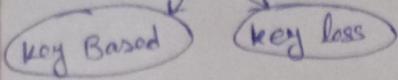


Cryptography

7/01/2025

Cryptography and Network Security



• Security

• Types of Security

- 1) No Security
- 2) ID & Password
- 3) Obscurity

4) Security through encryption

Security Services / Principle of Security

i) Non - Repudiation

(False Identification or you can't denied anything)

ii) Authentication

Role Management (User Specific)

iii) Access Control

Rule Management (Resource)

CIA → Confidentiality Integrity Availability

Various types of security :-

Attack

Two Types :-

Man
in the
middle
Attacks

1) Passive Attacks (Doesn't do any modification of actual msg)

Detection Difficult

2) Active Attacks (modification of actual msg)

Detection easier compare than passive attacks

(Detection → Solution)

Cryptography:

The art / science of achieving security through encryption

method to convert plain text to cipher text
[Easily readable & Understandable] [Non-Meaningful Text]

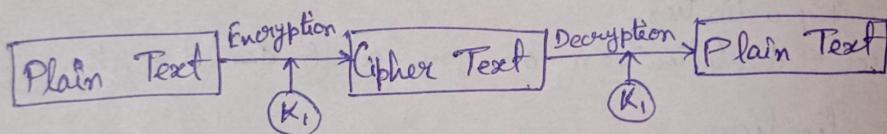
Key

① Symmetric key cryptography
(Private key cryptography)

① Symmetric key

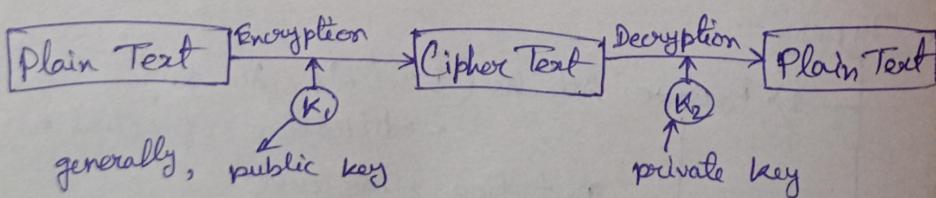
② Asymmetric key cryptography
(public key cryptography)

[used → i) public key
ii) private key]



• one of algorithm

- ① Data Encryption Standard (DES) / DEA → Algorithm
- ② Asymmetric : (public)
(public key + private key)



• Special case → nice-versa

⊕	A	B	C	D	.	.	.	z
	0	1	2	3				25

- ⊗ K ≥ 1, non-negative, K ≤ 25
 $1 \leq K \leq 25$ for ceaser cipher

Ex: HELLO, key = 4

$$e(H) \geq E(H, 4) = (H+4) \bmod 26 \geq (7+4) \bmod 26 \\ \geq 11 \bmod 26 \\ = 11 \\ \Rightarrow L$$

$$\begin{array}{ccc} B & \rightarrow & I \\ L & \rightarrow & P \\ L & \rightarrow & P \\ O & \rightarrow & S \end{array}$$

Cryptography Algorithm is divided into 2 parts

Substitution
+4 / +const

Transposition (changing position
of character)
Key based Key less

④ Hash Code: → Do not use any key
↓ → Uses Hash fn

Message Digest:

Fixed length for var.

MD5

* 1st Algo. ever proposed

Caesar Cipher → Mono alphabetic cipher

C B A S E R
 \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow
 $+3$ $+3$ $+3$ $+3$ $+3$ -3
 F H D N H U

Poly			TH B R E		
H	B	Y	T	H	R
X	A	Y	X	A	Y

Example:

Kampen
Meet me at Two PM, Key = 4

\downarrow \downarrow \downarrow \downarrow

④ Cyclic after 2

Formula: \rightarrow Encryption

$$\text{C} = E(P, K) = (P+K) \bmod 26$$

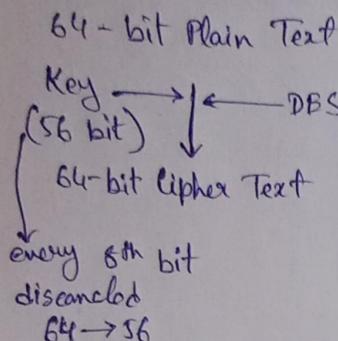
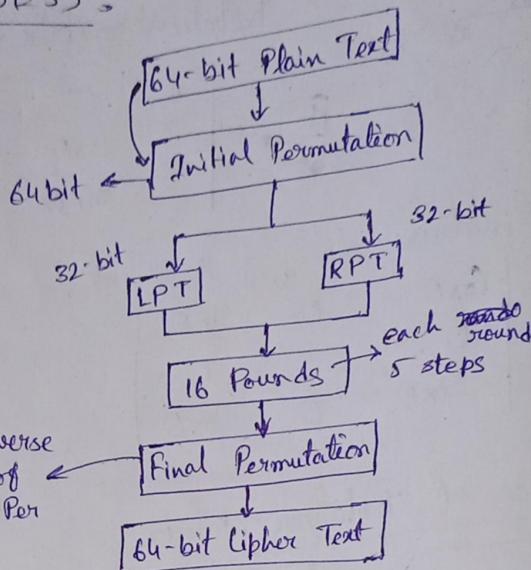
Formula

Cipher

no. of
Alphabet

$$P = D(C, K) = (C - K) \bmod 26.$$

Data Encryption Standard (DES)

Sum - 6

1. Key Transformation
 $[56 \text{ bit} \rightarrow 48 \text{ bit Key}]$
(left circular shift)

2. Expansion Permutation $[32 \text{ bit} \rightarrow 48 \text{ bit}]$

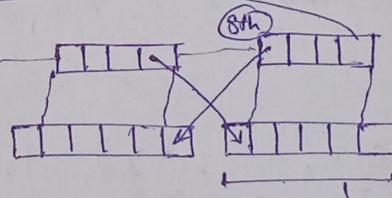
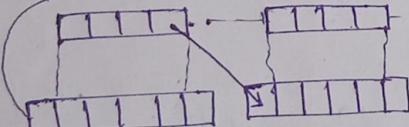
3. S-box

4. P-box

5. XOR and Swap

performed only on RPT

(2)



(3) Substitution Box:

XOR operation of 48 bit (for ①) / and 48 bit (for 2).

Then 48 bit result in S-box.

Final output 32 bit from S-box

8 S-box, 64-bit, matrix/array

0000	0001	0010	0011	0101	1111	
00						
01						
10						
11						

16 Col.

4 rows

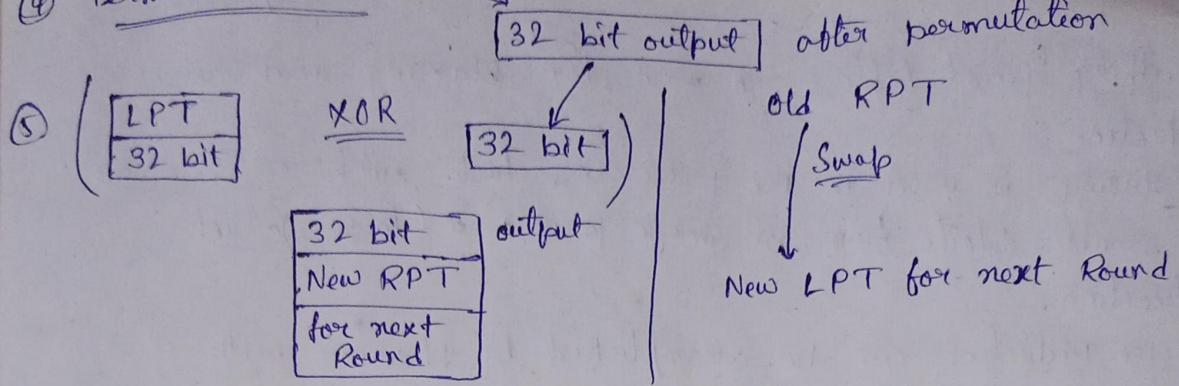
values (0-15) → 4 bit, 1111

col. number
 \downarrow

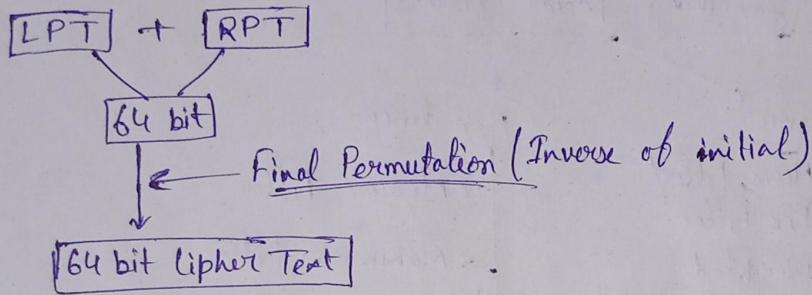
10 → row number
 \downarrow

4 bit × 8 S-box = 32 bit output

④ Permutation Box :



After 16 rounds



Analysis of DES:

1. Avalanche Effect:

A small change in plain text or key should create a significant change in Cipher Text.

2. Completeness Effect:

Each bit of the Cipher Text needs to depend on many bits of the plain Text.

Weakness / Disadvantage of DES

- i Parallel Processing in $< 2^{16}$ nsec
- ii Plain Text $\xrightarrow{\text{Enc.}}$ Cipher Text $\xrightarrow{\text{Enc. Again}}$ Plain Text
4 weak keys. All 0's, All 1's, Half 0's, Half 1's
- iii 6 seems - weak keys
- iv 2¹⁶ possible weak keys
- v 2 diff. plain Text \rightarrow Same Cipher
- vi 2 diff. keys \rightarrow same Cipher Text

Cryptography

7/2/2025



Diffie-Hellman Key Exchange Algorithm:

1. $n, g \rightarrow$ prime numbers

2. Alice, x , $A = g^x \bmod n$

3. Alice send A to Bob.

4. Bob, y , $B = g^y \bmod n$.

5. Bob sends B to Alice.

Large

Prime Number

Alice,
Bob

$$6. \text{ Alice} \rightarrow K_1 = B^x \pmod{n},$$

$$7. \text{ Bob} \rightarrow K_2 = A^y \pmod{n}.$$

Example:

$$1. n=7, g=11$$

$$2. \text{ Alice} \rightarrow A = \frac{7^3}{2} \pmod{7}$$

$$\text{let, } \\ \alpha=3, \gamma=6$$

$$3. \text{ Alice} \rightarrow 2 \rightarrow \text{Bob}$$

$$4. \text{ Bob} \rightarrow B = \frac{7^6}{4} \pmod{11} = 4$$

$$5. \text{ Bob} \rightarrow 4 \rightarrow \text{Alice}$$

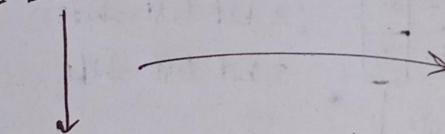
$$6. K_1 = 4^3 \pmod{11} = 9$$

$$7. K_2 = 2^6 \pmod{11} = 9$$

2000
Rijndael
2001

Advanced Encryption Standard (AES):

1 128 bit, plain Text

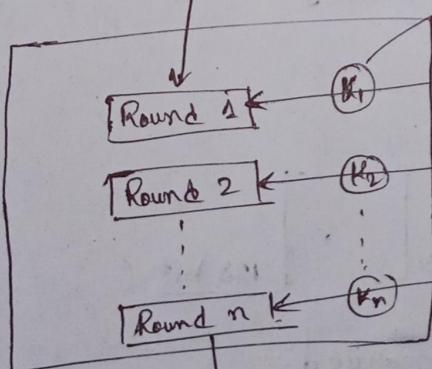


128 bits Cipher Text

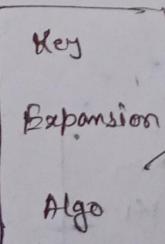
Rounds	Length of Key	
10	128 bits	\rightarrow AES - 128
12	192 bits	\rightarrow AES - 192
14	256 bits	\rightarrow AES - 256

[128 bit Plain Text]

XOR Operation \leftarrow Add Round Key \rightarrow Pre round transformation



→ 4 bytes, Subkey



several subkeys generated from one main key.

[128 bit Cipher Text]

No. of Rounds:

- ① For 128,
- No. of Round + 1

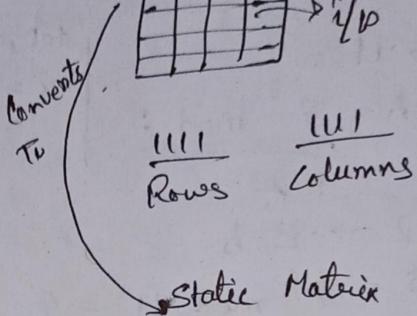
$$\begin{aligned} &= 10 + 1 \\ &= 11 \text{ subkeys} \\ &[0 \text{ to } 10] \end{aligned} \quad \begin{array}{l|l} 4 \times 11 & 44 \text{ bytes} \\ 44 \text{ bytes} & \text{subkeys} \end{array}$$

Steps:

1. Substitution Bytes.
2. Shift Rows.
3. Mix Columns
4. Add Round Key

4 words

(Hexadecimal values)



Step 1

ABS \rightarrow S-box

16×16

Step 2

Shift Rows

1	2	3D	S1
0	1	F	C
7	8	A	B
A	F	D	8

1	2	3D	S1
1	F	C	0
A	B	7	8
8	A	F	D

Left Shift

0 shift

1 shift

2 bit left shift

3 bit left shift

IP

Mix Columns:

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

(4×1)

Stats Matrix

(4×1)

Step 4

Add Round Key

$$\begin{bmatrix} \quad \end{bmatrix}_{4 \times 4} \times \begin{bmatrix} \text{Key} \\ K_1 \end{bmatrix}_{4 \times 1} = \begin{bmatrix} \quad \end{bmatrix}_{4 \times 1} \quad \underline{128 \text{ bit}}$$

④ In last round, 1 step is discarded.
 (mix col)

11/2/25

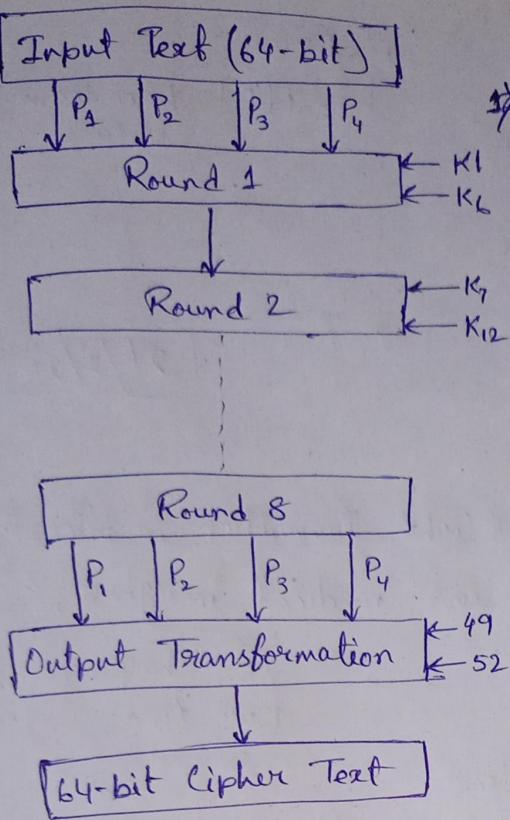
Cryptography

AES (4-steps)

International Data Encryption Algorithm (IDEA)

Plain Text (64 bits)

- Rounds = 8
- Keys = 128
- 6 - Subkeys
- 14 - steps are present



14-Steps

- 1) Multiply P_1 and K_1
- 2) Add P_2 and K_2
- 3) Add P_3 and K_3
- 4) Multiply P_4 and K_4
- 5) XOR 1 and 3
- 6) XOR 2 and 4
- 7) Multiply Step 5 and K_5
- 8) Add Step 6 and Step 7
- 9) Multiply Step 8 and K_6
- 10) Add Step 7 and Step 9
- 11) XOR Step 1 and Step 9
- 12) XOR Step 3 and Step 9
- 13) XOR Step 2 and Step 10
- 14) XOR Step 4 and Step 10

12-Rounds Rivest Cipher - 5 (RC-5)

Rounds $\rightarrow 0 - 255$

Keys $\rightarrow 0 - 255$
8-bits

2-word ip $\rightarrow 16, 32, 64$

1) Divide the Plain Text into two parts (Equal)

2) Add A and $S[1] \rightarrow C$

3) Add B and $S[2] \rightarrow D$

4) XOR C and D $\rightarrow E$

5) Circular Left Shift E by D bits

6) Add E with $S[2-i] \rightarrow F$

7) XOR E and F $\rightarrow G$

8) Circular Left Shift G by F bits

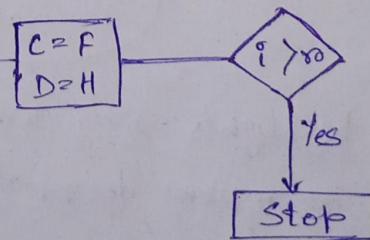
9) Add G with $S[2+i]$

Roger Rivest

proposed that technique

3-Steps

- 1) XOR
- 2) CLS (Circular Left Shift)
- 3) Add with the key



H.W.

Take one Binary Number & Solve

Blow Fish :-

Key Size \rightarrow 32 to 448 bits

Plain Text \rightarrow 64 - bits

Sub Keys \rightarrow 18

S-box \rightarrow 4

(256 bits)

P-Array

$\hookrightarrow P[0]$ \Rightarrow hexa decimal values

Cryptography

Date : 14/2/2025

1) Encrypt the following plain text using ceaser cipher:

Plain Text : ~~All the Best~~ ALL THE BEST

Key : 4

2) Encrypt the plain text "HOW ARE YOU" using key "NCBTQZARG" by the substitution technique called Vernam Cipher.

3) Transform the below mentioned plaintext into cipher text using the key "COLLEGEB" by using play fair cipher.

Plain Text : STUDENTS ARE PLAYING FOOTBALL

Answers

1) Encryption:

$$E(A) + K = 4 \rightarrow E$$

$$E(L) + K = 4 \rightarrow P$$

$$E(T) + K = 4 \rightarrow X$$

$$E(H) + K = 4 \rightarrow L$$

$$E(E) + K \rightarrow I$$

$$E(B) + K \rightarrow F$$

$$E(S) + K \rightarrow W$$

∴ Cipher Text = BPP XLI FIWX

2)		A → D.		
7	14 22	0 17 4	24 14 20	
H O W		A R E	Y O U	
N C B		T Q Z	A R G	
13 21		19 16 25	0 17 6	
20 16 23	19 33 29	24 31 26		
U Q X	T / H / D	Y (F A		
	33%26=7	29%26=3	26%26=0	
			34%26=5	

35

COLLEGE

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

S T U D E N T S
T T T T
T: T U S H E T U

A R B P L A Y I N G
T T T T
B Q G N C D V N P E

F O O T B A L L
T T T
B B R B B D D
L D D 2

Cryptography

21/02/2025

Symmetric

- (i) This is also known as private key or secret key cryptography.

- (ii) Only one key is used for both encryption and decryption.

Asymmetric

- (i) This is also known as public key cryptography.

- (ii) Two different keys (public key and private key) are used for encryption and decryption respectively.

Symmetric

- (iii) This is faster in execution.
- (iv) It is less complex and less computational power is required.
- (v) It is used for the transfer of bulk data (because it executes faster).
- (vi) Sharing the key between sender and receiver is not safe.
- (vii) Commonly used algorithms are DES, AES, RC5, 2DES, 3DBS etc.

Asymmetric

- (iii) This is slower in execution.
- (iv) It is more complex and more computational power is needed.
- (v) It is used for secretly exchanging the secret key.
- (vi) No problem of key sharing because of private key concept.
- (vii) Commonly used algorithms are RSA, DSA etc.

Digital Signal Algorithm

DES Algorithm DES Analysis

Q) Avalanche Effect

- (i) Avalanche Effect —
 - A small change in plain text or the key should create a significant change in cipher text.

(ii) Completeness Effect —

- Each bits of the cipher text needs to depend many bits of the plain text.

Weakness of DES :-

- (i) Key Size : In DES 56 bits keys are required for encryption. Hence a total of 2^{56} combinations can be made out of these 56 bits keys. In today's parallel processing, it is very easy to crack the actual key.

(ii) Weak Keys: There are 4 weak keys. These are -

- (a) All 0's, (b) All 1's, (c) Half 0's, (d) Half 1's

(iii) Semi Weak Keys: 6 pairs of keys are called semi-weak keys.

(iv) Possible Weak Keys: There are 48 possible weak keys out of 2^{56} combinations.

(v) Key Clustering: It means that 2 or more keys can create the same cipher text from the plain text.

(vi) Weakerness in Cipher Design: Two specifically chosen input to X-box array can create same output.

Imp. Questions:-

- ① Types of Adapt
- ② What is security, types,
- ③ Virus, Worm, Trojan Horse
- ④ Hill Cipher

Book:

ATUL RAHATE
CRYPTOGRAPHY
Text Book

Transposition

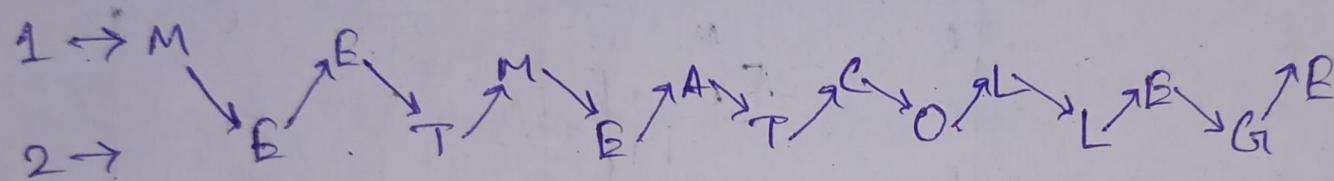
Cryptography

Rail Fence Technique (Keyless Transposition)

Plain Text \rightarrow MEET ME AT COLLEGE

No. of rows = 2. (by default) (fixed)

No. of columns depends upon the length of the input text.



Cipher Text \rightarrow MEMALLBEBETETBTOLG
(non-spaces)

Row Transposition / Simple Columnar Technique :-

(Keyed Transposition)

PT \rightarrow MEET ME AT COLLEGE

Key \rightarrow Integer (Ex - 41235, 52134)

CRYPTO (Here the alphabet)

1 4 6 3 5 2

1	4	6	3	5	2
M	B	E	T	M	B
A	T	L	O	L	L
E	G	E	X	Y	Z

Write \rightarrow Row
Read \rightarrow Column

Dummy bits | Bogus Characters

Cipher Text \rightarrow

MAEELZTOXETGMLYEC

Double Columnar Technique

Step - 1

PT \rightarrow MEET ME AT COLLEGIE

key \rightarrow CRYPTO
1 2

4. Keyed Transposition —

PT \rightarrow ATTACK POSTPONED UNTIL TONIGHT

key \rightarrow 4 3 15 2 * *
 ↓ ↓ ↓ ↓ ↓ Input Text Length = Key length
 1 2 3 4 5

Input \rightarrow ATTAC KPOSTPONED UNTIL TONIGHTXYZ
 \Rightarrow ATACT SOKIP BNPD0 ITULN INTGOYXHZT

Input Text's 4th character will be 1st character of the cipher text.

Cipher Text \rightarrow ATACTSOKTPENPD0ITULNINTGOYXHZT

Substitution Method

Vernam Cipher —

Plain Text \rightarrow HOW ARE YOU

Keysize = Input size

key \rightarrow NCBTZ & ARX

Encryption

PT \rightarrow H O W A R E Y O U
7 14 22 0 17 4 24 14 20

key \rightarrow N C B T Z & A R X
13 2 1 19 25 16 0 17 23

Add \rightarrow 20 16 23 19 42 20 24 31 43

Subtract 26 from \rightarrow U Q X T Q U Y F R
those which is ≥ 26

Cipher Text \rightarrow UQXTQUYFR

Decryption (CT as PT)

PT → U Q X T Q U Y R R
 20 16 23 19 18 20 24 5 17

Key → N C B T Z Q A R X
 13 2 1 19 25 16 0 17 23

subtract → 7 14 22 0 -9 4 24 -12 -6

Add 26 → 7 14 22 0 17 4 24 14 20
 with those H O W A R E Y O U

which is < 0
*** Playfair Cipher** — (I & J are considered as a single character) 5×5 matrix

PT → SISTER NIVEDITA UNIVERSITY

Key → CRYPTOGRAPHY

- whatever input text is given, we have to change it as a pair i.e. 2.
- Onech can be filled in the matrix as 1 time.
- After writing the key in the matrix we have to write the other 26 alphabet.

PT → SI ST ER NI NB DI TA UN IN

ER SI TY

* same row to 26th ch 26th char
 char replaced 27th immediate next ch
 Ex, Ex → AB → HO

T	A	L	L
T	A	L	X
I	→	T	Z

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

* same column 26th, 27th
 char replace 28th immediate next down ch
 Ex, Ex → FW → NY

if not same col = / same row →
 diagonally form a sub matrix
 First ch → same row → 2nd ch →
 corresponding 26th 27th,
 28th 29th 30th replace 26th,
 Ex → NZ → SW

SI ST ER NI NE DI TA UN IN ER SI TY QK
ZB MG BF RM BK YB WL BX MG ZB CP

Cipher Text → QKZBMGQFRMEKYBWLEXMGZBCLP

H/W PT → NETWORK SECURITY

Key → SOFTWARE