Thu, Feb, 01 Lecture 02

1. Ceaser Cipher ✓
2. Mono alphabetic Subsi
3. Vigenere Cipher
4. Affine Cipher
5.

$C = (ap + b) \bmod n$

$P = a^{-1}(c - b) \bmod n$

Inverse ? Extended Euclidean Algo

b	o	o	k
a	n	n	x

$a = 17$

$b = 19$

$B = 1$

$Q = 2$

$P = (17 \times 1 + 19) \bmod 26$

$P =$

$a = n$

$n = a - nq$

$U = V$

$V = U - Vq$

$q = a/n$

a	n	q	U	V
7	26	0	1	0
26	7	3	0	1
7	5	1	1	-3
5	2	2	-3	4
2	1		4	-11
				+ 26

25 ✓

$GCD(a, b) = 1$

26/17

Relative prime is necessary

$-1 - (2)(1) \quad -1-2$

a	0	s	18
b	1	t	19
c	2	u	20
d	3	v	21
e	4	w	22
f	5	x	23
g	6	y	24
h	7	z	25
i	8		
j	9		
k	10		
l	11		
m	12		
n	13		
o	14		
p	15		
q	16		
r	17		

a	n	q	u	v
17	26	0	1	0
26	17	1	0	1
17	9	1	1	-1
9	8	1	-1	2
8	1		2	-3 +26
				23

b o o k

k x x h

↓ ↓ ↓

b o o

$$\boxed{\begin{array}{l} 23(10-19) \bmod 26 \\ 23(-9) \bmod 26 \\ -207 \bmod 26 \end{array}}$$

$23(23-19) \bmod 26 = 23 \times 4 \bmod 26$
$= 14$

$23(7-19) \bmod 26 =$

$23(-12) \bmod 26 = 11$

★ Homework

Groups / Feeds / Rings in Maths.

Sat Feb, 03 Lecture 03

ZICVTWQNZRGZVTWAVZHCQYGLMGJ

Selected - Frequency Analysis

To break a Vigenere cipher, you can use frequency analysis. Here are the steps to follow:

1. Determine the length of the key: The first step is to find the length of the key used in the Vigenere cipher. You can do this by looking for repeating patterns in the encrypted text. If the key length is unknown, you can try different key lengths and analyze the results.

2. Divide the encrypted text into groups: Once you have the key length, divide the encrypted text into groups of that length. Each group will correspond to a letter encrypted with the same key letter.

3. Analyze the frequency of each group: Count the frequency of each letter in each group. This will give you a frequency distribution for each group.

4. Compare the frequency distributions: Compare the frequency distributions of the groups with the expected frequency distribution of the English language. The most common letters in English are E, T, A, O, I, N, S, H, R, and D. Look for similarities between the frequency distributions of the groups and the expected frequency distribution.

5. Determine the key: Once you have identified the most likely letters for each group, you can determine the key by finding the shift between the encrypted letters and the corresponding decrypted letters. This shift will give you the key letter for each group.

6. Decrypt the text: Finally, use the key to decrypt the entire text by shifting each letter back to its original position.

Remember that frequency analysis is not foolproof and may not always work, especially if the text has been encrypted using additional techniques to counter frequency analysis.

Auto Key (extension of viginere Cipher)

key => book
PT => Information
key => bookinforma

PlayFair

m	e	s	a	g
b	c	d	f	h
i/j	k	l	n	o
p	q	r	t	u
v	w	x	y	z

key = message

information
kO hn

Hill Cipher

Modular Mathematic don't have division.

$$\begin{bmatrix} \quad \text{key} \quad \end{bmatrix}\begin{bmatrix} \quad \end{bmatrix} = \begin{bmatrix} \quad \end{bmatrix}$$

↓

$\frac{1}{Det}[Adj]$ $Det^{-1}[Adj]$

Rail Fence

key = 2 -----.

Information Security

```
I       r       i       e       i
  n   o   m   t   o   s   c   r   t
    f       a       n       u       y
```

I r ie i

Columnar Transposition Cipher

key => Alphabetic

secret

	5	2	1	4	3	6
	s	e	c	r	e	t
PT →	l	n	f	o	r	m
	a	t	i	o	n	s
	e	c	u	r	i	t
	y	x	x	x	x	x

f i u nt c r n i o o r l a ey

x x x x

Chapter 2 of Cryptography and Network Security

Ciphers

Symmetric

DES

Asymmetric

P_u = Public
P_r = Private

RSA.

Data Small, Critical
→ Banking Information
→ Signature RSA

Algammel, ECC

$M \rightarrow \text{Encryption} \rightarrow E \rightarrow C$

Pr_A Pu_B — ①
Pu_B Pr_A — ②

Only using Private key of sender
→ Source Authentication

$M - E \rightarrow E \longrightarrow D \rightarrow D \leftarrow C$

$\boxed{Pr_A \quad Pu_B \quad Pr_B \quad Pu_A}$ This is correct

$Pu_B \quad Pr_A \quad Pu_A \quad Pr_B$

This is useless as public key of A is available everywhere.

It is more secure because we are encrypting the cipher text.

During Decryption Entropy of 1st one is greater.

(AS/1 AS/2 → Youtube. Gallowa Field)

PT → E

K → E

E → C

Quiz # 02

det of key 2

Key 1 $\begin{bmatrix} 9 & 7 \\ 3 & 4 \end{bmatrix}$ $= \dfrac{1}{\det A} \text{Adj } A$

$= \dfrac{1}{36-21} \begin{bmatrix} 4 & -7 \\ -3 & 9 \end{bmatrix}$

Z_{26} → letters must be range 0 - 25

EED

a n q v v

$= 15^{-1} \begin{bmatrix} 4 & -7 \\ -3 & 9 \end{bmatrix}$

15 mod 26

$= 7 \begin{bmatrix} 4 & 19 \\ 23 & 9 \end{bmatrix}$

$= \begin{bmatrix} 25 & 133 \\ 161 & 63 \end{bmatrix}$

$$= \begin{bmatrix} 2 & 3 \\ 5 & 11 \end{bmatrix}$$

Cipher must be even

$$\begin{bmatrix} 2 & 3 \\ 5 & 11 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 11 \end{bmatrix} = \begin{matrix} 3 \longrightarrow D \\ 11 \longrightarrow L \end{matrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 11 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 13 \\ 43 \end{bmatrix} = \begin{matrix} 13 \longrightarrow N \\ 17 \longrightarrow R \end{matrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 11 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 23 \\ 75 \end{bmatrix} = \begin{matrix} 23 \longrightarrow X \\ 23 \longrightarrow X \end{matrix}$$

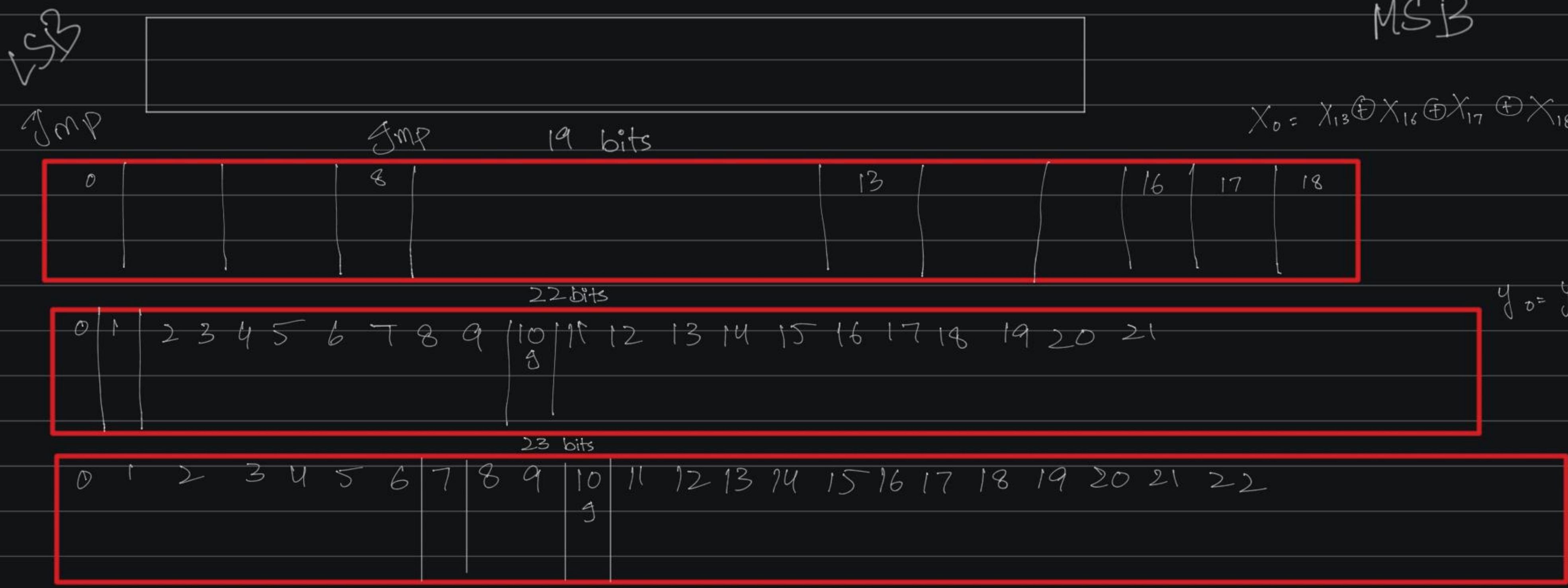
William Stalling Cryptography 8th edition

Tuesday, Feb 13 Lecture

LSFR Left shift feedback register

A5/1

0110 1100



$X_0 = X_{13} \oplus X_{16} \oplus X_{17} \oplus X_{18}$

$y_0 = y_{20} \oplus y_{21}$

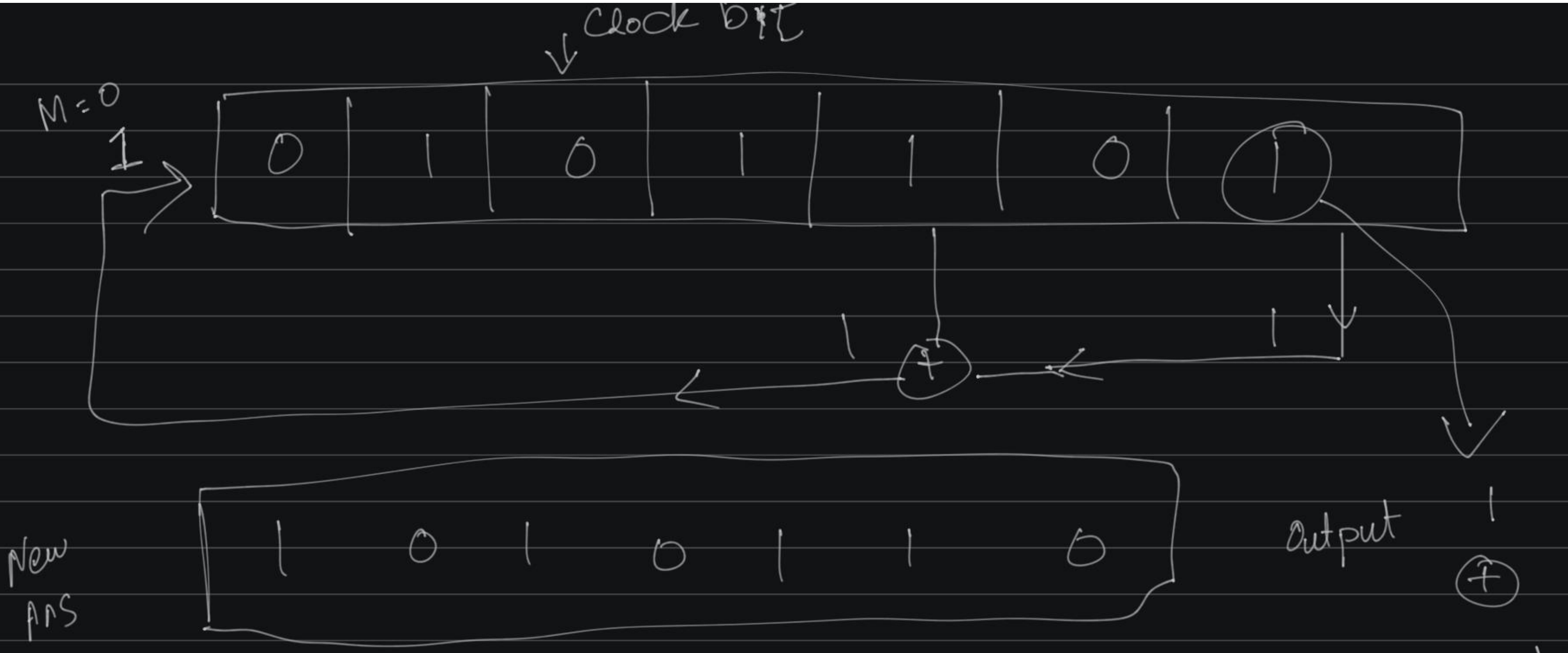
$Z_0 = Z_7 + Z_{20} + Z_{21} + Z_{22}$

$K_i = X_{18} + Y_{21} + Z_{22}$

$\text{Maj}(X_8, y_{10}, Z_{10})$

$\boxed{\text{Maj}(1, 1, 0) = 1} \rightarrow x, y$ will shift

$\boxed{\text{Maj}(1, 0, 0) = 0}$ y, Z will shift



⊕

Output

⊕

Output

⊕

→ 64 cycles → session key

→ 22 cycles → frame number

→ 100 cycles →

16 bytes

~~24~~ bits

~~8~~

Block Cipher DES (Mode of Encryption)

n-bits plaintext → n-bits

$2^4 \times 4$ required key for 4-bit

$2^{10} \times 10$ required key for 10-bit encryption

$n \times 2^n$ $\quad 2^{64} \times 64$ for 64-bit

Fiestal came up with a design

2^k

Confusion and diffusion are two fundamental concepts in cryptography, specifically in the context of block ciphers like DES.

1. Confusion: Confusion refers to the process of making the relationship between the plaintext and the ciphertext as complex and obscure as possible. It involves introducing confusion by using mathematical operations, such as substitution or permutation, to ensure that even a small change in the plaintext results in a significant change in the ciphertext. This makes it difficult for an attacker to deduce any information about the plaintext from the ciphertext.

2. Diffusion: Diffusion refers to the process of spreading the influence of each plaintext bit over a large number of ciphertext bits. It aims to distribute the statistical properties of the plaintext uniformly throughout the ciphertext. Diffusion ensures that any change in the plaintext affects multiple bits in the ciphertext,

making it harder for an attacker to identify patterns or correlations.

Both confusion and diffusion are essential in achieving strong encryption. Confusion helps to hide the relationship between the plaintext and the ciphertext, while diffusion ensures that any changes in the plaintext have a widespread effect on the ciphertext. By combining these two concepts, block ciphers can provide a high level of security and resistance against various cryptographic attacks.

$\boxed{P \to C}$

Diffusion

Any change in plain text should induce a significant change in cipher

$\boxed{K - C}$

Confusion

but with K and C

$D \to P$

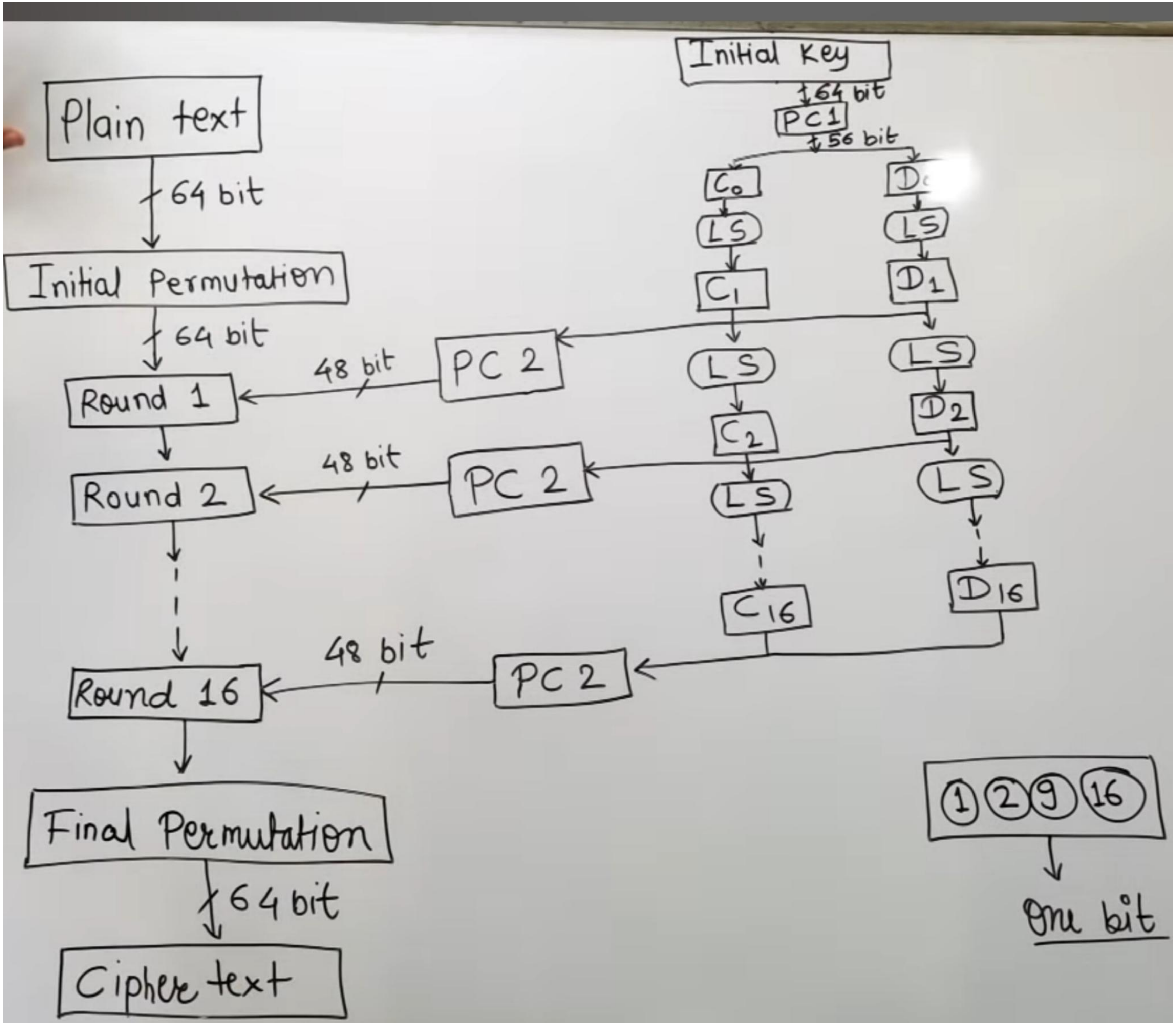
$C \to S$

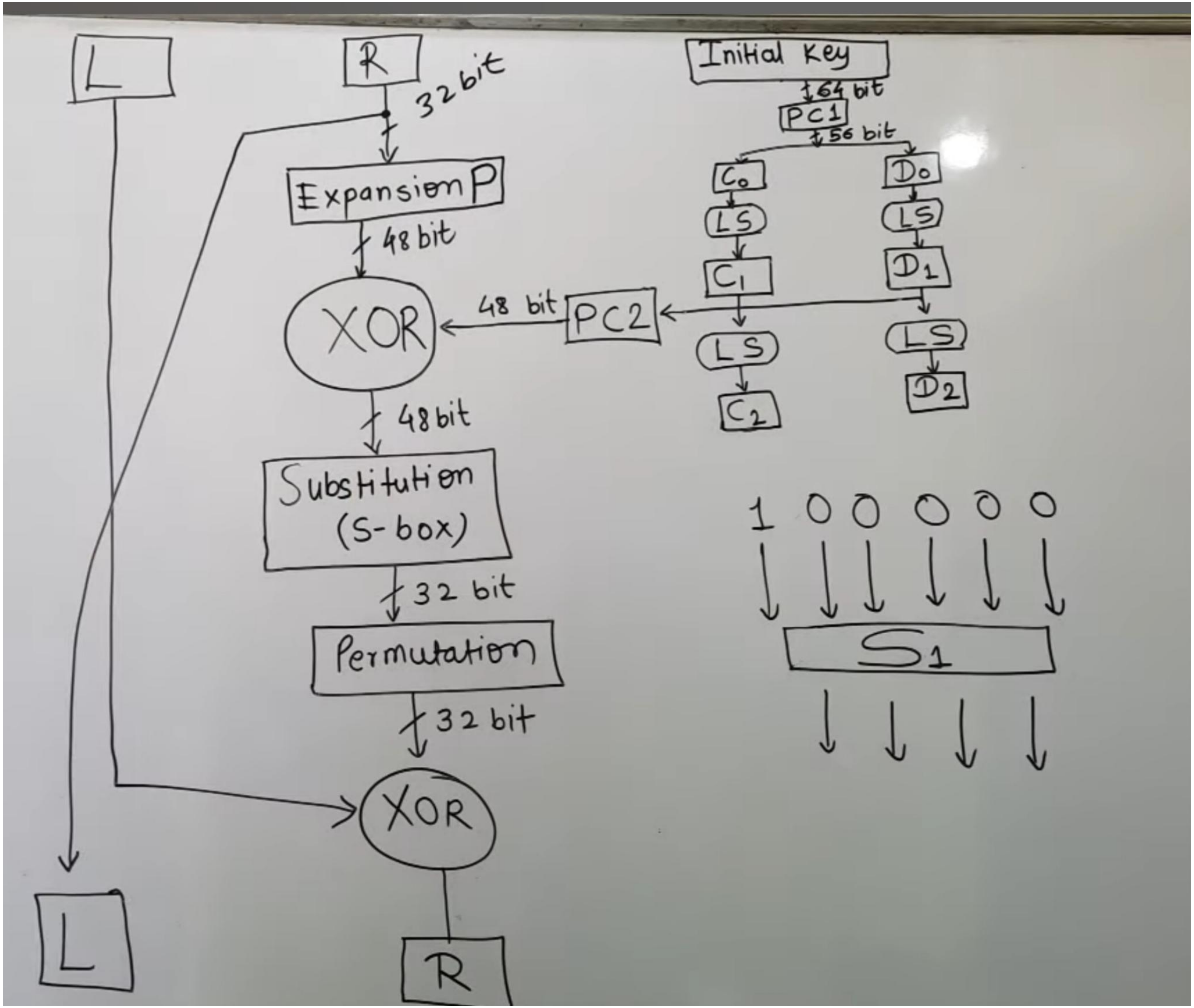
Fiestal Decryption

Just the order of keys is reversed

As for keys, if a key has majority of 0s and minority of 1s the permutation wouldn't change the structure significantly. So you must use substitution

Plaintext cannot be substituted. The substitution boxes would give away things


Initial Key
64 bit
PC1
56 bit
C0
D0
LS
LS
C1
D1
LS
LS
C2
D2
LS
LS
C16
D16
Plain text
64 bit
Initial Permutation
64 bit
Round 1
48 bit
PC 2
Round 2
48 bit
PC 2
Round 16
48 bit
PC 2
Final Permutation
64 bit
Cipher text
1 2 9 16
One bit


L
R
32 bit
Initial Key
64 bit
PC1
56 bit
C0
D0
Expansion P
LS
LS
48 bit
C1
D1
XOR
48 bit
PC2
LS
LS
D2
C2
48 bit
Substitution
(S-box)
1 0 0 0 0 0
32 bit
Permutation
S1
32 bit
XOR
L
R

1977 – 2001 DES Avalanche

birthday Paradox → 99% chance of finding a key from 50% brute force

Fri, Feb 16 Galloa Fields

- Finite Field.

→ $GF(P^n)$

Groups → Rings → Fields → Finite Fields

↳ Abelian Groups

↳ Commutative rings → Integral domains

Group

Generalize all operators

Denoted by { G, ⊙ } Usually addition k operator ko use kya jaata hai.

A group should follow some properties.

Abelian Group defined another property

Rings (Inherit properties of Groups)

→ Ring specified the use of + to groups

also defined multiplicative rules.

[should always have addition property of groups]

Commutative Ring defined another multiplicative

Internal Domain

Fields (inherit A1 – A5 and M1 – M6 from previous)

Defined another M7 property

Types of Fields

Infinite Field

Set of infinite field

Finite Fields

Include finite sets only

For example Galloa Field GF(8)

Only 8 elements

Classical Cipher aren't in Finite Fields / Different maths

$GF(P)$ $GF(P^n)$ → These deal with polynomials.

Additive inverse in modulo 8

$a + b = 0$

$\boxed{1 + 7 \equiv 0}$ Additive inverse

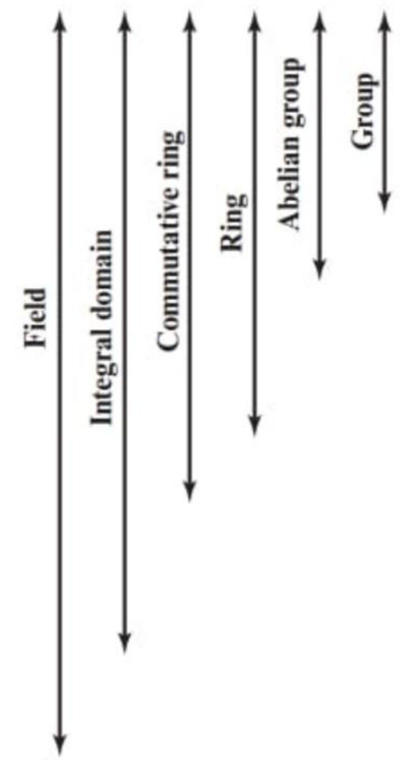
Polynomial Arithmetic:

$GF(p)$ mai co-efficients mod p ho jatay hai

$GF(p^n)$ → coff mod p tak jaye ga

→ coff mod p [highest power mod n]

that we are using ordinary modular arithmetic to define the operations over these fields.



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 5.2 Properties of Groups, Rings, and Fields

$GF(2^3)$ → Coff will always be mod 2 $\boxed{3x^2+x+1}$ wrong

→ x ki power 0, 1, 2 hosakti hai $\boxed{x^2+x+1}$ Valid.

$GF(2^8)$ → AES

$GF(p^n) = (2^3) = 4+6$

Addition in $GF(2^3)$

$$4 = \boxed{\begin{array}{ccc} x^2 & x^1 & x^0 \\ 1 & 0 & 0 \end{array}} \quad \boxed{\begin{array}{ccc} x^2 & x^1 & x^0 \\ 1 & 1 & 0 \end{array}} = 6$$

$(X + X + X) \bmod n =$

$(X + X) \bmod n + x \bmod n$

$\boxed{2 \bmod 2 = 0}$

$$\begin{array}{ccc} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \hline 0 & 1 & 0 \end{array}$$

$\boxed{1+1 = 2 \bmod 2 = 0}$

$$\begin{array}{ll} 111 & = 7 \\ 100 & = 4 \\ \hline 011 & = 3 \end{array} \qquad \begin{array}{ll} 111 & = 7 \\ 101 & = 5 \\ 010 & = 2 \end{array}$$

Multiplication $G(2^8)$

The binary method is only applicable for 2^n not p^n

$F(x) = x^7 + x^5 + x^3$

$G(x) = x^4 + x^2 + x$

$F(x) \times G(x)$

$= x^4(F(x)) + x^2(F(x)) + x(F(x))$

→ $F(X) =$ 1 0 1 0 1 0 0 0

$XF(x) =$ 1 0 1 0 1 0 0 0 0

Left shift results in multiplication

Left shift is multiplaction

if = $\oplus$ xor 00011011

$xF(x) = 01001011$

$x^2F(x) = 10010110$

$x^3F(x) = 00101100$

$\oplus$ 00011011

00110111

$x^4F(x)$ is: 01101110

$x^4 + x^2 + x + 1$

00011011

$x^4F(x) = 01101110$

$x^2F(x) = 10010110$

$xF(x) = 01001011$

Ans = 10110011

Multiplication of two number in $GF(2^8)$

$x^3 + x + 1$

$x(x^2 + 1) + 1$