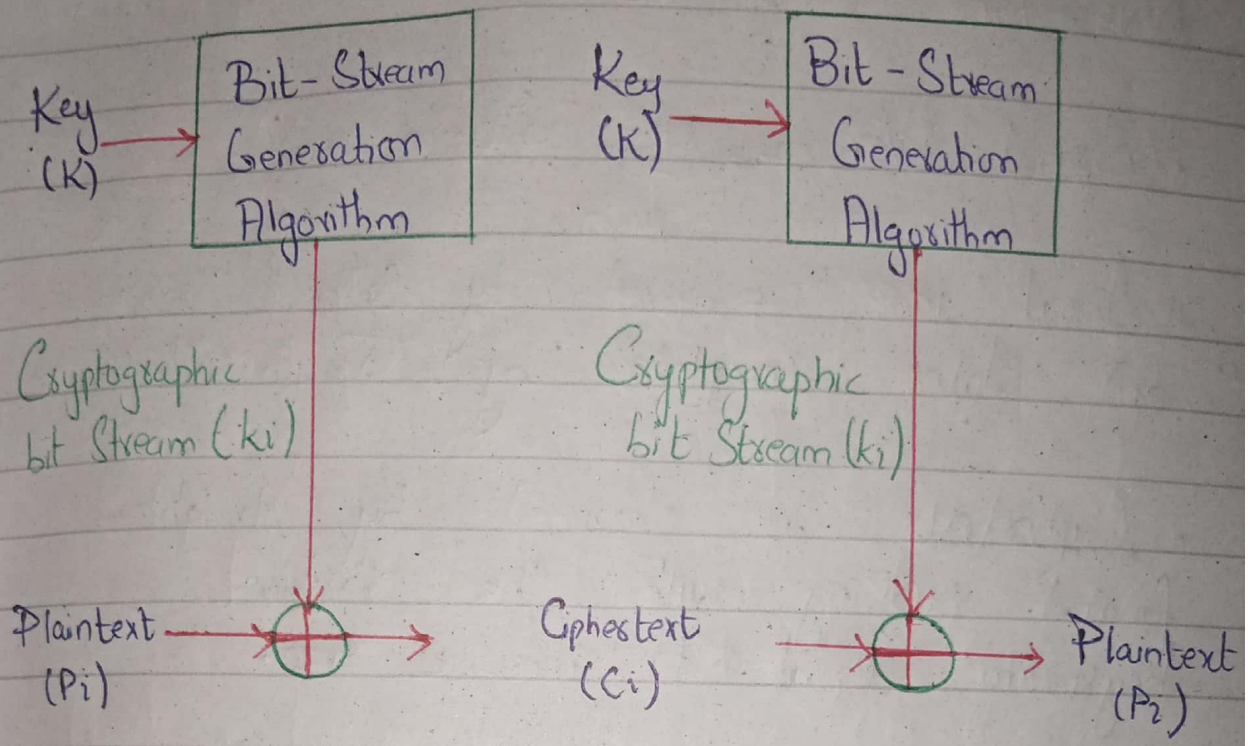
Key: 1 1 1 1 0 1 0 1 Add mod 2

Ciphertext: 1 0 1 0 0 0 0 0

Receiver (Decryption)



Book Diagram:



- A Stream Cipher is one that encrypts a digital data stream one bit or one byte at a time.

- Realtime Communication is possible.

Examples:

1 - Autokeyed Vigenere Cipher
2 - Vernam Cipher (One-Time Pad)
3 - RC4

One-Time Pad: (OTP)

- Special Variant of Stream Cipher.

- Initial idea proposed by Gilbert Vernam and later completed by Joseph Mauborgn

- Ciphertext is obtained by straight-forward XORing with the random keystream equal to message size.

- If we make keystream, a truly random ~~scheme~~ sequence then this scheme will be called OTP.

- The size of plaintext & keystream will be same.

- If used properly it is provably unbreakable (Shannon, 1949)

- Provides:
  - Perfect Security /
  - Unconditional Security /
  - Information theoritic Security

if the following Challenges are met successfully:

- Secret Key Distribution
- True Randomness of Key
- Message Authentication

- Avoid Using The Same Key Again!

The Key will not be repeated with certain patterns.

+ In one time pad, we will not use the previously generated keys as it will help the attacker decrypt all the messages encrypted with the previous keys.

- Cannot use OTP in practical system because beside volume of data there will also be a huge volume of keys.

- This scheme will be the most secure scheme in the world, if we are able to keep the key secure and truly random. And the size of P, K and C is same. Then, this ~~key~~ scheme is perfect

Shannon's Theorem:

Suppose $(P, C, K, E_K(\cdot), D_K(\cdot))$ is a crypto system with $\#P = \#C = \#K$ and the key is truly random & secret.

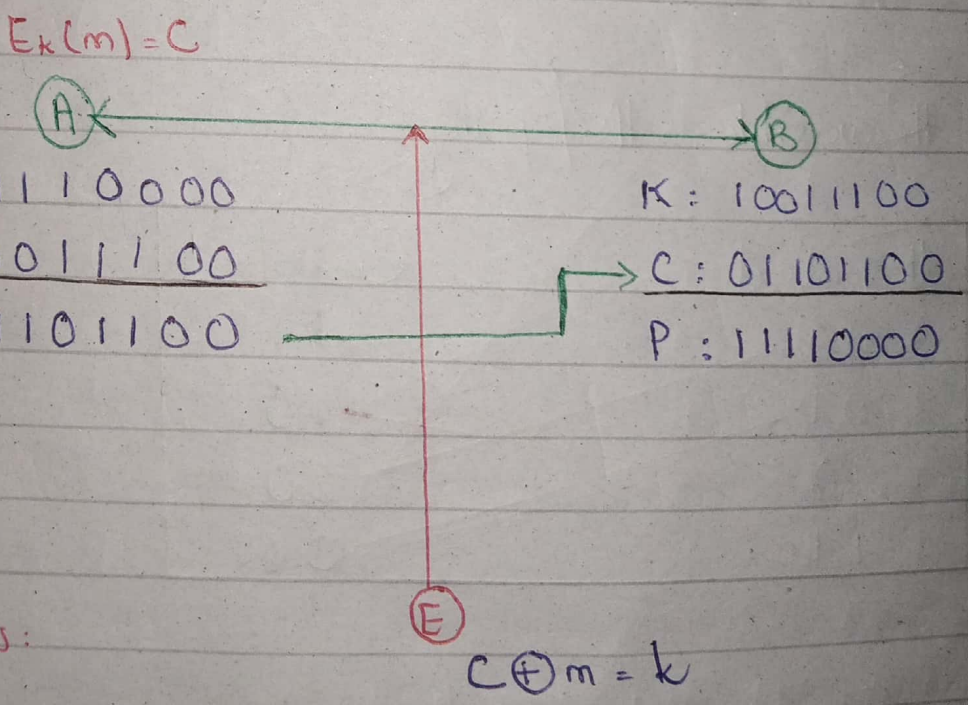
This cryptosystem provides perfect secrecy if and only if

- Every key is used with equal probability $1/\#K$ and
  (50-50 probability of 0 or 1 in Key)
  0.5 on each bit

- For each $m \in P$ and $c \in C$, there is a unique key k such that $E_k(m) = c$

How To Break OTP?

- Eve generates m and asks Alice to encrypt it.
- Eve receives $c = m \oplus k$ from Alice.
- Eve can now compute the key $k = c \oplus m$.
- Eve can decrypt all messages encrypted with k



Assumptions:

- E has access to the channel b/w A and B.
- E impersonate B for A.
- A reuses a key several times

Reversible Vs Irreversible Mapping

A block ciphes operates on a plaintext block of n bits to produce a ciphertext block of n bits.

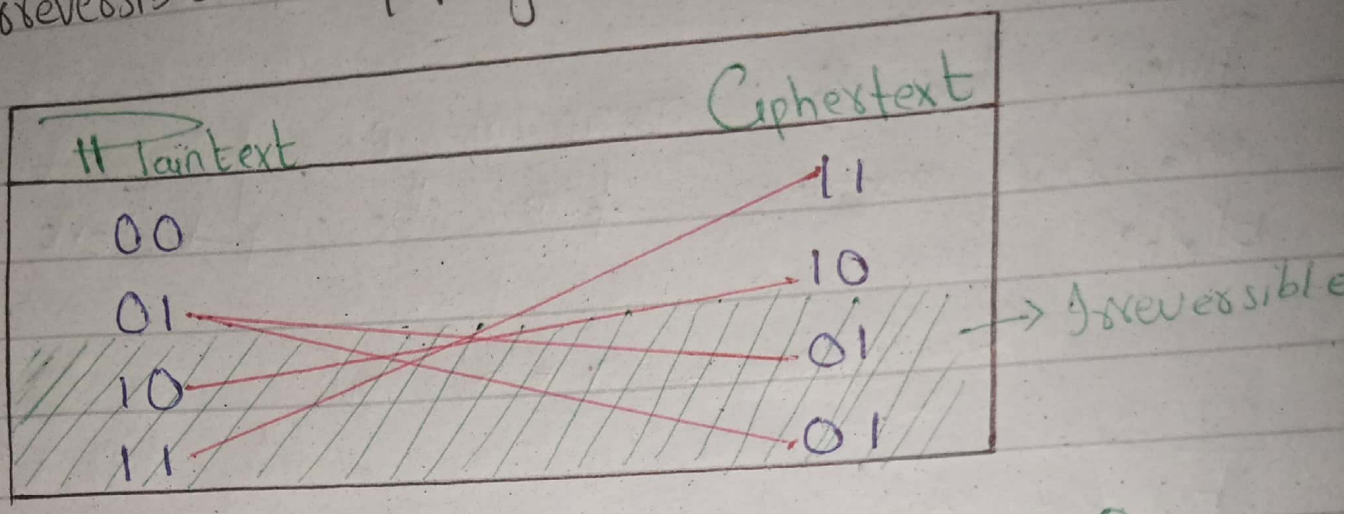
There are 2^n possible different plaintext block and, for the encryption to be reversible (i.e, for decryption to be possible), each must produce a unique ciphertext block.

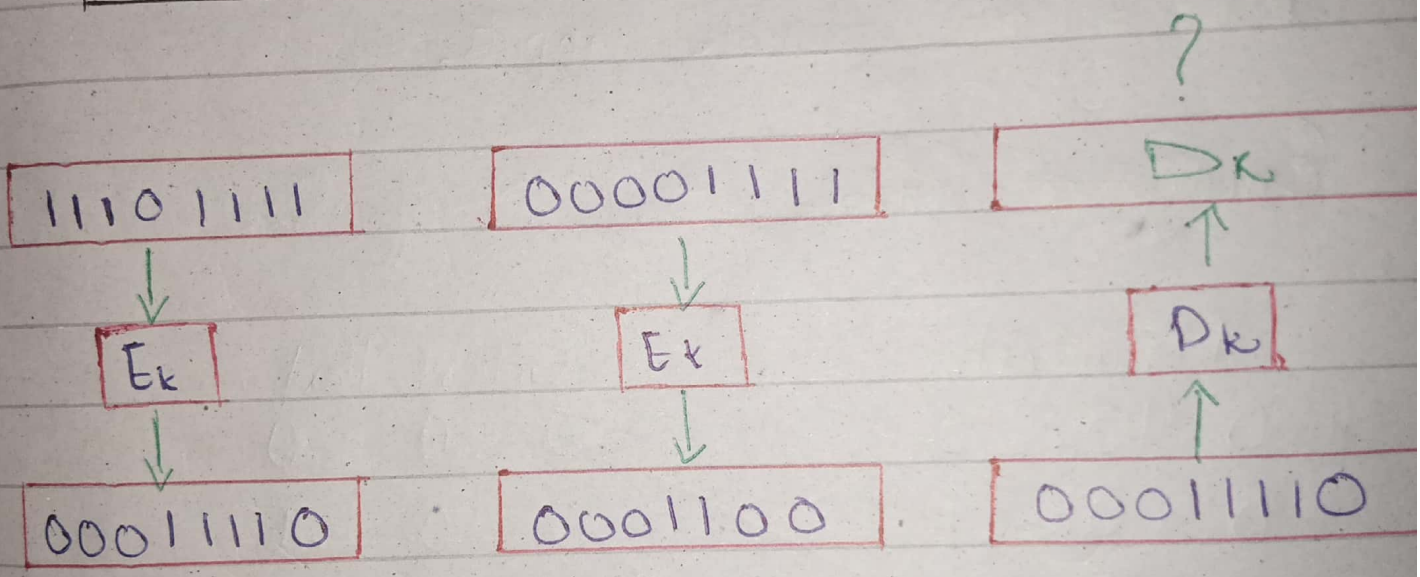
Reversible aka Non-singular
Irreversible aka Singular

Reversible Mapping:

Plaintext	Ciphertext
00	11
01	10
10	00
11	01

Irreversible Mapping:





When we design a block cipher scheme, we have to avoid irreversible mapping.

P	K	C
00		11
01		10
10		01
11		00

=> Ideal block Cipher

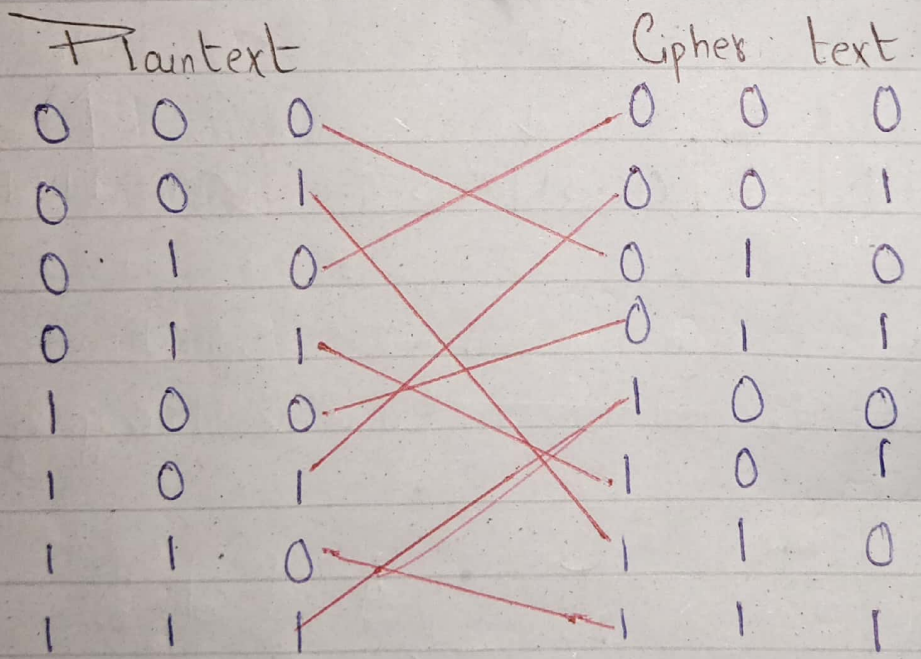
Ideal Block Cipher Scheme:

Allows for the maximum no. of possible encryption mappings from the Plaintext block.

Key Size = $n * 2^n$ bits

For 3 bits possible inputs,

Encryption Table

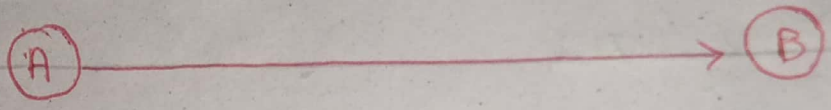


Plaintext: 011 011 000 101 010

Ciphertext: 101 101 010 001 000

What will be the key?

The encryption key for the ideal block cipher is the key table / codebook itself.
(Table that shows the relationship b/w input blocks and output blocks)



I	Key Table
0	0 1 0
1	1 1 0
2	0 0 0
3	1 0 1
4	0 1 1
5	0 0 1
6	1 1 1
7	1 0 0

Check the index of Ciphertext in Key Table

I	Key Table
0	0 1 0
1	1 1 0
2	0 0 0
3	1 0 1
4	0 1 1
5	0 0 1
6	1 1 1
7	1 0 0

Plaintext : 011 011 000 101 010
Ciphertext : 101 101 010 001 000

101 is at index 3, 3 is 011 in binary
I -> Index So, 011 will be plaintext.

If A has no key, would it be easy for attacker to decrypt the message?

Yes! Using Brute force.

General Formula For Ideal Block Cipher Key Size:

Block Size	Key Size
3 bits	24 bits
4 bits	64 bits
5 bits	160 bits
⋮	⋮
64 bits	$2^{64} \times 64 = 1.8 \times 10^{21}$ bits

General formula: $2^n \cdot n$

$= 2^3 \cdot 3 = 24$

$= 2^4 \cdot 4 = 64$

$= 2^5 \cdot 5 = 160$

Block Size ↑ Security ↑

Brute force attack ↑

FEISTEL CIPHER: (by Horst Feistel)

- Approximate ideal block cipher.
- Utilize concept of Product Cipher.
- Feistal proposed the use of a cipher that alternates:
  - Substitution
  - Permutation
- Practical Approach of Claude Shannon's proposal of Product Cipher.

SP-Network (Claud Shannon)

Provide:

- Confusion (Substitution)
- Diffusion (Permutation)

of message & key.

- Symmetric Key
- Block Cipher
- Product Cipher

Confusion - Diffusion

↓ ↓

Substitution - Permutation

Diffusion dissipates statistical structure of plaintext over bulk of ciphertext.

Makes relationship b/w ciphertext and key as complex as possible

Feistal network depends on the choice of following parameters & design features:

- Block Size:

- Larger block size ↑ Larger Security ↑
  But
  Reduced Encryption / Decryption Speed ↓

- Greater Security acheived by Greater diffusion.

- 64-bits -> reasonable trade off
  and
  nearly universal in block cipher design.

- KEY SIZE:

- Larger Key Size ↑ Greater Security ↑
  But
  Decrease Encryption / Decryption Speed ↓

- Greater Security acheived by:
  - Greater Resistance to Brute-Force attacks.
  - Great Confusion

- 128-bits has become a common size now.

- NUMBER OF ROUNDS:

- Number of Rounds ↑ Greater Security ↑

- A typical size is 16 rounds.

- SUBKEY GENERATION ALGORITHM:

Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

- ROUND FUNCTION (F):

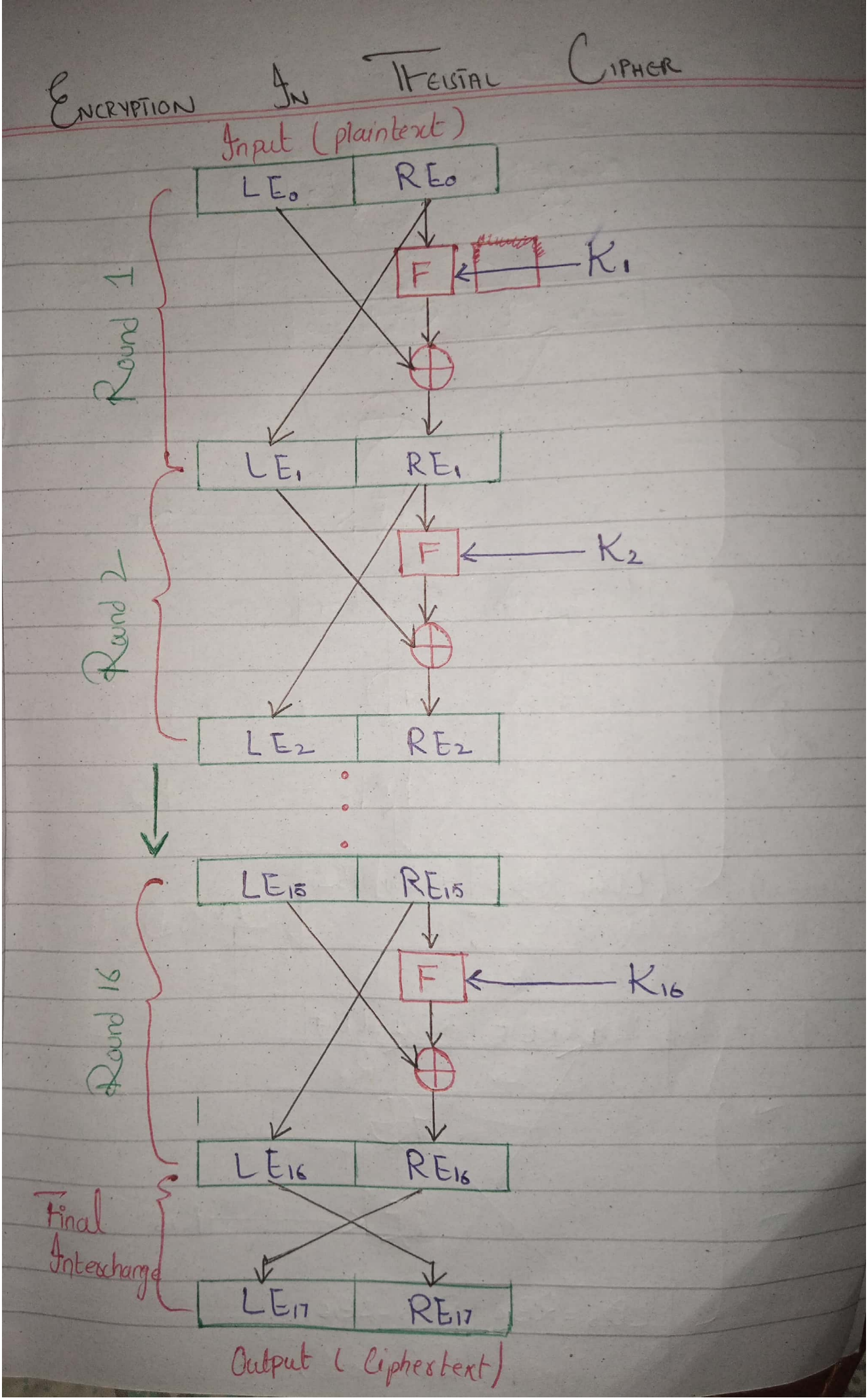
Again, greater complexity generally means greater resistance to cryptanalysis.

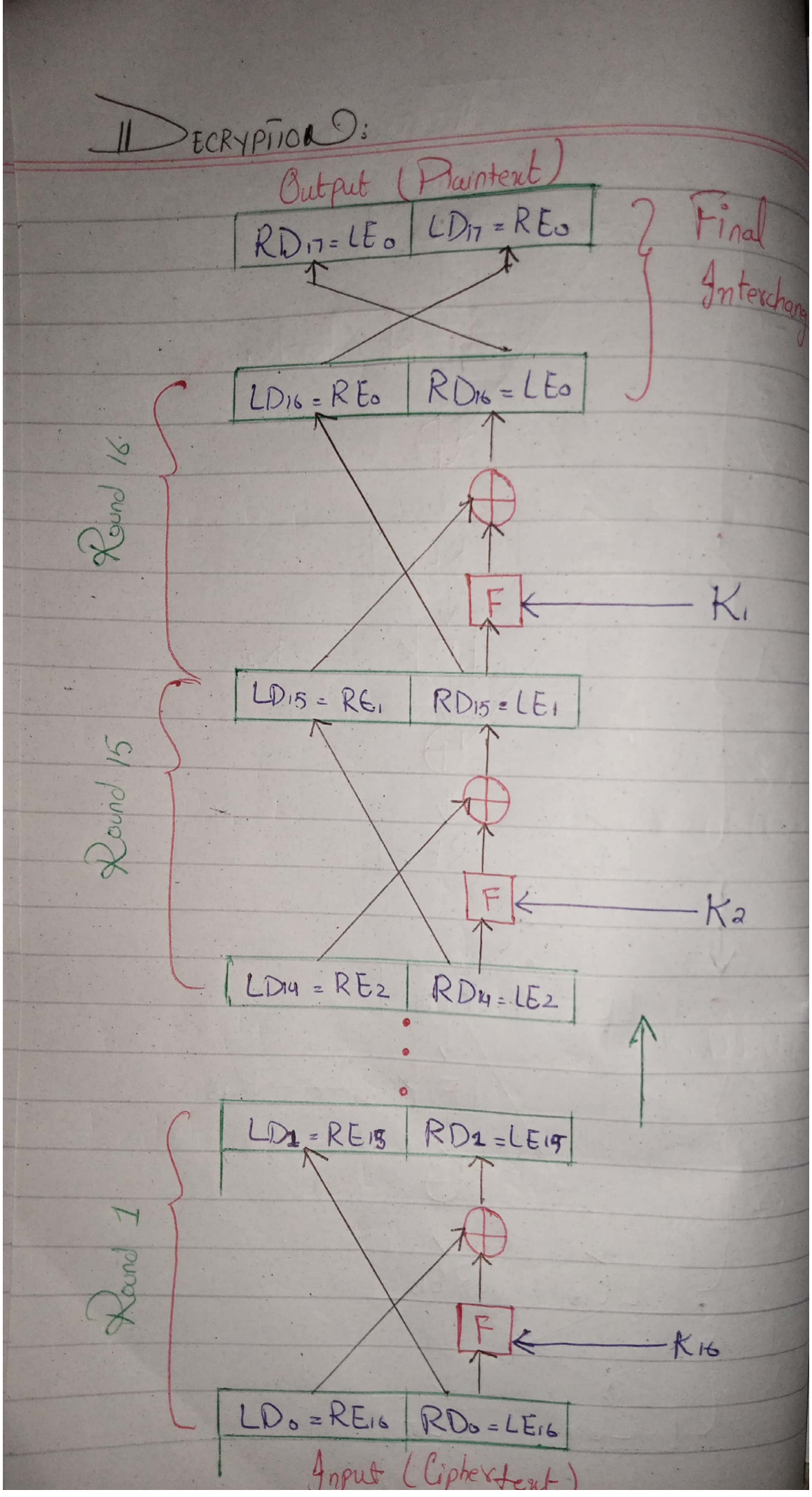
- Fast software encryption / decryption
- Ease of analysis

STRUCTURE: (SP-Network)

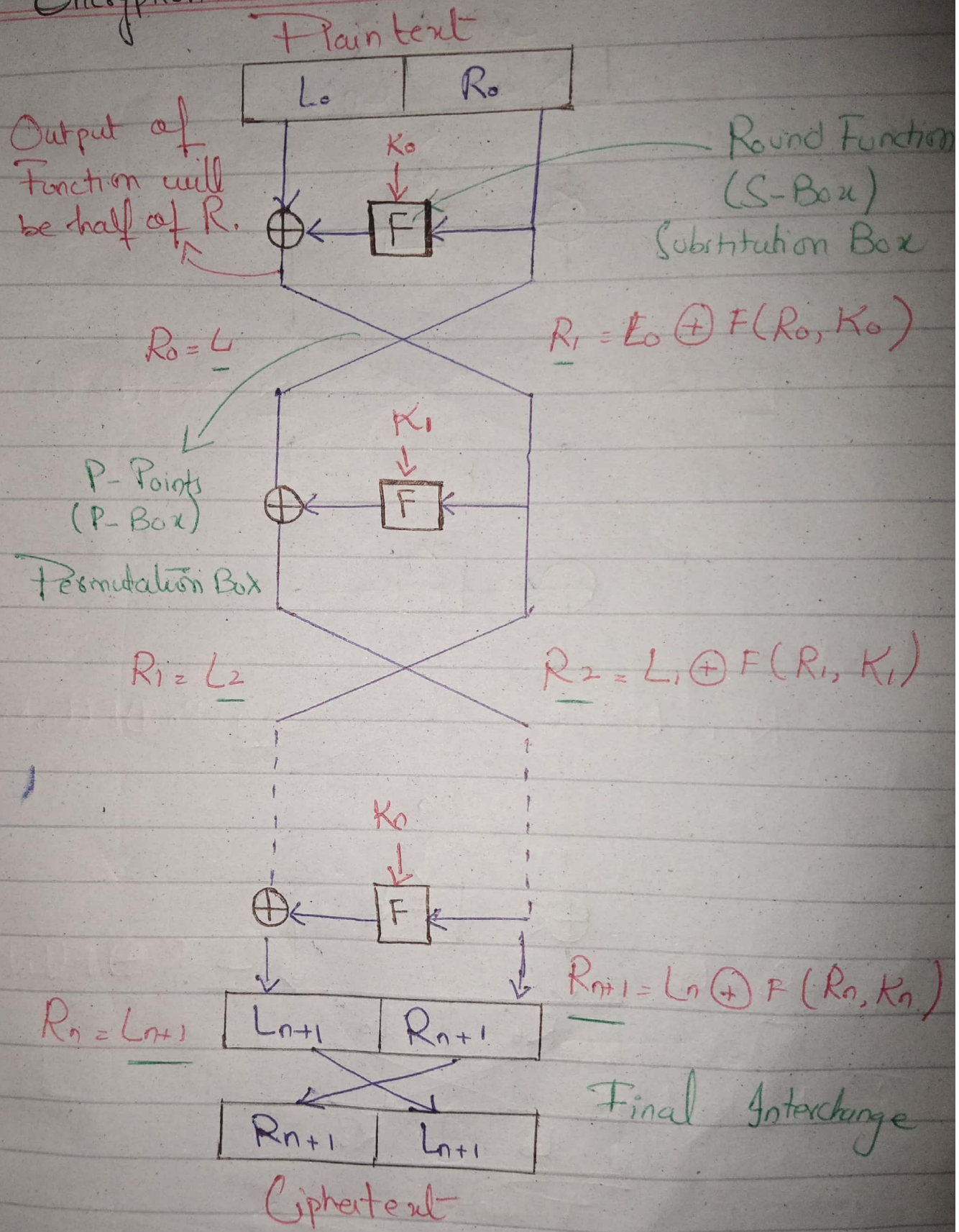
A Substitution is performed on the left half of the data. This is done by applying a round function F to the right half of the data and then taking the XOR of the output of that function and the left half of the data. The round function has the same general structure for each round but is parameterized by the round subkey K_i. Another way to express this is to say that F is a function of right-half block of w bits & a subkey of y bits, which produces an output value of length w bits: $F(RE_i, K_{i+1})$. Following this substitution, a permutation is performed that consists of interchange of two-halves of the data.

Encryption in Feistal Cipher

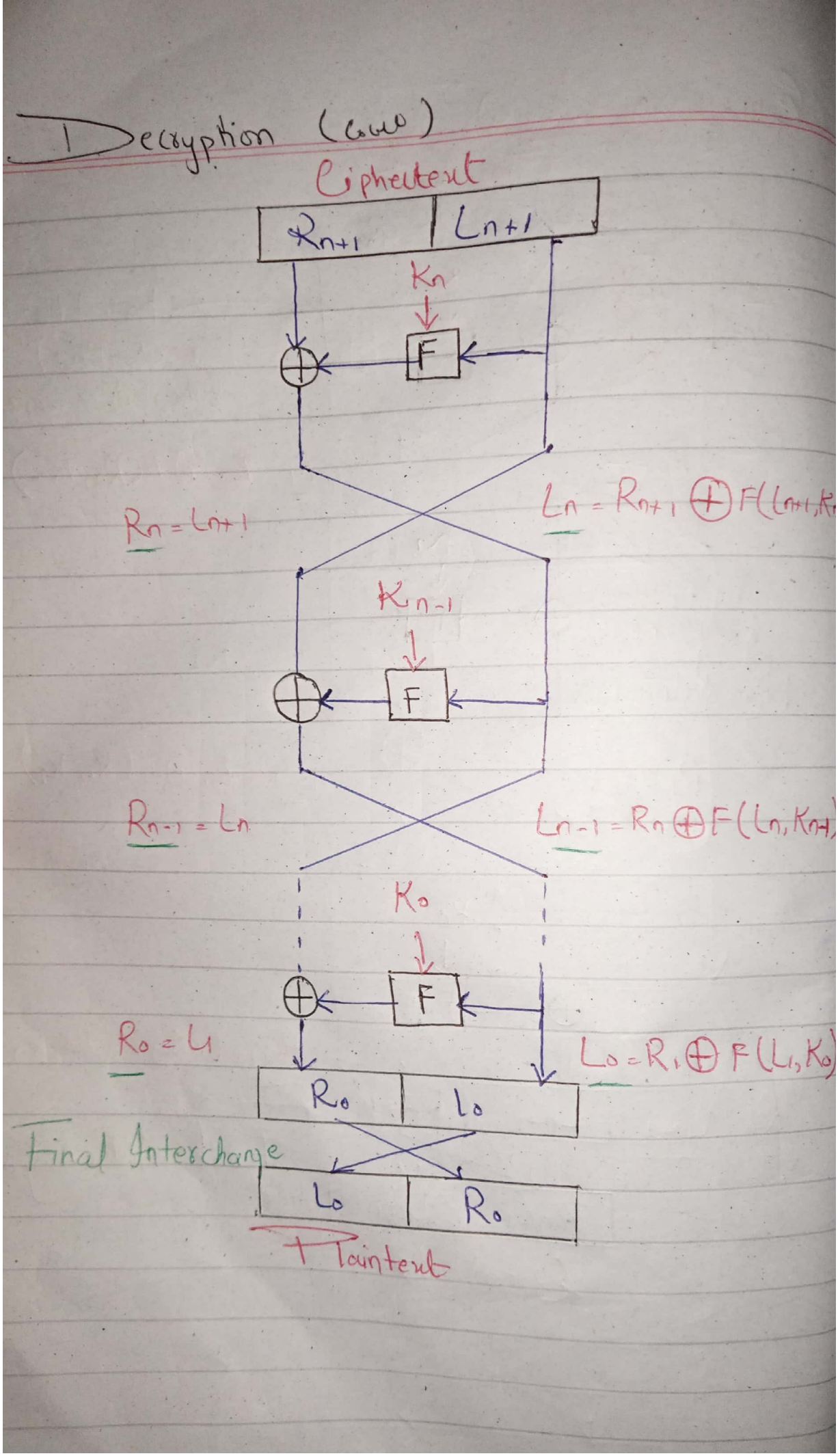



Decryption:
Output (Plaintext)
RD17 = LE0
LD17 = RE0
Final
Interchange
LD16 = RE0
RD16 = LE0
Round 16
F
K1
LD15 = RE1
RD15 = LE1
Round 15
F
K2
LD14 = RE2
RD14 = LE2
LD1 = RE15
RD1 = LE15
Round 1
F
K16
LD0 = RE16
RD0 = LE16
Input (Ciphertext)

Encryption (C.ω)



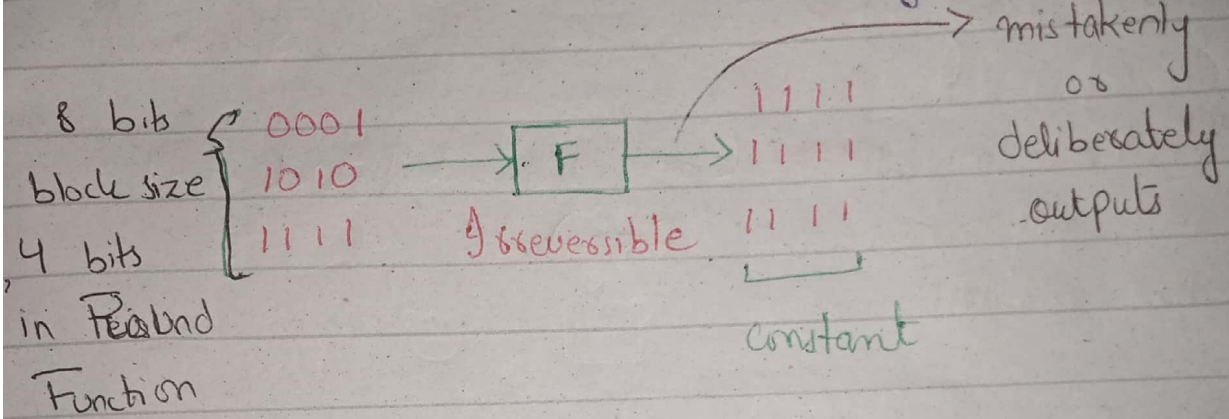
Decryption (cont)



constant Function -> Irreversible
e.g

Round Function in Feistal Cipher:

- Round Function F is always invertible.



It can still be successfully encrypted or decrypted. How? How

Fix,

Block size = 8-bit
No. of rounds = 6
F is constant

If we neglect the fact that the round function outputs constant value mistakenly then the encryption done will be trivial.

P: 1100 1010

C: 1010 1100

DES (Data Encryption Standard)

- 1976 → 1999 Standard by NBS (National Bureau Standard)
- named by FIPs
- Broken in 1999 (by distributed.net and EFF) in 22 hours 15 minutes
- based on Feistal Ciphers
  - DES Design

DES Design:

- based on Feistal Ciphers

Fix:

Block Size = 64 bits
No. of Rounds = 16
Key = 64 bits

Key Generation Algorithm

- Internal Structure of Round Function F is specifically designed for DES.

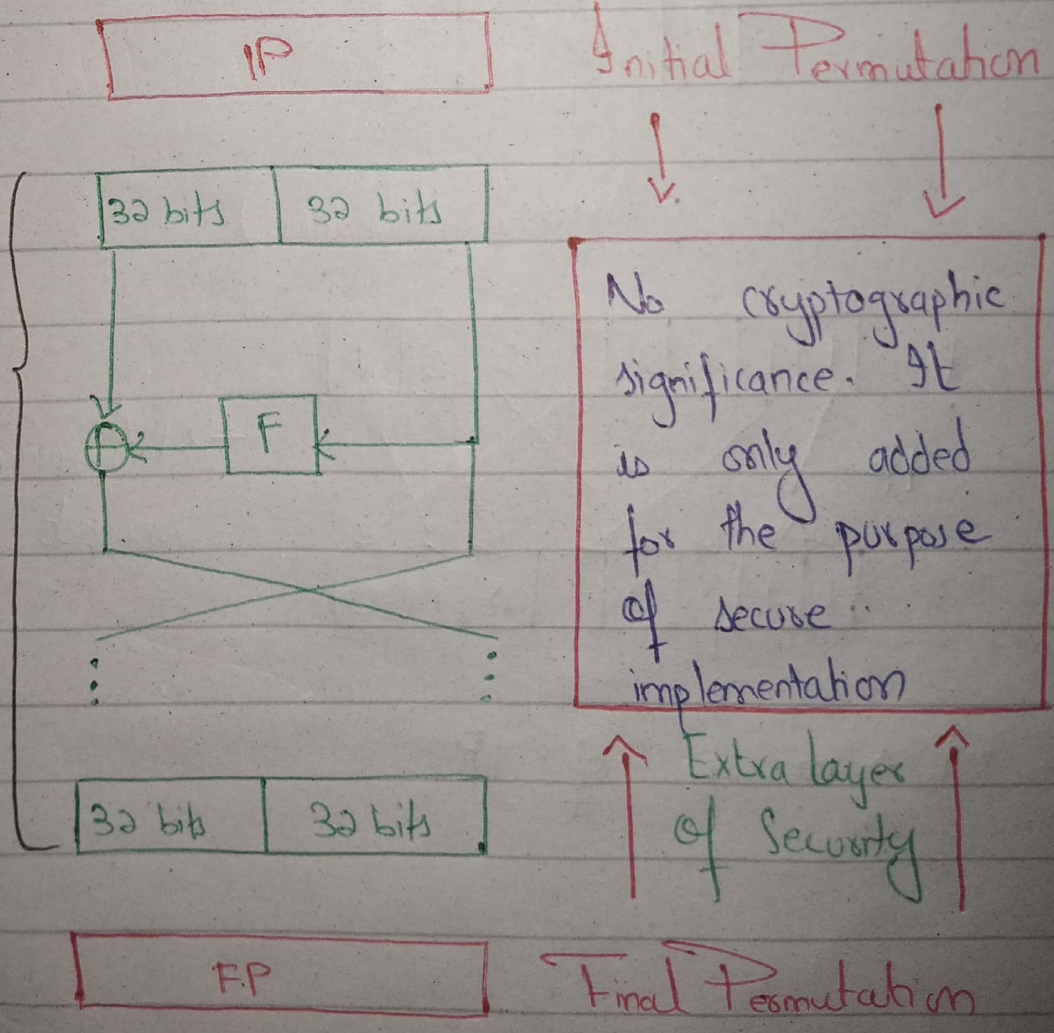
For each of the Round Function, there will

be a unique key.

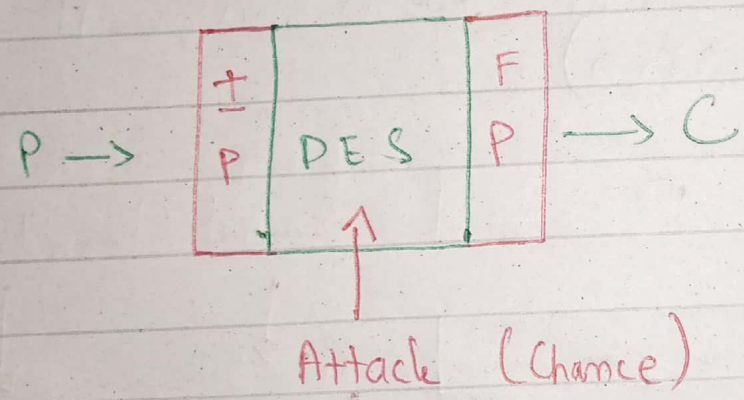
- Key generation algorithm is specifically designed for DES.

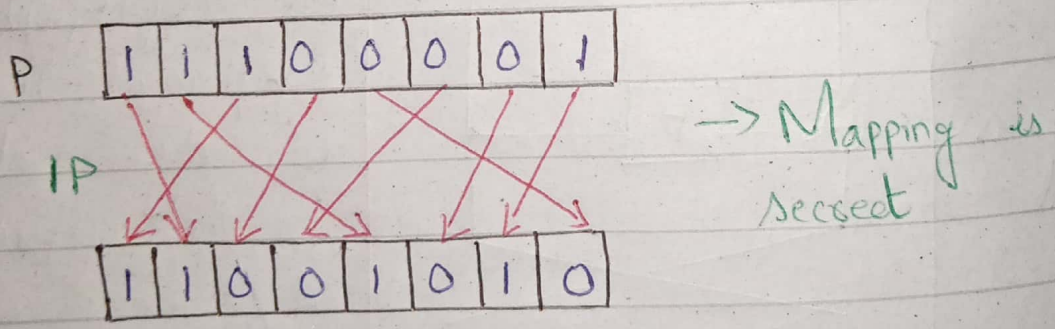
- Unique Keys till 16 rounds.

- There is a process that is defined on top of block known as IP (Initial Permutation)

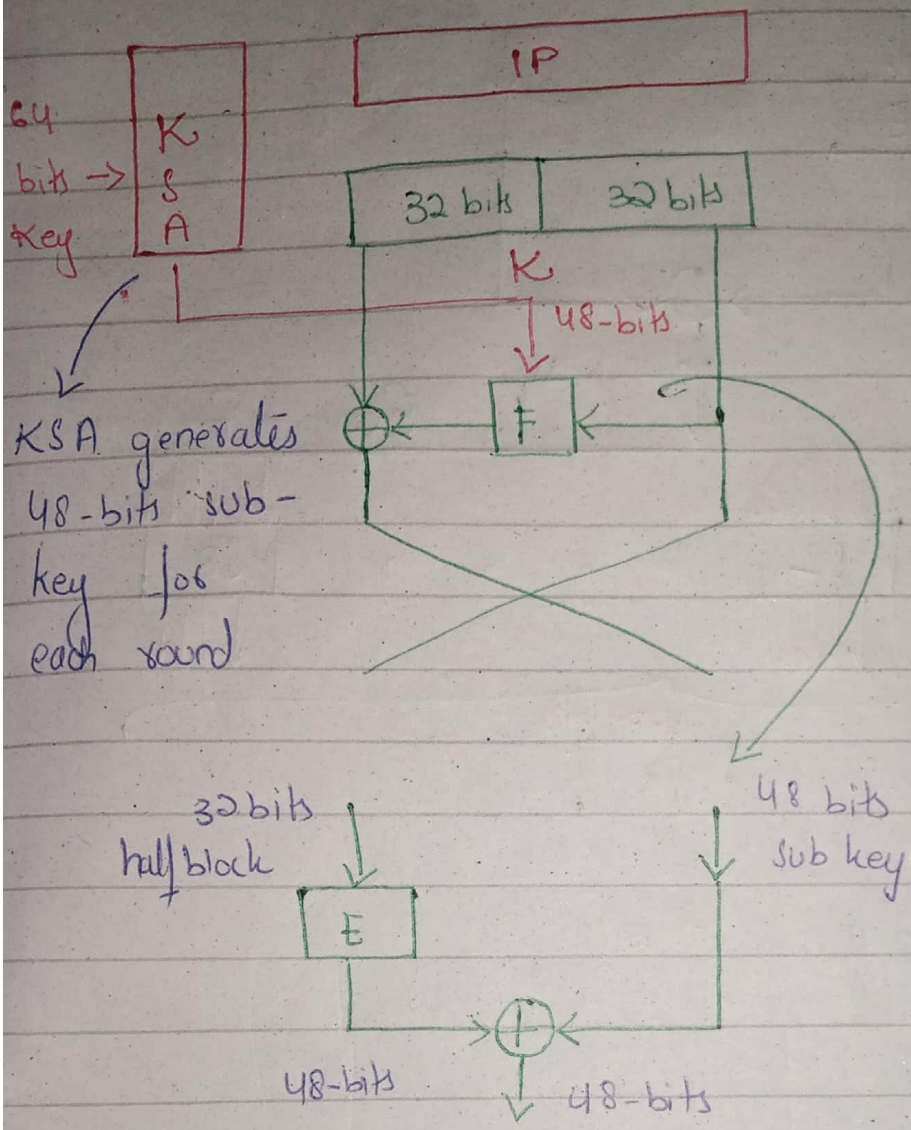


- At the Implementation point, there is chance that the plaintext is retrieved by the attackers when it is given to the hardware for encryption. Therefore, Initial & Final Permutation has been added at the start and end of hardware (DES). IP and FP Just shuffles the bits.



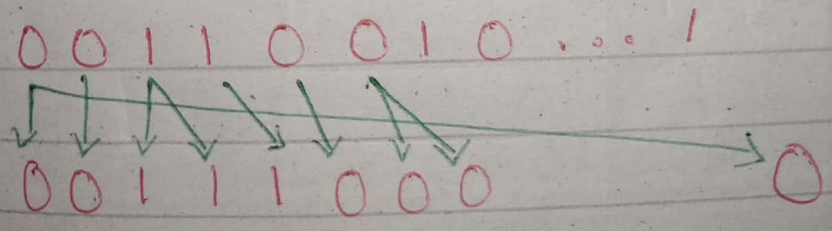


- FP → mirror of IP

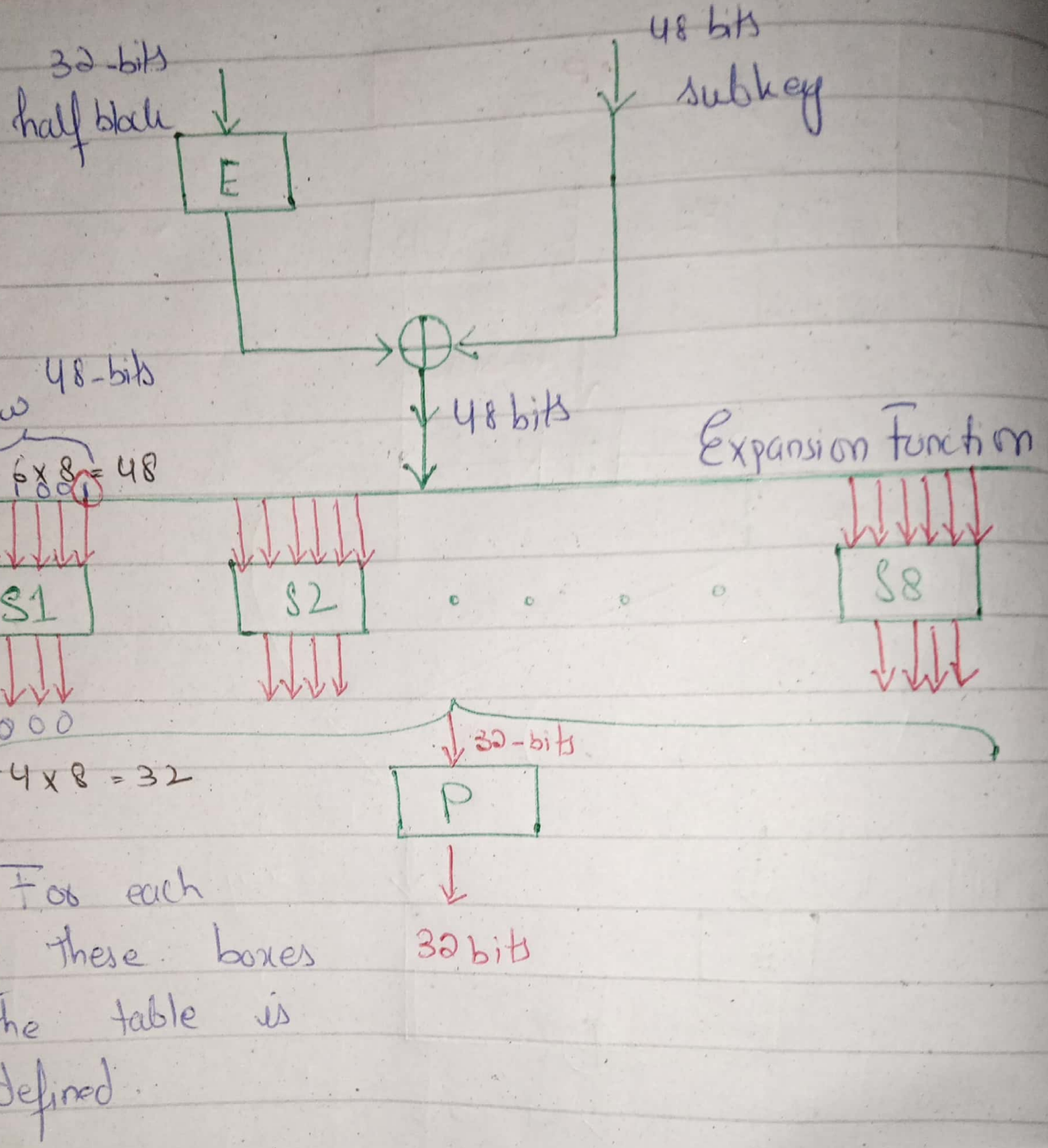


32 and 48 cannot be XORed because of different bit size.

Expansion Function : Duplicate some of the bits.



F



For each of these boxes the table is defined.

	0	1	2	3	4	5	6	7	A	B	C	D	E	F
0	F	E	3	D	4	5	0	C	1	8	2	9	A	
1														
2														
3														

S-box: S1

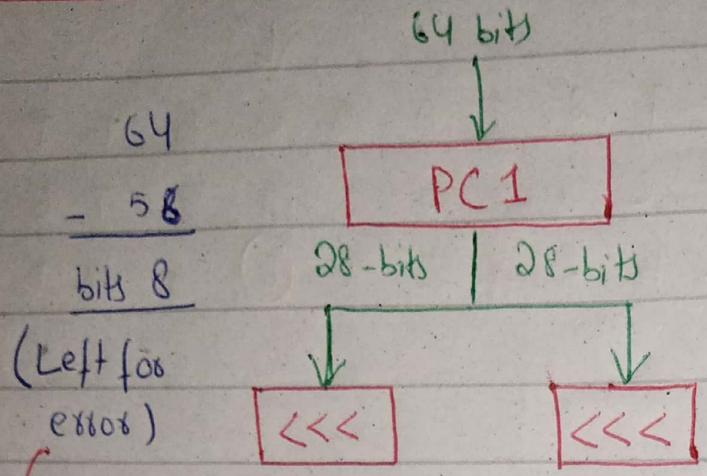
1100

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	F	E	3	D	4	5	0	C	1	B	2	9	A	8	7	E
01	F	0	E	D	1	C	2	B	3	A	4	9	8	5	7	E
02																
13																

P-box: P

3	12	13	11
10		4	
2			6
	1	5	
14	15	0	
9	8	7	
			18
	16	17	

KEY SCHEDULING ALGORITHM:



Permuted Choice 1

64
- 56
bits 8
(Left for error)

To put the layer of confusion to hacker.

Only 56 bits are effectively used.

1 1 0 0 0
1 0 0 0 1 ROL 1 → Rotate Left 1
0 0 0 1 1 ROL 1

How many rotates?

Round No	No. of Rotates
0	1
1	1
2	2
3	1
⋮	
F	2