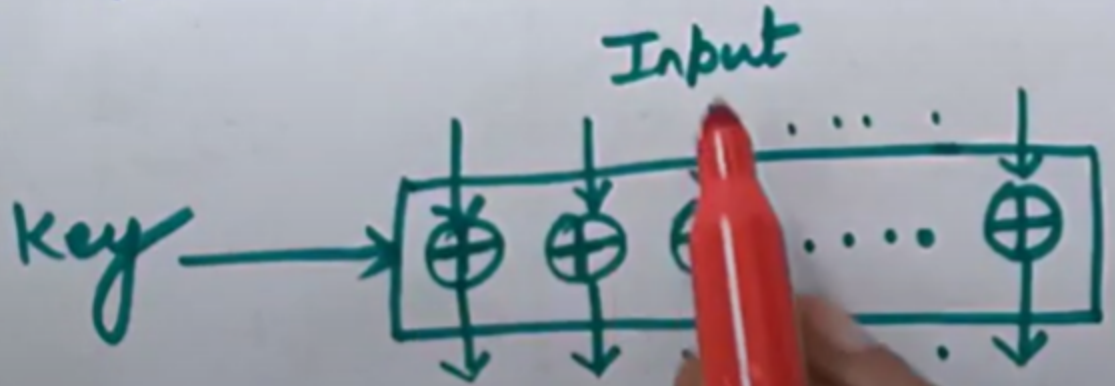
XOR Cipher

- Simple Modern Cipher
- Needs two data inputs - plaintext & key
- uses same key for encryption & decryption
- A string of text can be encrypted by applying bitwise XOR operator to every character using a given key.
- used in complex ciphers.
- it is simple to implement
- XOR operation is computationally inexpensive.

Input


Input
Key

P.T	Key	C.T
0	0	0
0	1	1
1	0	1
1	1	0

plaintext : KIWI 8 bit ASCII

key : 11110011

	K	I	W	I
	01001011	01001001	01010111	01001001
⊕	11110011	11110011	11110011	11110011
	10111000	10111010	10100100	10111010

↳ Encryption

Study Table

C.T

C.T 10111000 10111010 10100100 10111010

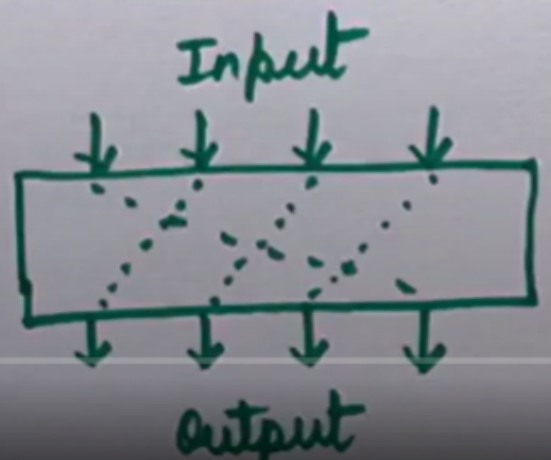
⊕ 11110011 11110011 11110011 11110011

01001011 01001001 01010111 01001001

Plaintext

Rotation Cipher

- Simple modern cipher
- input bits are rotated to the left or right
- can be keyed or keyless
- special case of transpositional cipher using bits instead characters.
- The decryption algo uses the same key and the opposite rotation direction.



Study Table

5:19

left rotation -1

1 0 1 1

0 1 1 1

Right Rotation 3

1 0 1 1

= 0 1 1 1

L rotation 2

1101

0111

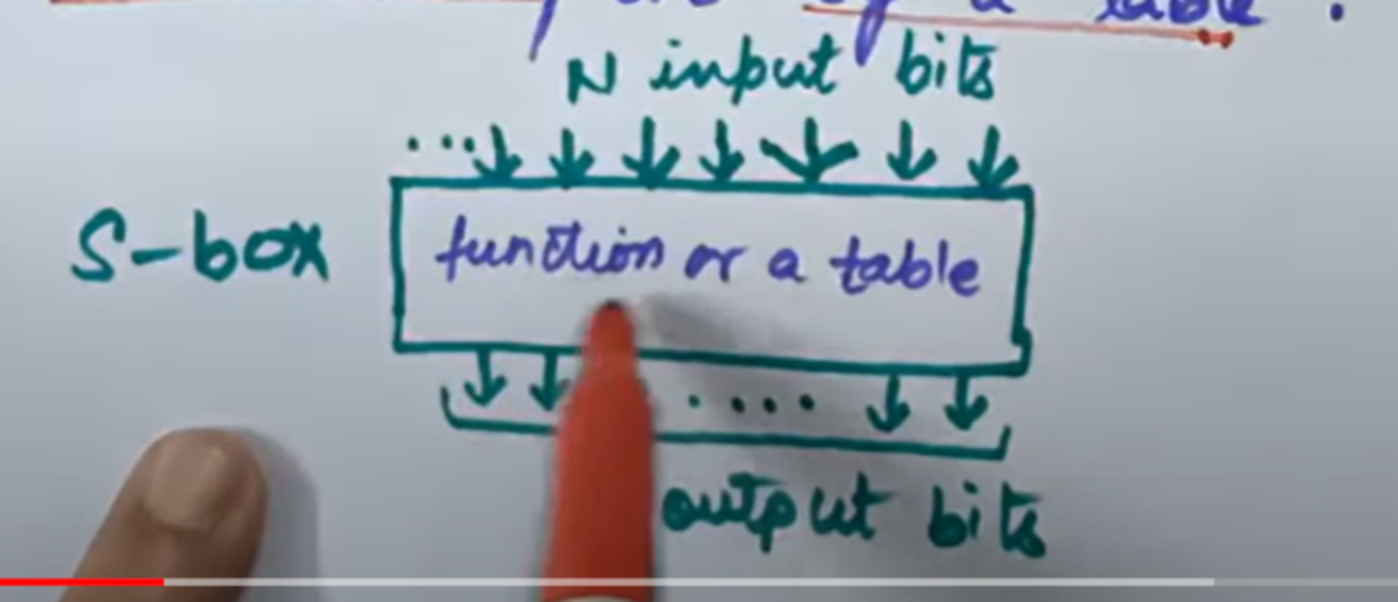
Right rotation 2

0 1 1 1

1 1 0 1

S-box (Substitution box)

- S-box can have different no. of inputs and outputs.
- basic component of symmetric key algorithms which per substitution.
- can be keyed or keyless, but modern block ciphers ~~use~~ normally use keyless
- even small modification to an S-box could significantly weaken DES.
- used as an intermediate stage of encryption or decryption.
- The function that matches the input to the output may be defined mathematically or by a table.

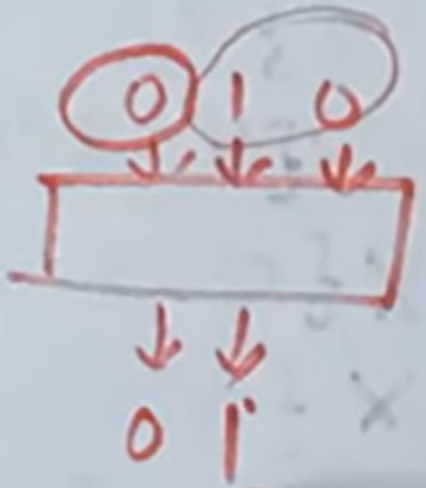

N input bits
S-box
function or a table
output bits

Leftmost bits

	00	01	10	11
0	00	10	01	11
1	10	00	11	01

Rightmost bits

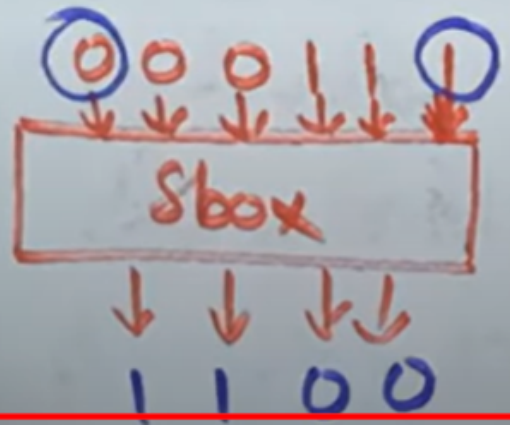
S-box of size 3×2



mapping 6-bit input into a 4-bit output.

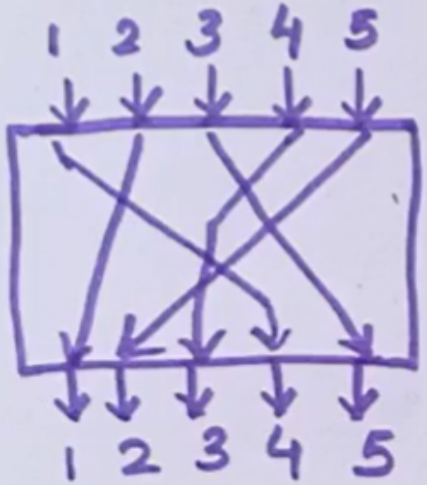
4 Middle bits

outer bits	0000	0001	0010	0011	0100	0101	0110	0111	.....
00	0010	1100	0100	0001	0111	1010	1011	0110	....
01	1110	1011	0010	1100	0100	0111	1101	0001	....
10	0100	0010	0001	1011	1010	1101	0111	1000	....
11	1011	1000	1100	0111	0001	1110	0010	1101	....

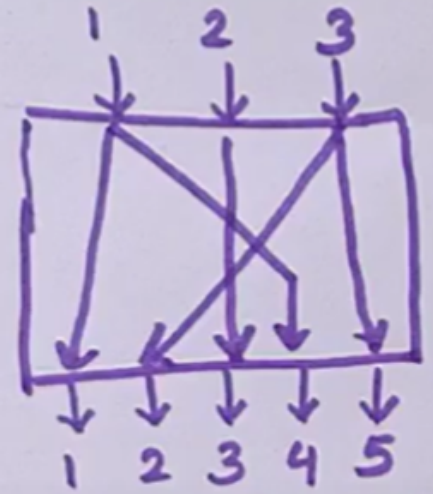


Permutation Box (P- box)

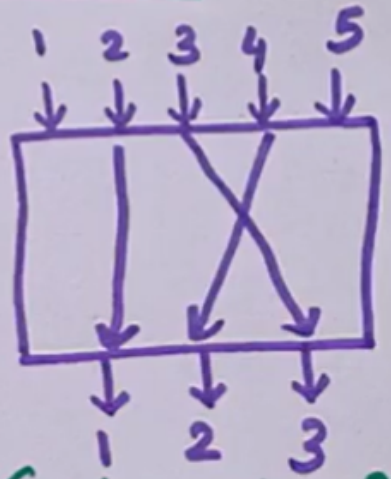
or Transposition Cipher — P-Box



straight Permutation

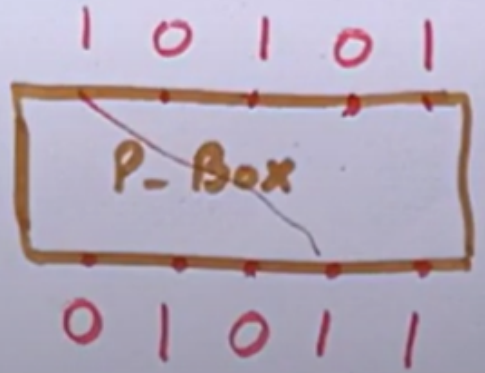


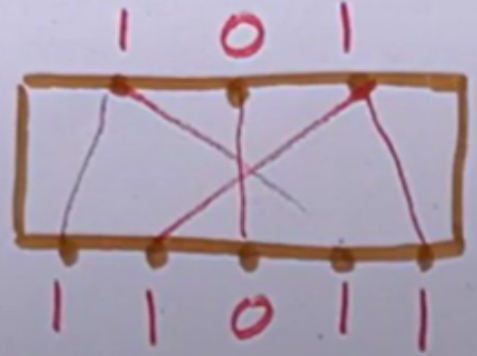
Expansion Permutation

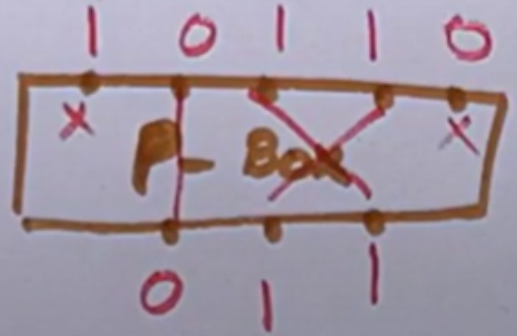


Compression Permutation

Study Table

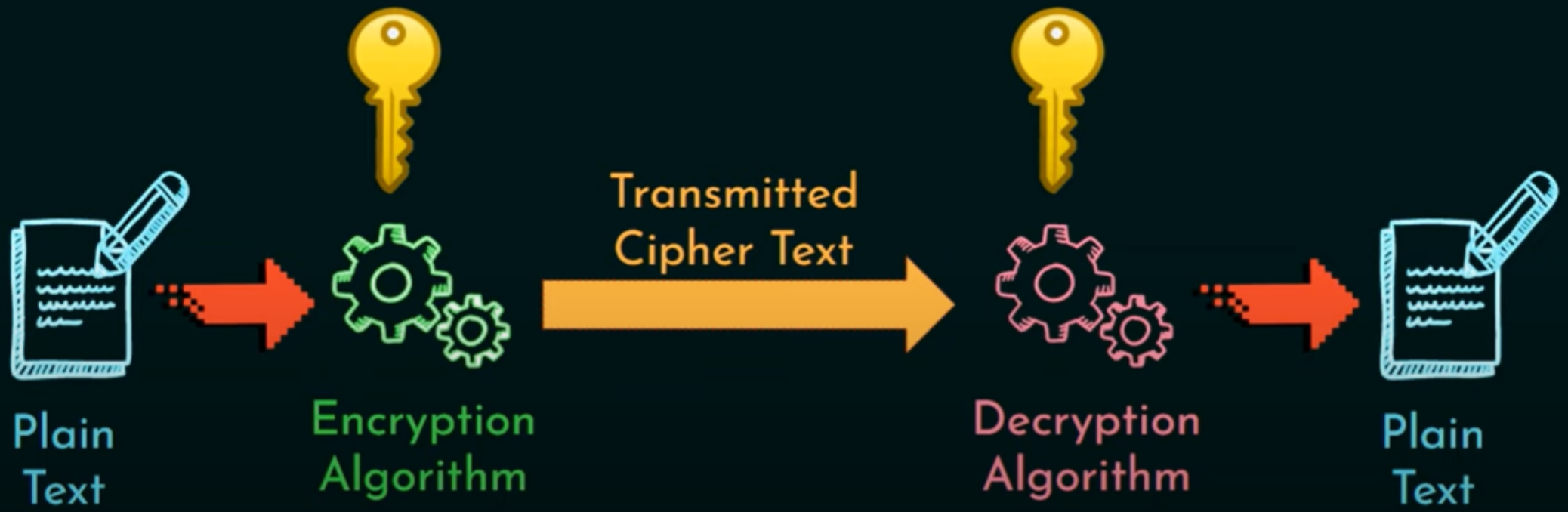

1 0 1 0 1
P-Box
0 1 0 1 1


1 0 1
1 1 0 1 1


1 0 1 1 0
P-Box
0 1 1

Cryptography

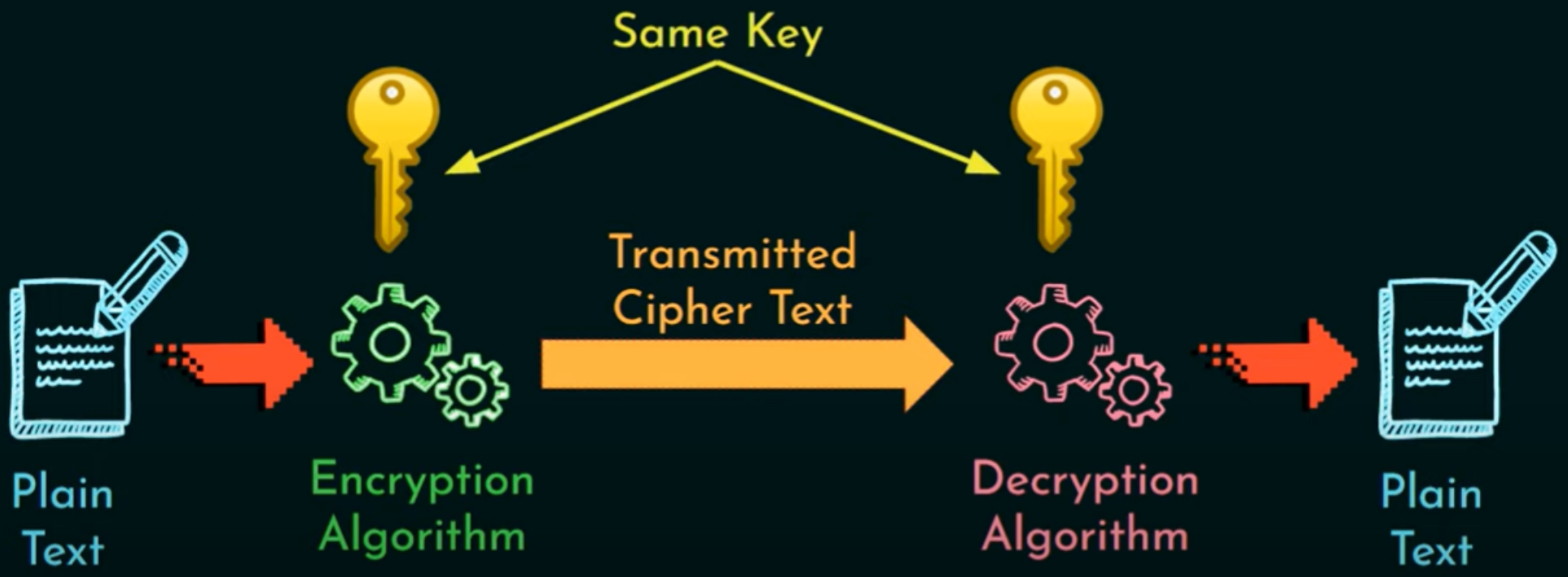
"The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form."



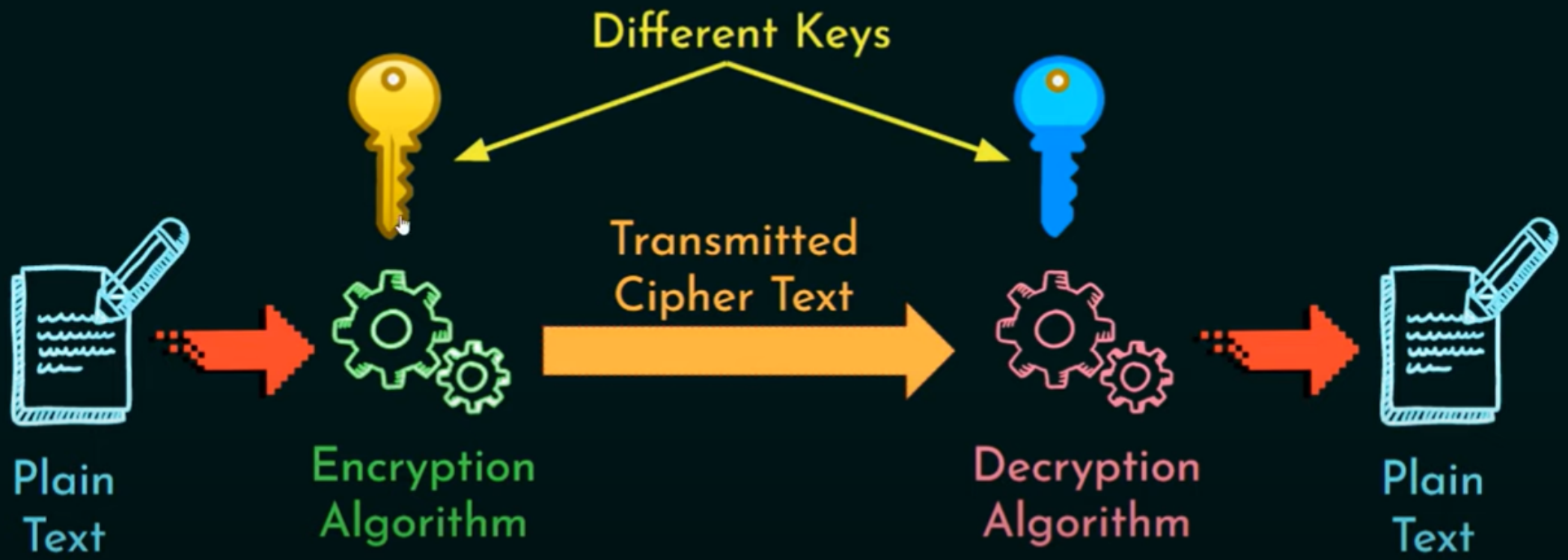
Types of Cryptography

- ★ Symmetric Cryptography (Private Key Cryptography)
- ★ Asymmetric Cryptography (Public Key Cryptography)

Symmetric Cryptography



Asymmetric Cryptography



Encryption schemes

- ★ Unconditionally secure
- ★ Computationally secure

Ciphertext – Plaintext

Ciphertext

2D570755676DFF11E71B6C8511EFE7A7D3B02A3CEE63165050AB5
F4C4D19A4AAB07656A636654C6F39A4AC0FEA2035CCDD7181C0
EBB482A6EBDAEF2AEB35CB5C325CBF0738AEC27D77BEC3938C
590CE77F62CBDCC3EA3D03E06A386BD70BC99A843DD6B7B975
3635C919FA17FC40A3C3DCBD13633D2D56A1A073EA0E73E60C60

Plaintext

Hello World

Algorithm

RSA Algorithm

General approaches

1. Cryptanalysis

2. Brute-force attack

Classical Encryption Technique

Substitution	Transposition
❖ Caesar Cipher	❖ Rail Fence
❖ Monoalphabetic Substitution	❖ Row Column Transposition
❖ Playfair Cipher	
❖ Hill Cipher	
❖ Polyalphabetic Ciphers	
❖ One-Time Pad	

Caesar Cipher

- ★ Letters are replaced by other letters or symbols.
- ★ The earlier known and simplest method used be Julius Caesar.
- ★ Replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Example:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher

Algorithm:

For each plaintext letter 'p', substitute the ciphertext letter 'C':

$C = E(p, k) \bmod 26 = (p + k) \bmod 26$

$p = D(C, k) \bmod 26 = (C - k) \bmod 26$

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher – Pros and Cons

Pros

1. Simple
2. Easy to implement.

Cons

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try. (Vulnerable to Brute-force attack)

Permutation

- ★ A permutation of a finite set of elements 'S' is an ordered sequence of all the elements of 'S', with each element appearing exactly once.
- ★ For example S = { a , b , c }
- ★ There are six permutations of S.

abc
acb
bac
bca
cab
cba

15:58
NESO ACADEMY

Monoalphabetic Cipher

- ★ The "cipher" line can be any permutation of the 26 alphabetic characters.
- ★ This would seem to eliminate brute-force techniques for cryptanalysis.
- ★ A single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.
- ★ English language - Nature of plain text is known.

Monoalphabetic Cipher – Pros and Cons

Pros

1. Better security than Caesar cipher.

Cons

1. Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
2. Prone to guessing attack using the English letter frequency of occurrence of letters.
3. A countermeasure is to provide multiple substitutes, known as homophones, for a single letter.

:58
ESO ACADEMY

Playfair Cipher

- ★ Aka Playfair square or Wheatstone-Playfair cipher.
- ★ Manual symmetric encryption technique.
- ★ The first literal digram substitution cipher.
- ★ Invented in 1854 by Charles Wheatstone.
- ★ Bore the name of Lord Playfair for promoting its use.

Playfair Cipher

- ★ Multiple letter encryption cipher.
- ★ Digrams.
- ★ 5 x 5 matrix constructed using a keyword (Ex: Monarchy)

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

Rules for encryption using Playfair Cipher

1. Digrams.
2. Repeating Letters - Filler letter.
3. Same Column | ↓ | Wrap around.
4. Same row | → | Wrap around.
5. Rectangle | ⇆ | Swap

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

Example

Plaintext: attack

Digrams: at ta ck

Plaintext: neso academy

Digrams: ne so ac ad em yx

Plaintext: balloon

Digrams: ba ll oo n

Digrams: ba lx lo on

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

Understanding the rules

Example 1: attack

Digrams: at ta ck

at	ta	ck
RS	SR	DE

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

Plaintext: attack

Digrams: RSSRDE

Hill Cipher

- ★ Multi-letter cipher.
- ★ Developed by Lester Hill in 1929.
- ★ Encrypts a group of letters : digraph, trigraph or polygraph.

Hill Cipher

- ★ Review few terminologies from linear algebra.
- ★ Concepts to be known:
  - Matrix arithmetic modulo 26.
  - Square matrix.
  - Determinant.
  - Multiplicative inverse.

The Hill Algorithm

This can be expressed as

$$C = E(K,P) = P \times K \bmod 26$$

$$P = D(K,C) = C\,K^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26$$

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

Encryption

$$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$
$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$$
$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$$

Hill Cipher Example

Question: Encrypt "pay more money" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution:

p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

Key = 3 x 3 matrix.

PT = pay mor emo ney

Hill Cipher Example

Encrypting: pay

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (15\ 0\ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (15\text{x}17+0\text{x}21+24\text{x}2 \quad 15\text{x}17+0\text{x}18+24\text{x}2 \quad 15\text{x}5+0\text{x}21+24\text{x}19) \bmod 26$$

$$= (303\ 303\ 531) \bmod 26$$

$$= (17\ 17\ 11)$$

$$= (R\ R\ L)$$

17:38

Hill Cipher Example

Encrypting: mor

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (12\ 14\ 17) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (12\text{x}17+14\text{x}21+17\text{x}2 \quad 12\text{x}17+14\text{x}18+17\text{x}2 \quad 12\text{x}5+14\text{x}21+17\text{x}19) \bmod 26$$

$$= (532\ 490\ 677) \bmod 26$$

$$= (12\ 22\ 1)$$

$$= (M\ W\ B)$$

/ 17:38 O ACADEMY

Hill Cipher Example

Encrypting: emo

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (4\ 12\ 14) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (4\text{x}17+12\text{x}21+14\text{x}2 \quad 4\text{x}17+12\text{x}18+14\text{x}2 \quad 4\text{x}5+12\text{x}21+14\text{x}19) \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (10\ 0\ 18)$$

$$= (K\ A\ S)$$

Hill Cipher Example

Encrypting: ney

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (13\ 4\ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (13\text{x}17+4\text{x}21+24\text{x}2 \quad 13\text{x}17+4\text{x}18+24\text{x}2 \quad 13\text{x}5+4\text{x}21+24\text{x}19) \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (15\ 3\ 7)$$

$$= (P\ D\ H)$$

Hill Cipher Example

PT	p	a	y	m	o	r	e	m	o	n	e	y
CT	R	R	L	M	W	B	K	A	S	P	D	H

Hill Cipher

- ★ Review few terminologies from linear algebra.
- ★ Concepts to be known:
  - Matrix arithmetic modulo 26.
  - Square matrix.
  - Determinant.
  - Adjoint matrix.
  - Multiplicative inverse.

The Hill Algorithm

This can be expressed as

Encryption:

$C = E(K,P) = P \times K \bmod 26$

Decryption:

$P = D(K,C) = C \times K^{-1} \bmod 26$

Decryption requires K^{-1}, the inverse matrix K.

The Hill Algorithm

Decryption requires K^{-1}, the inverse matrix K.

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

To find Det K, Adj K

The Hill Algorithm

To find the determinant of K: $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

$$\text{Det} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{ mod } 26$$

$$= 17(18\text{x}19 - 2\text{x}21) - 17(19\text{x}21 - 2\text{x}21) + 5(2\text{x}21 - 2\text{x}18) \text{ mod } 26$$

$$= 17(342 - 42) - 17(399 - 42) + 5(42 - 36) \text{ mod } 26$$

$$= 17(300) - 17(357) + 5(6) \text{ mod } 26$$

$$= 5100 - 6069 + 30 \text{ mod } 26$$

$$= -939 \text{ mod } 26$$

$$= -3 \text{ mod } 26$$

$$= 23$$

0:02
RO ACADEMY

The Hill Algorithm

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adjoint } K$$

To find Adjoint K

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

30:02
AO ACADEMY

The Hill Algorithm

$$\text{Adj K} = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$\text{Adj K} = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$\text{Adj K} = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$\begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \end{matrix}$$

0:02

The Hill Algorithm

$$= \begin{bmatrix} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{bmatrix}$$

Performing the operation - Column wise

Entering the matrix - Row wise

$$= \begin{matrix} 18\text{x}19-2\text{x}21 & 2\text{x}5-17\text{x}19 & 17\text{x}21-18\text{x}5 \\ 21\text{x}2-19\text{x}21 & 19\text{x}17-5\text{x}2 & 5\text{x}21-21\text{x}17 \\ 21\text{x}2-2\text{x}18 & 2\text{x}17-17\text{x}2 & 17\text{x}18-21\text{x}17 \end{matrix}$$

$$= \begin{matrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{matrix}$$

5 / 30:02

$$= \begin{matrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{matrix} \bmod 26$$

$$\begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix}$$

The Hill Algorithm

Decryption requires K^{-1}, the inverse matrix K.

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

$$K^{-1} = \frac{1}{23} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = \boxed{23^{-1}} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$23^{-1} \times 23 = 1 \bmod 26$	$9 \times 23 = 25 \bmod 26$
$1 \times 23 = 23 \bmod 26$	$10 \times 23 = 22 \bmod 26$
$2 \times 23 = 20 \bmod 26$	$11 \times 23 = 19 \bmod 26$
$3 \times 23 = 17 \bmod 26$	$12 \times 23 = 16 \bmod 26$
$4 \times 23 = 14 \bmod 26$	$13 \times 23 = 13 \bmod 26$
$5 \times 23 = 11 \bmod 26$	$14 \times 23 = 10 \bmod 26$
$6 \times 23 = 8 \bmod 26$	$15 \times 23 = 7 \bmod 26$
$7 \times 23 = 5 \bmod 26$	$16 \times 23 = 4 \bmod 26$
$8 \times 23 = 2 \bmod 26$	$17 \times 23 = 1 \bmod 26$

/ 30:02

$$K^{-1} = \boxed{17} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

The Hill Algorithm

$$K^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

The Hill Algorithm

@nesoacademy
Follow

$$K \times K^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

This is demonstrated as

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

30:02
NESO ACADEMY

Hill Cipher Example

Decrypting: RRL

$$(P_1\ P_2\ P_3) = (R\ R\ L)\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

Decryption

$$(C_1\ C_2\ C_3) = (17\ 17\ 14)\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (17x4+17x15+11x24 \quad 17x9+17x17+11x0 \quad 17x15+17x6+11x17) \bmod 26$$

$$= (587\ 442\ 544) \bmod 26$$

$$= (15\ 0\ 24)$$

$$= (P\ A\ Y)$$

Hill Cipher Example

Decrypting: MWB

$$(P_1\ P_2\ P_3) = (M\ W\ B) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (12\ 22\ 1) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (12x4+22x15+1x24 \quad 12x9+22x17+1x0 \quad 12x15+22x6+1x17) \bmod 26$$

$$= (402\ 482\ 329) \bmod 26$$

$$= (12\ 14\ 17)$$

$$= (M\ O\ R)$$

/ 30:02

Hill Cipher Example

Decrypting: KAS

$$(P_1\ P_2\ P_3) = (K\ A\ S) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (10\ 0\ 18) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (10\text{x}4+0\text{x}15+18\text{x}24 \quad 10\text{x}9+0\text{x}17+18\text{x}0 \quad 10\text{x}15+0\text{x}6+18\text{x}17) \bmod 26$$

$$= (472\ 90\ 456) \bmod 26$$

$$= (4\ 12\ 14)$$

$$= (E\ M\ O)$$

/ 30:02

Hill Cipher Example

Decrypting: PDH

$$(P_1\ P_2\ P_3) = (P\ D\ H) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (15\ 3\ 7) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (15\text{x}4+3\text{x}15+7\text{x}24 \quad 15\text{x}9+3\text{x}17+7\text{x}0 \quad 15\text{x}15+3\text{x}6+7\text{x}17) \bmod 26$$

$$= (273\ 186\ 362) \bmod 26$$

$$= (13\ 4\ 24)$$

$$= (N\ E\ Y)$$

Hill Cipher Example

CT	R	R	L	M	W	B	K	A	S	P	D	H
PT	p	a	y	m	o	r	e	m	o	n	e	y

Polyalphabetic Cipher

- ★ To improve on the simple monoalphabetic technique.
- ★ General name: Polyalphabetic substitution cipher.

Common features

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

Vigenere Cipher

★ It consists of the 26 Caesar ciphers with shifts of 0 through 25.

Encryption process:

$$C_i = (P_i + K_{i \bmod m}) \bmod 26$$

Decryption process:

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

Vigenere Cipher

Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT	25	8	2	21	19	22	16	13	6	17	25	6	21

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT	19	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenere Cipher – Cryptanalysis

- ★ Determining the length of the keyword.
- ★ Key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied.

Autokey system

- ★ The periodic nature of the keyword can be eliminated by using a non-repeating keyword that is as long as the message itself.
- ★ Vigenère proposed autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key.

Example

Key : deceptivewearediscoveredsav

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGKZEIIGASXSTSLVVWLA

Vernam Cipher

- ★ Need of ultimate defense against cryptanalytic attack.
- ★ Length of the keyword = Length of the plaintext.
- ★ No statistical relationship to it.
- ★ AT&T engineer named Gilbert Vernam in 1918.
- ★ His system works on binary bits rather than letter.
- ★ The system can be expressed as follows:

$$C_i = P_i \oplus K_i$$

Vernam Cipher

$$C_i = P_i \oplus K_i$$

where

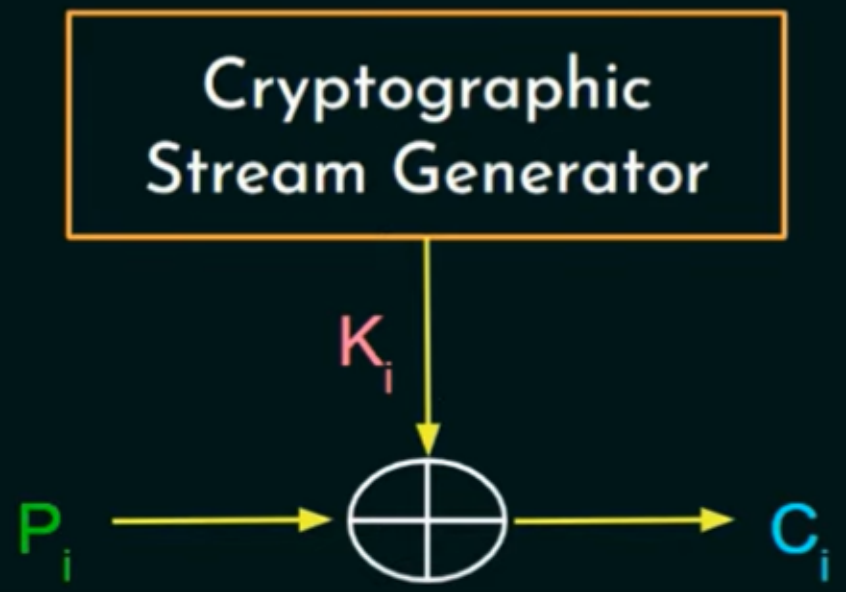
P_i = i^{th} binary of the plaintext.

K_i = i^{th} binary of the key.

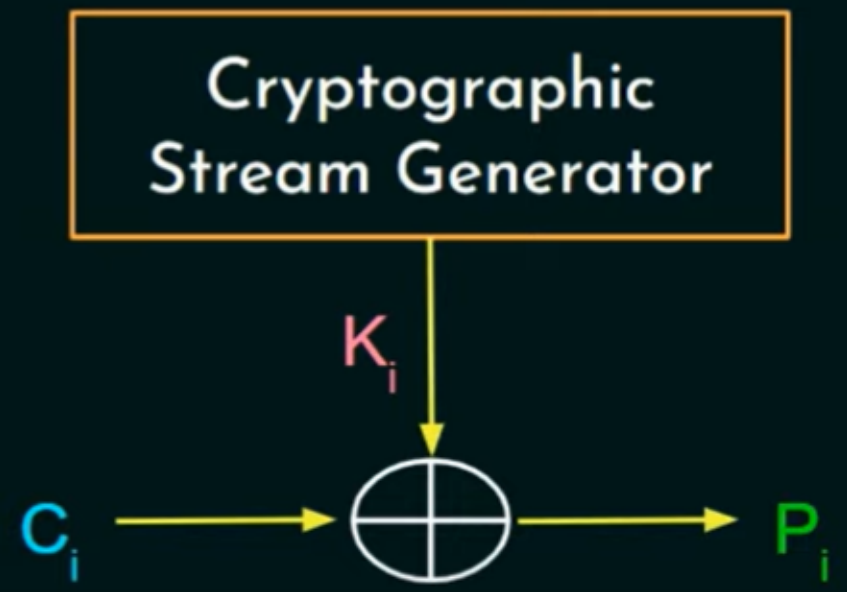
C_i = i^{th} binary of the ciphertext.

$\oplus$ = XOR operation.

Vernam Cipher



Encryption



Decryption

Vernam Cipher – Cryptanalysis

- ★ Construction of the key.
- ★ The use of a running loop of tape that eventually repeated the key.
- ★ The system worked with a very long but repeating keyword.
- ★ This technique can be broken with sufficient ciphertext, the use of known or probable plaintext sequences, or both.

One Time Pad

- ★ Improvement to the Vernam cipher.
- ★ It yields the ultimate in security.
- ★ Random key that is as long as the message.
- ★ The key need not be repeated.
- ★ In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded.
- ★ Each new message requires a new key of the same length as the new message.
- ★ Such a scheme, known as a one-time pad, is unbreakable.

One Time Pad

- ★ It produces random output.
- ★ No statistical relationship to the plaintext.
- ★ Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.
- ★ The code is unbreakable.
- ★ The security of the one-time pad is entirely due to the randomness of the key.

Two Fundamental Difficulties

- ★ The practical problem of making large quantities of random keys.
- ★ Even more daunting is the problem of key distribution and protection.
- ★ Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security.

Perfect Secrecy

★ The one-time pad is the only cryptosystem that exhibits what is referred to as perfect secrecy.

Perfect secrecy is the notion that, given an encrypted message (or ciphertext) from a perfectly secure encryption system (or cipher), absolutely nothing will be revealed about the unencrypted message (or plaintext) by the ciphertext.

Transposition Cipher

- ★ Some sort of permutation applied on the plaintext letters.
- ★ This technique is referred to as a transposition cipher.
- ★ The simplest such cipher is the rail fence.

Rail Fence Technique

★ The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Example:

Encipher the message "neso academy is the best" with a rail fence of depth 2.

Rail Fence Technique

Plaintext : neso academy is the best.

Depth : 2

n		s		a		a		e		y		s		h		b		s	
	e		o		c		d		m		i		t		e		e		t

Ciphertext : NSAAEYSHBSEOCDMITEET

Row Column Transposition

- ★ A more complex scheme.
- ★ Rectangle.
- ★ Write : Row by row.
- ★ Read : Column by column.
- ★ Key : Order of the column

Row Column Transposition

Plaintext : "Kill Corona Virus at twelve am tomorrow"

Key →	4	3	1	2	5	6	7
Plaintext (Input) →	K	i	l	l	c	o	r
	o	n	a	v	i	r	u
	s	a	t	t	w	e	l
	v	e	a	m	t	o	m
	o	r	r	o	w	y	z

Ciphertext : LATARLVTMOINAERKOSVOCIWTWOREOYRULMZ

Row Column Transposition

Plaintext : "Kill Corona Virus at twelve am tomorrow"

Key →	4	3	1	2	5	6	7
Ciphertext (Input) →	L	A	T	A	R	L	V
	T	M	O	I	N	A	E
	R	K	O	S	V	O	C
	I	W	T	W	O	R	E
	O	Y	R	U	L	M	Z

Ciphertext : TOOTRAISWUAMKWYLTRIORNVOLLAORMVECEZ