বিছমিল্লাহির রহমানির রাহীম

Segment : 02

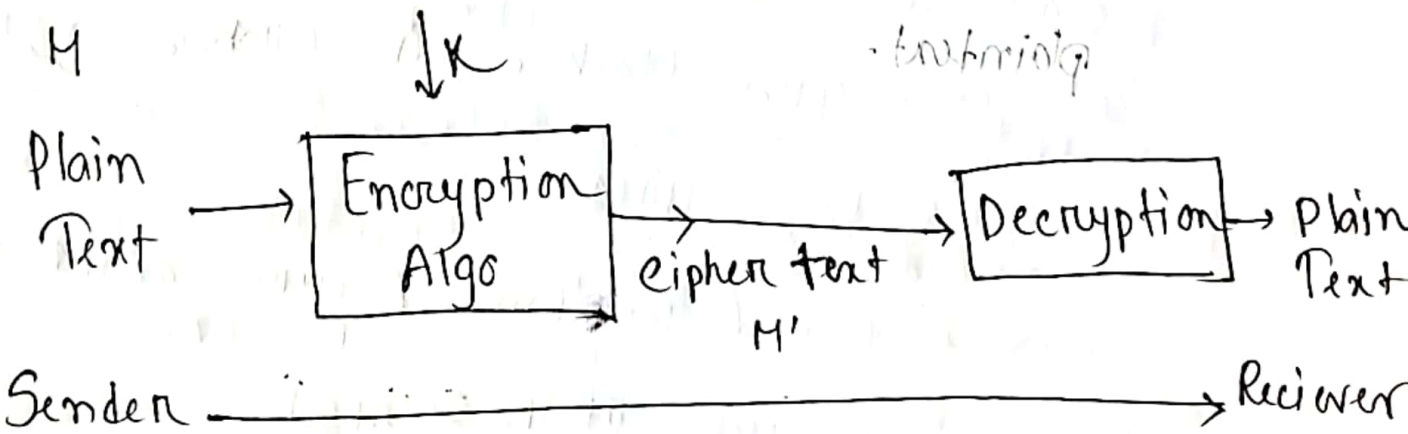
(*) Cryptography:

যেসব যেকোন technique যার মাধ্যমে আমরা plaintext কে cipertext করিতে বা ciphertext কে plaintext এ convert করি

Plaintext → Normal Massage

Ciphertext → Secret Massage [যাকে read করতে পারে না বা hard to understand]

(*) Confidentiality রক্ষা করার জন্য আমরা cryptography use করি



⑧ Symantic Cipher Model:

① Secret key: The key used for encryption and decryption. Also reffered an symantic key.

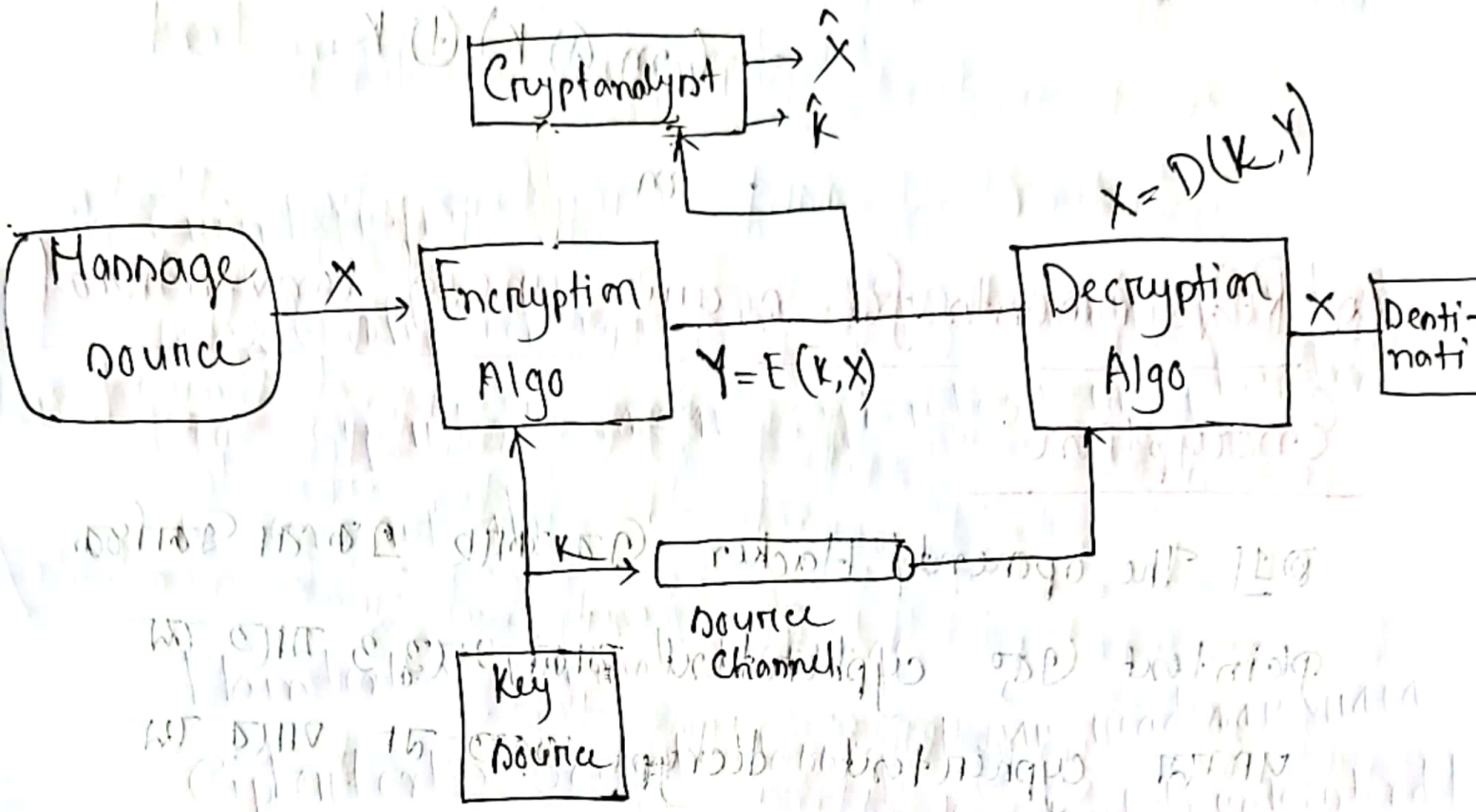
② Plaintext: Normal Mannage

③ Ciphertext: Secret Mannage

④ Encryption Algorithm: Performn encryption and does various substitution and transformations on the plaintext.

⑤ Decryption Algorithm: It taken secret key and ciphertext and produces the original plaintext.

⊛ Symmetric Cipher Model:



Key → 0 1 0 1 1 1 0 0 1 0

Plain text → 1 1 0 0 0 1 1 0 0 0

XOR → same output 0
different 1

Encryption $C = E_K(m) = m \oplus K$

$$\begin{array}{r} 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \\ \oplus\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0 \\ \hline \end{array}$$

cyphertext → 1 0 0 1 1 0 1 0 1 0

Decryption $D_K(C) = C \oplus K$

$= (m \oplus K) \oplus K$

$= m$

⊛ Requirements for secure use of conventional Encryption:

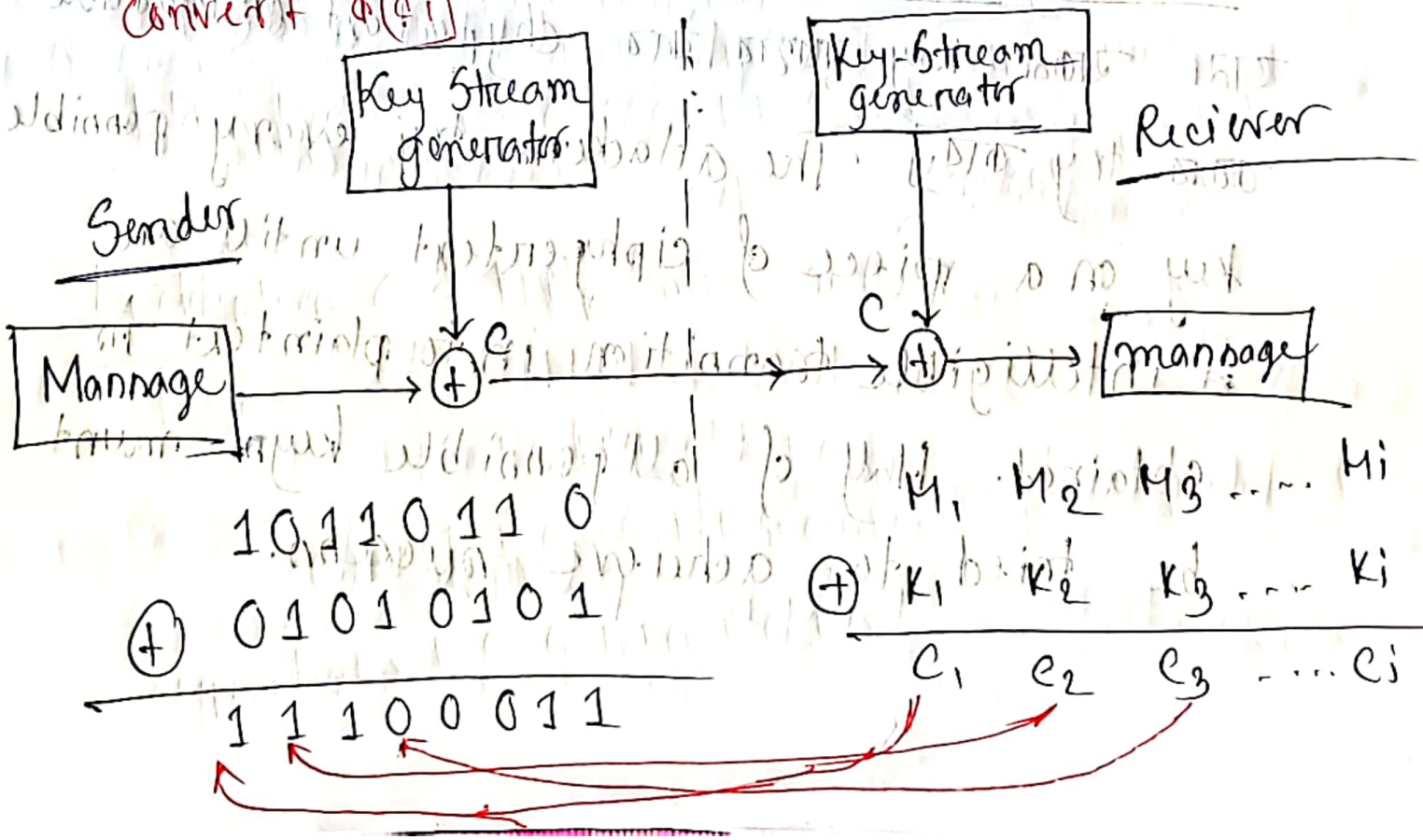
⊛ 1] The opponent/ Hacker এর কাছে একটা বা একাধিক plaintext এবং ciphertext থাকা সত্ত্বেও যাতে সে পরবর্তী ciphertext decrypt করতে না পারে সে ব্যবস্থা নিতে হবে।

2] যে key টি ciphertext এ ব্যবহার হয়েছে তার কপি sender এবং reciever এর কাছে থাকতে হবে এবং তা secure রাখতে হবে, কারণ secret key যদি কোন Hacker বা যেকেউ manage পেয়ে ও জানতে পারবে।

3] Encryption Algorithm secure রাখার প্রয়োজন নেই key secure রাখা প্রয়োজন।

(A) Encryption Algorithm যেভাবে বাধার সম্মুখীন হয়েছে তার কারণ এই algo use করে অনেক developer রা কম খরচে ভালো encryption করতে পারে এবং encryption algorithm এর chip বাজারজাত করে।

(X) Stream Cipher: এটি message কে, বা plaintext কে bits এ রূপান্তর করলে এবং bits এর উপর বা প্রত্যেকটি bit এর উপর algorithm (Encryption) and key apply করে Encrypt করার technique কে stream cipher বলে। [pseudurandom generator Manage কে bits এ convert করে।]



⊛ Cryptoanalysis: [cyphertext কে key, add করে plain text, plain text কে understand করা।] Cryptanalytic aHackn relay on the nature of the algorithm plus perhaps some knowledge of general characteristics of plaintext and key which the hacker use to understand the plaintext and make readable/ decrypt the unreadable cypher text.

⊛ Brute force AHack: [AHacker বা Hacker যারা সকল key ব্যবহার করে cypertext কে readable করার try করে।] The aHackers try every possible key on a piece of ciphertext until an intelligible transition into plaintext is obtained. Half of all possible keys must be tried to achieve success.

Trial and Error

A Encryption is said to be secure if it contains two criteria:

① The cost of breaking the cipher exceeds the value of the encrypted information. [cyphertext break করতে যদি cyphertext encryption এর চেয়ে বেশি টাকা খরচ হয়।]

② The time required to break the cipher exceeds the lifetime of the information. [cyphertext break করতে করতে যদি data/information এর validity শেষ হয়ে যায়।]

* Substitution Cipher: It is a technique in which the pattern of plaintext are replaced by other pattern or by numbers or symbols.

[যে letter বা symbol একবার replaced করতে ব্যবহৃত হয়েছে সে 2nd time ব্যবহার হবে না।]

Substitute করে ciphertext তৈরি করা,

⑧ Substitution Technique:

① Ceasar Cipher: (Shift Cipher)

name ↑ 3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Plain:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Cipher:	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

	16	17	18	19	20	21	22	23	24	25
Plain:	Q	R	S	T	U	V	W	X	Y	Z
Cipher:	t	u	v	w	x	y	z	a	b	c

Encryption:

$C = E(3, P) = (P + 3) \bmod 26$ (ভাগ শেষে যা থাকে)

Ciphertext

$A \rightarrow = (0 + 3) \bmod 26$

$= 3 \rightarrow d$

Encryption:

FIVE MINU TES

Plaintext:

Ciphertext: i l y h p l a x w h v

Decryption:

$$P = D(3, C) = (C - 3) \mod 26$$

(*) Brute Force Cryptanalysis for Caesar Cipher:

MEET ME After THE PARTY

Key: Plain: PHHW PH DIWHU WKH NRJD

1: oggv og chvgt vjg vaic

2: nffu nf bgufn uif uphb

3: meet me after the party

Key গুলোর মাধ্যমে plain text টা আলাদা তৈরি করে,

⊛ One Time Pad (Vernam Cipher)

Plaintext: H E L L O

0 1 2 4 5
A B C D E ---]

7 4 11 11 14

Key: b d x y c [randomly taken]

1 0 23 24 2

Adding: 8 4 34 35 16

Subtract: 8 4 8 9 16 [যদি সংখ্যা 26 থেকে বড় হলে 26 (-) করে]

Ciphertext: i e i j q [যদি 26 এর বড় alphabet → 26]

⊛ Single use

⊛ Cannot be cracked.

⊛ Key is random and never reuse so it is impossible to learn anything about Message and Ciphertext without secret key.

⊛ Transposition Techniques / Ciphers

⇒ Some sort of permutation applied on the plaintext latters. [plaintext lattern গুলোর position change করে করা হয় যাকে তাকে transposition বলে।]

⊛ Rail fence: (Simplest) / Keyless

Plaintext : Neso Academy is the best

depth : 2 → Row

R-1	n		s		a		a		e		y		s		h		b		s	
R-2		e		o		c		d		m		i		t		e		e		t

[1st এ R-1 গুলো লিখবো than R-2 লিখলে Ciphertext পাব।]

Ciphertext: nsaaeyshbseocdmiteet

(*) Columnar Transposition Technique:

Plaintext: FIVE MINUTES ENGENEERING

Key: 4 3 5 1 2 [column এর চাহা ক্রম হবে যা]

1	2	3	4	5
F	I	N	E	M
I	N	U	T	E
S	E	N	G	I
N	E	E	R	I
N	G			

Ciphertext: ETGRVUNEMEIIFISNNINEEG

⊛ Block Cipher:

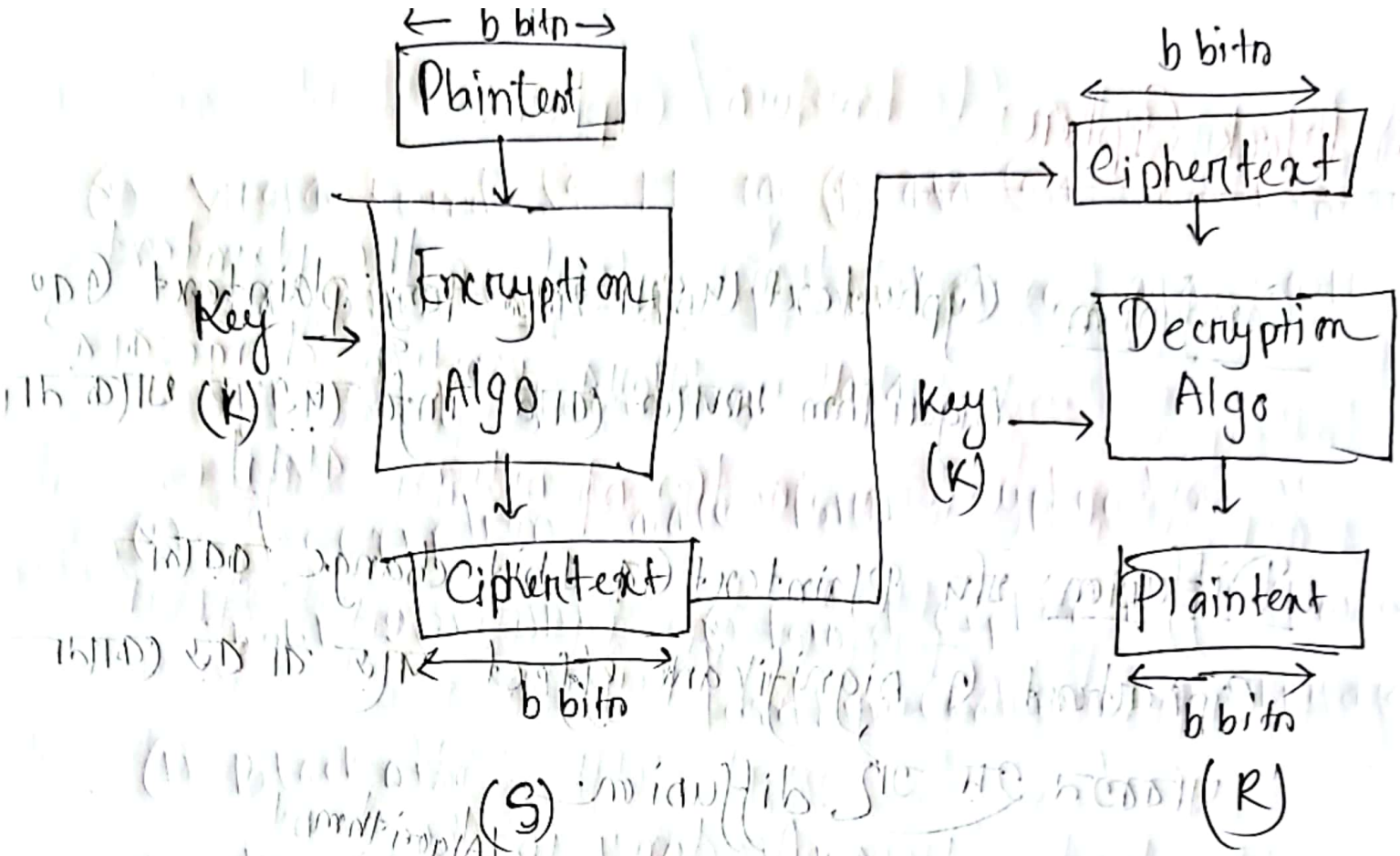
Confusion: Ciphertext দেওয়া থাকে কিন্তু plaintext এবং Algorithm সম্পর্কে কোনো info দেওয়া থাকে না।

Diffusion: যদি Plaintext এর 1 bit change করলে Ciphertext এ significant effect পড়ে বা বড় কোনো পরিবর্তন হয় তাই diffusion.

⇒ Plaintext কে blocks এ devide করে key (Algorithm) কে প্রত্যেক block এ apply করে encrypt করা হয়, Ciphertext এ block এ generated হয়।

Key size → (40, 56, 64, 128, 256 bits)

যে size এর key তার size এর key প্রত্যেক block এর উপর apply হবে।



(*) Difference between Stream & Block Cipher.

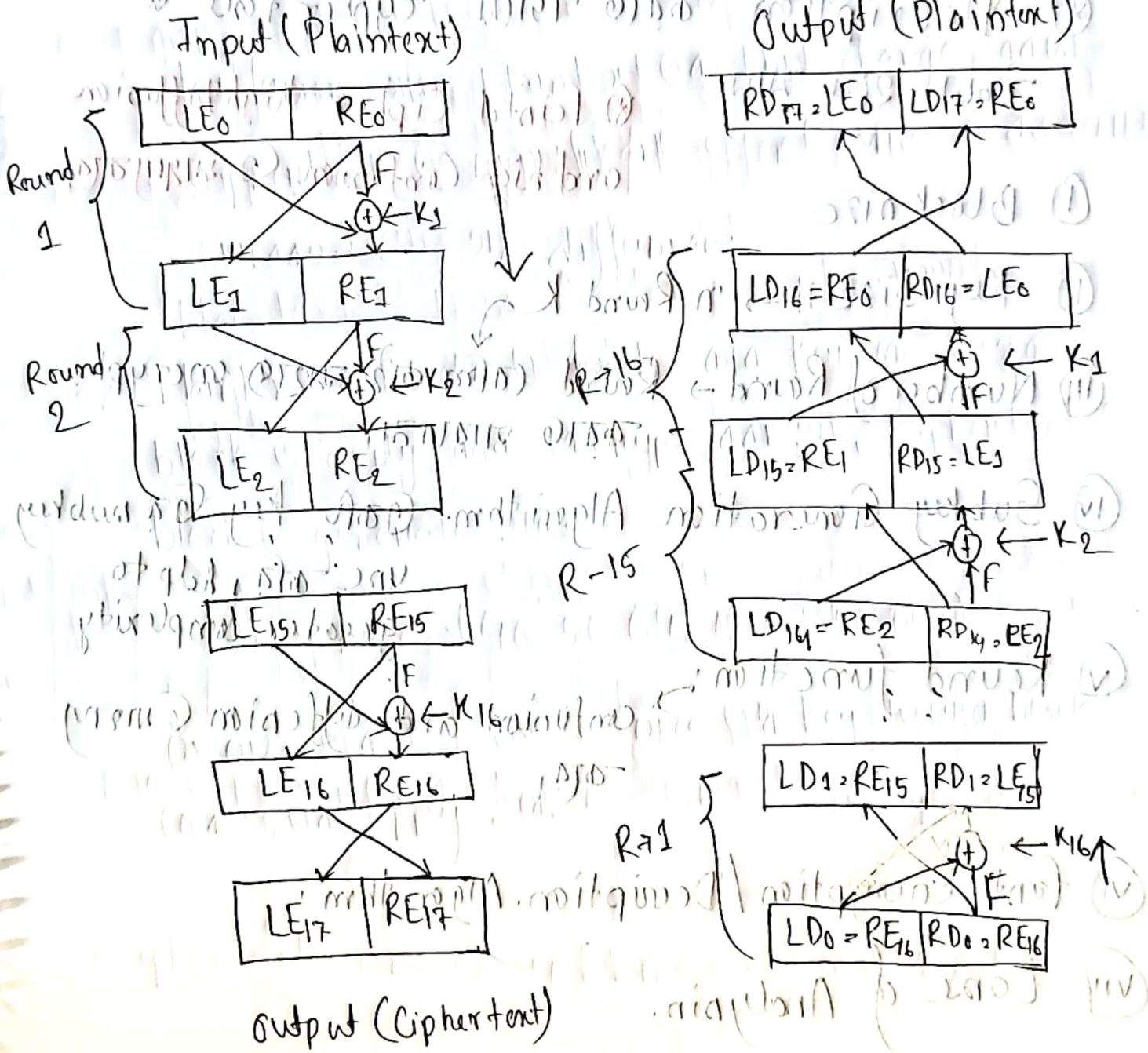
	Stream Cipher	Block Cipher
Length	Bits or Bytes	Block size → 64 or 128 bits
Design	Complex	Simple
Principle	Confusion	Confusion & Diffusion
Speed	Faster	Slower
Encryption	CFB (Cipher Feedback) and OFB (Output Feedback)	Electronic Code Book (ECB) and Cipher Block Chaining (CBC)
Decryption	XOR	Reverse of Encryption
Example	Vernam Cipher	DES, AES

Feistel Cipher Structure: (Encryption

(*) Input ... LE_0 ও RE_0

↓

(Plaintext)



* প্রত্যেক Round এ LE কে ⊕ করি Function এর সাথে এবং permutation করি এবং LE ও RE Rearrange করি।

* Decription করতে গিয়ে cypher text ও key উল্টা/হয়ে যায়।

* Feistel Cipher high Diffusion and high Confusion এ সাহায্য করে।

(i) Block size

(ii) Key Size → n Round K

(iii) Number of Round → Round বেশিবার সহজে encrypt করতে পারবে।

(iv) Subkey Generation Algorithm. এটি key এর subkey তৈরি করি, help to greater complexity

(v) Round function → confusion and diffusion এর জন্য করি।

(vi) Fast Encryption / Decription. Algorithm

(vii) Ease of Analysis.