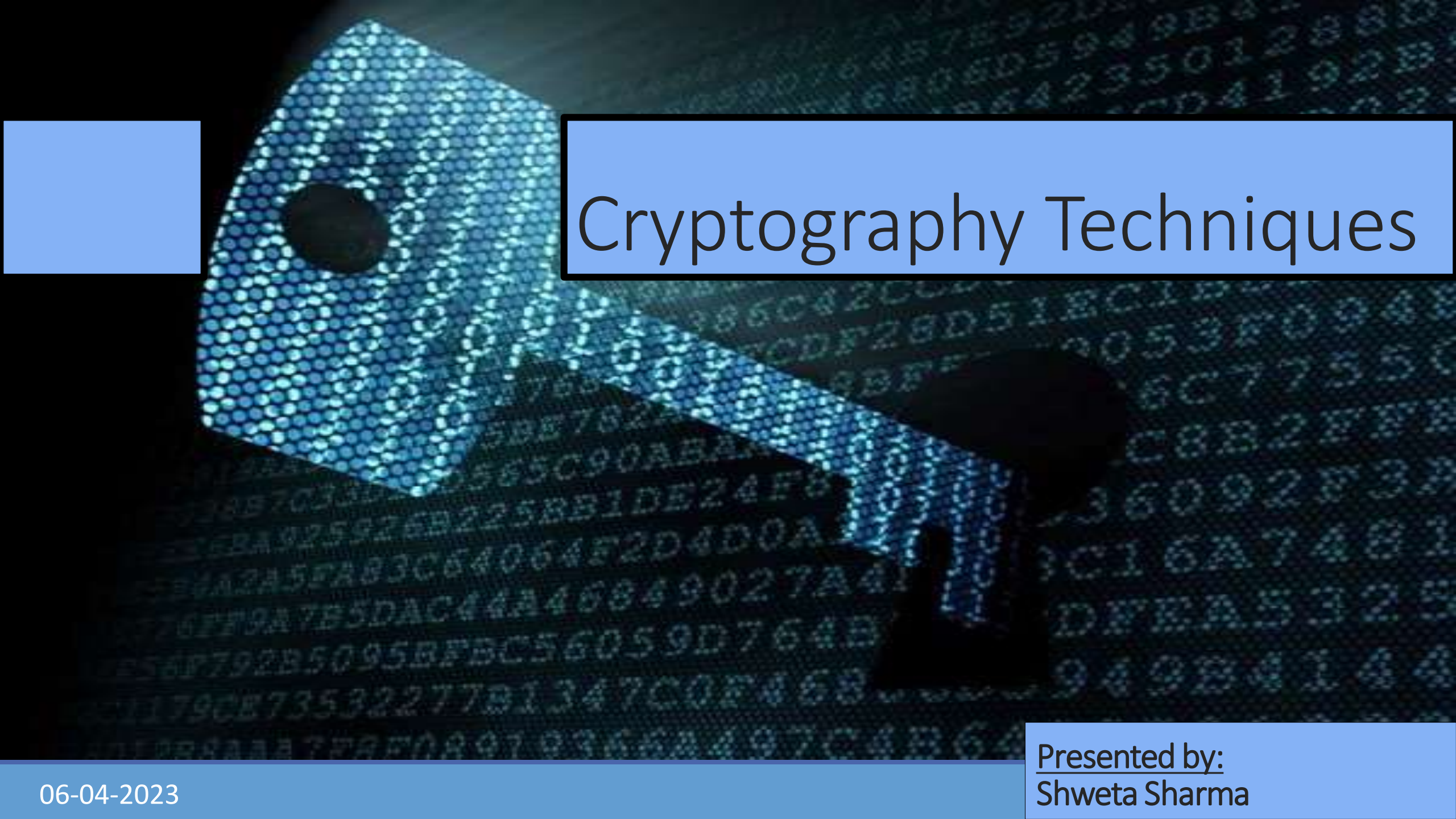


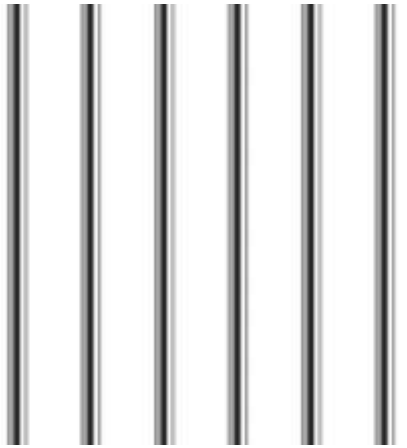
Cryptography Techniques

Presented by:
Shweta Sharma

06-04-2023

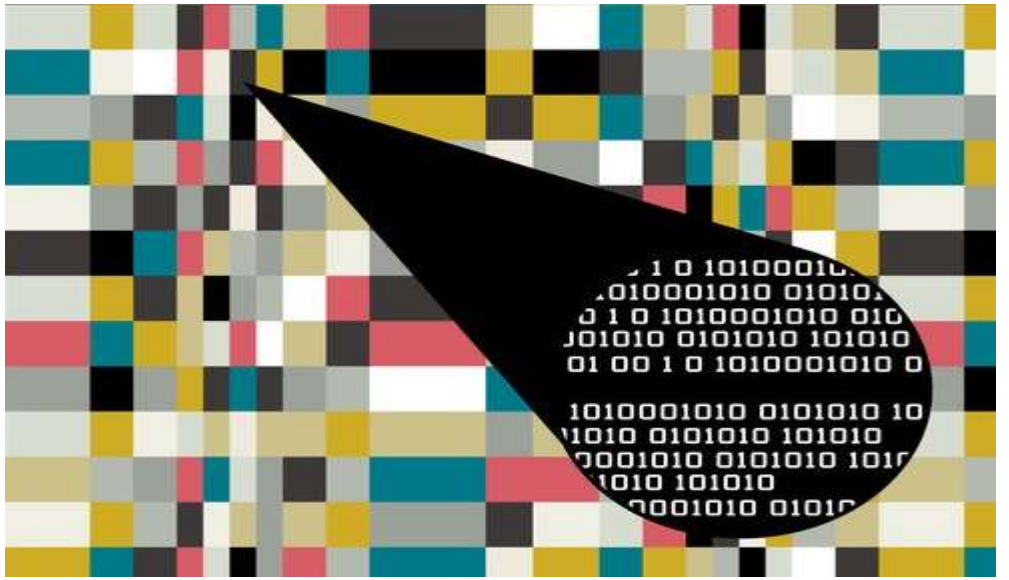
Contents

1. History of secret communication



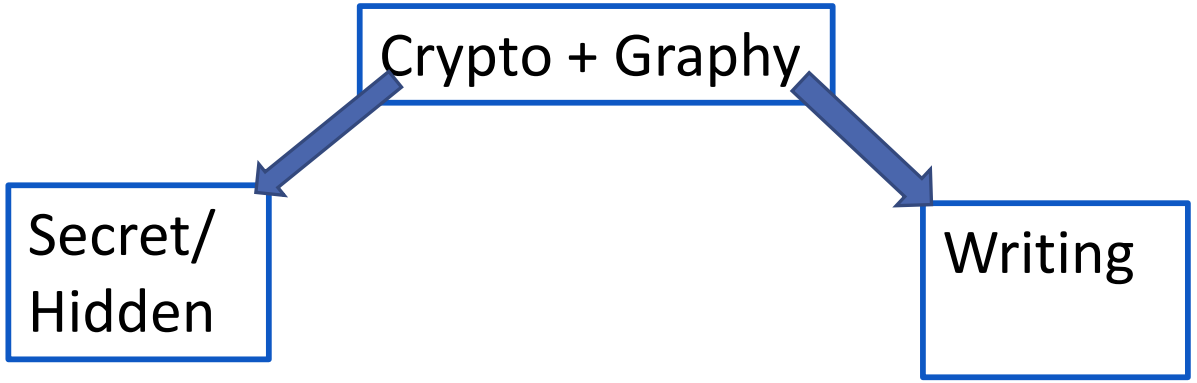
1. History of secret communication

- Steganography
- Secret communication is achieved by hiding the existence of a message.



- Steganography suffers from a serious weakness: If the messenger is searched and the hidden message is discovered, its contents are revealed at once.

2. Cryptography

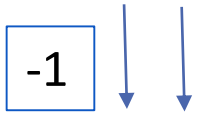


- Cryptography deals with the actual securing of information. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services.
- It is not an attempt to hide the existence of the message.

2. Cryptography

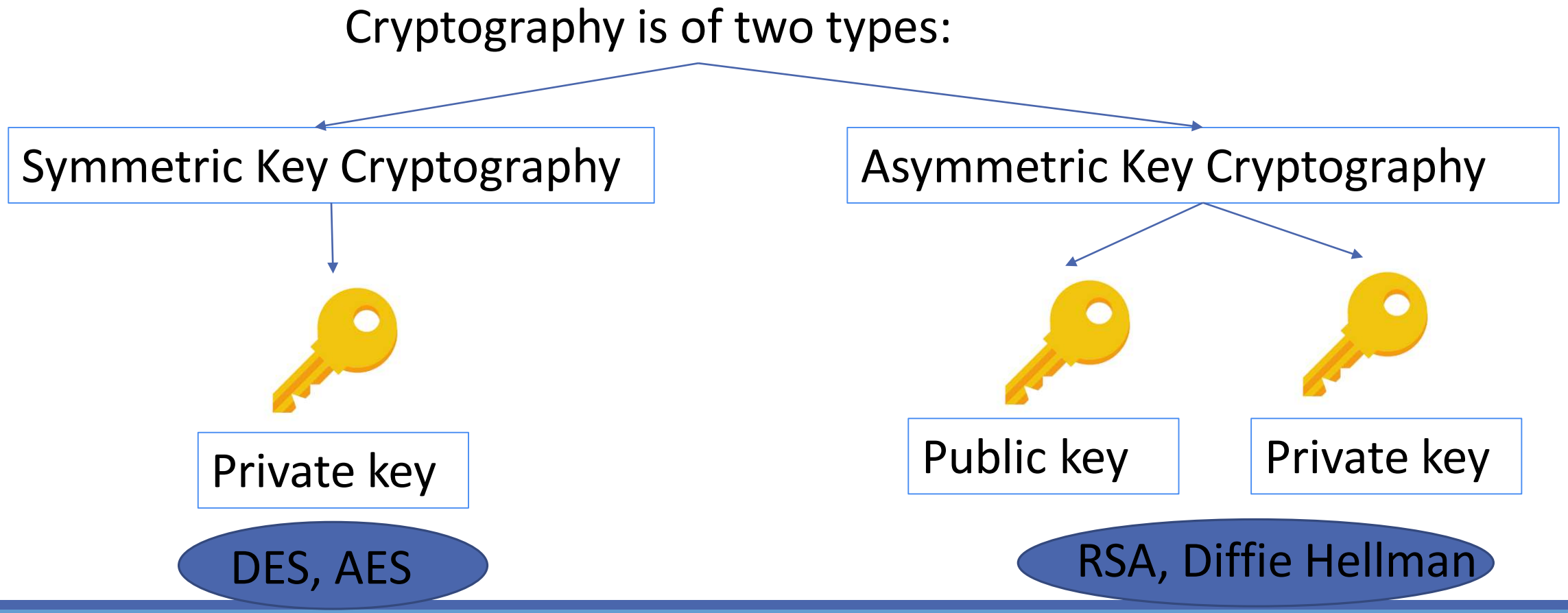
- Cryptography hides the meaning of a message by a process known as encryption.

Example: meet me after party



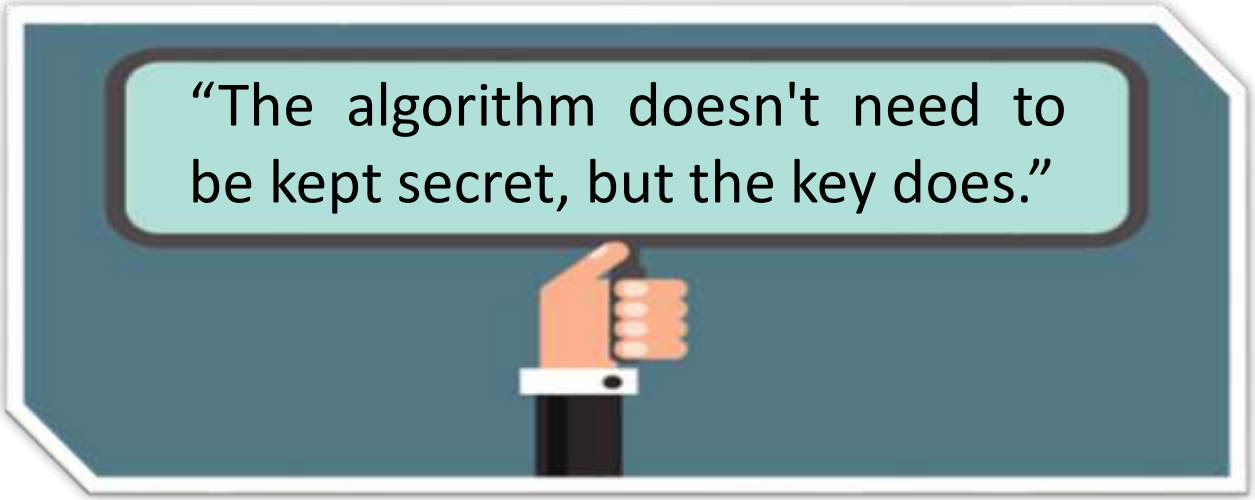
ldds ld zesdq ozqsx

2. Cryptography



3. Private Key

- A private key (secret key) is an input to the encryption algorithm. The key is a value independent of the plain text and of the algorithm.
- A secret key is agreed between the sender and the receiver. The receiver can reverse the converted message by using the secret key to make it comprehensible.



4. Private Key Cryptography

- Plain text
- Encryption algorithm
- Private key
- Cipher text
- Decryption algorithm

4. Private Key Cryptography

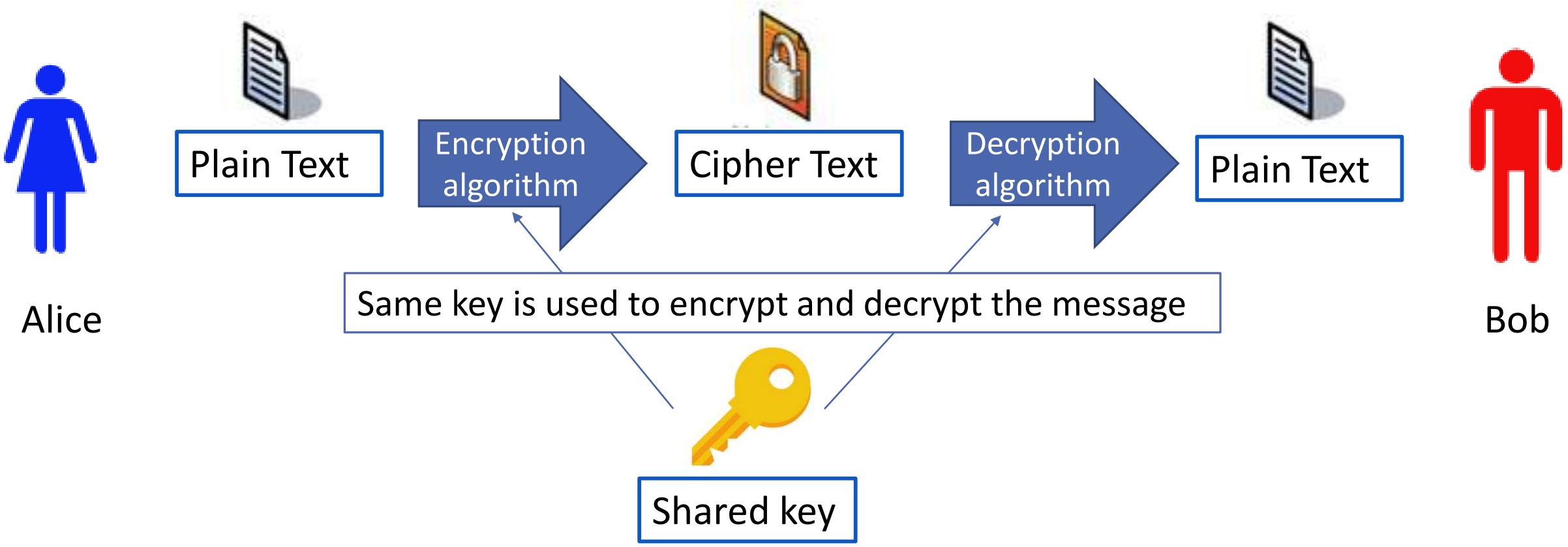
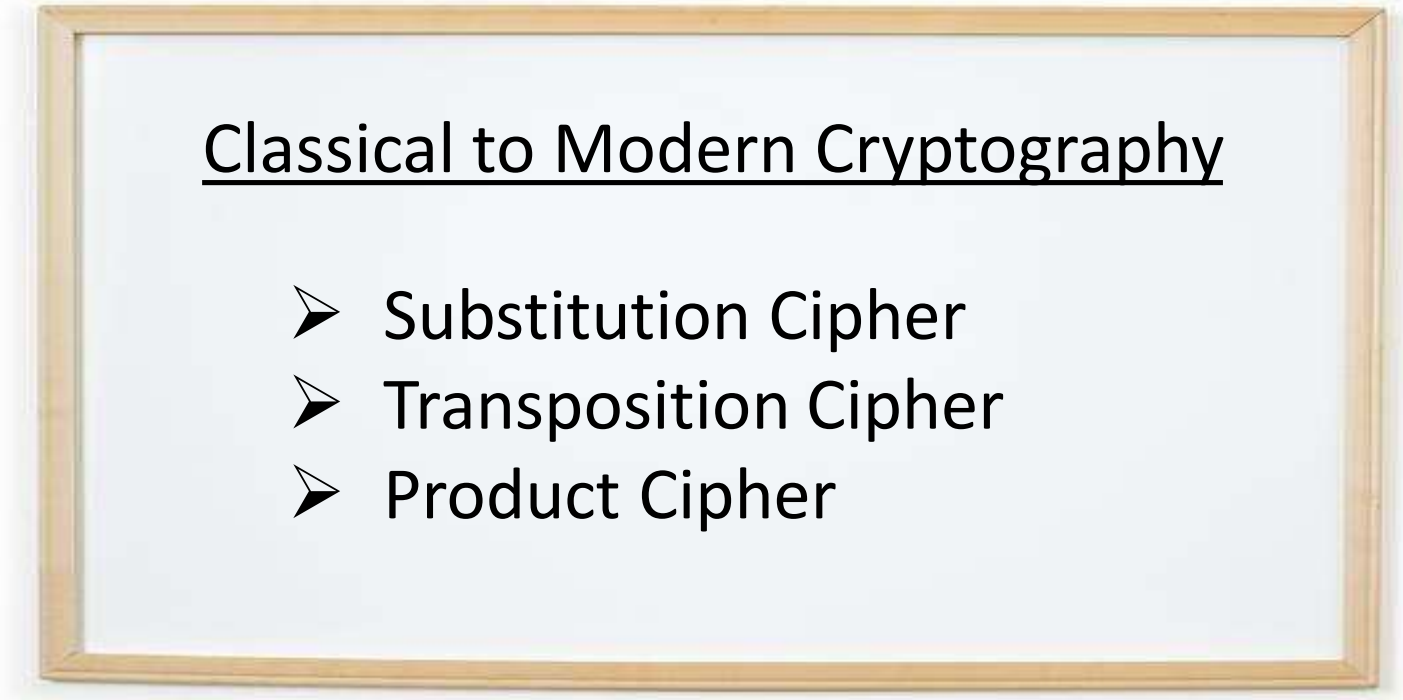


Figure 1 Symmetric key cryptographic system

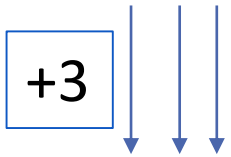
4. Private Key Cryptography



4.1 Caesar Cipher

- Substitution cipher by Julius Caesar
- Each letter is replaced by the letter three positions further down the alphabet.

Example: meet me after party



phhw ph diwhu sduwb

4.1 Caesar Cipher

Mathematically- Assign a numerical equivalent to each letter.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Algorithm:

c=E(p)
=(p+k)mod 26

p=D(c)
=(c-k)mod 26

E→ Encryption
D→ Decryption
p→ plain text
k→ key
c→ cipher text

Example->

p=**a**
(0+3)mod 26
3=**d**

(3-3)mod 26
0=**a**

4.1.1 Cryptanalysis of Caesar Cipher

Advantage: Easy to use

Disadvantage: Easy to break

- Brute force search
- Given cipher text, just try all shifts of letters

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Exercise

Q 1: Encode: hello tom (Shift+3)

⇒khoor wrp

Q 2: Decode: adiy evhzn wjiy (shift+21)

=> find james bond

4.2 Monoalphabetic Ciphers

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

Plain Text: If we wish to replace letters

Cipher Text: wi rf rwaj uh yftsdvf sfuufya

4.2 Monoalphabetic Ciphers

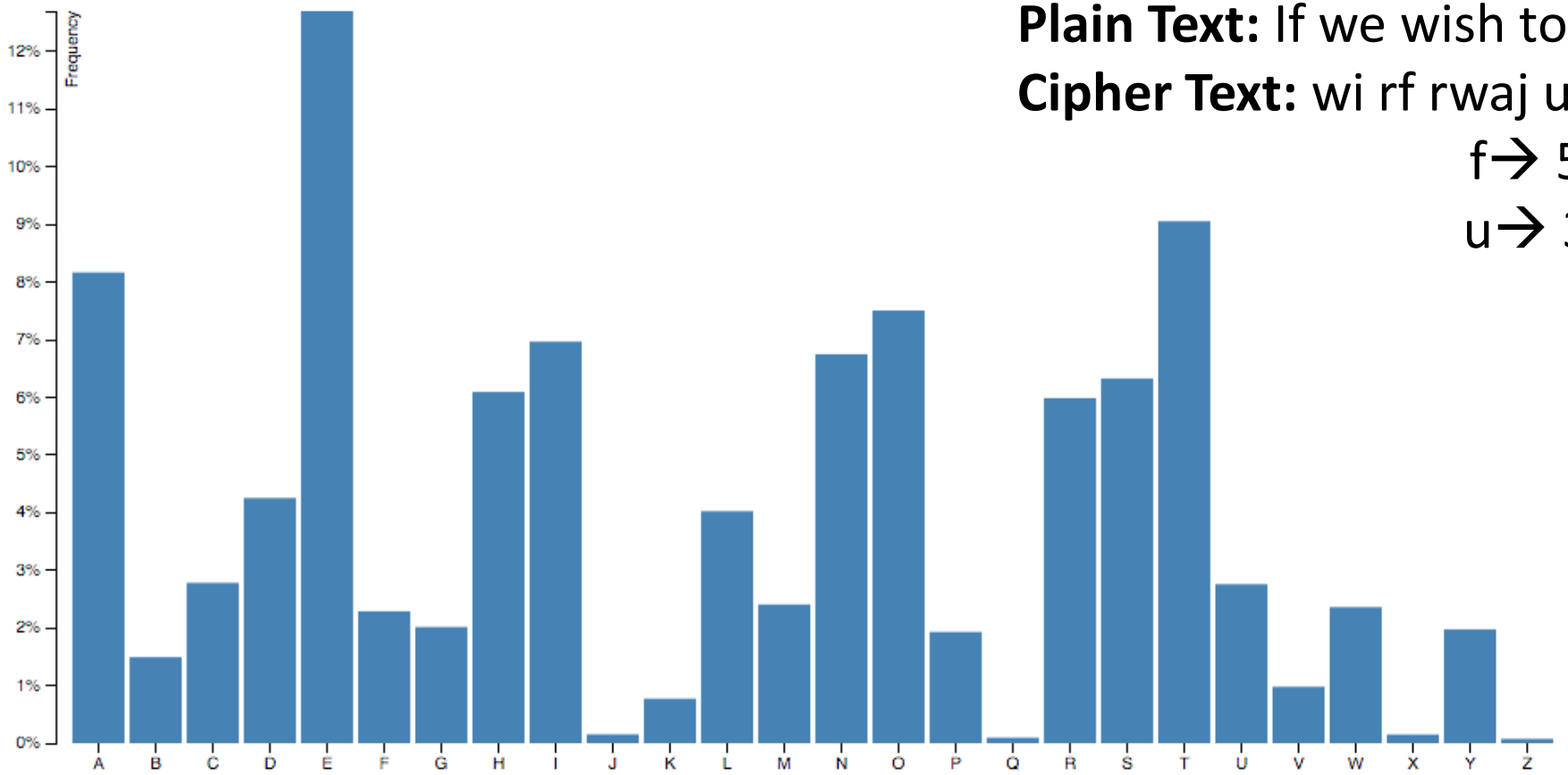


Figure 2: Relative frequency of letters in English text

Plain Text: If we wish to replace letters

Cipher Text: wi rf rwaj uh yftsdvf sfuufya

f→ 5

u→ 3

4.3 Playfair Cipher

Invented by British scientist “Sir Charles Wheatstone” in 1854, but it bears the name of his friend “Baron Playfair” of St. Andrews, who championed the cipher at the British foreign office.

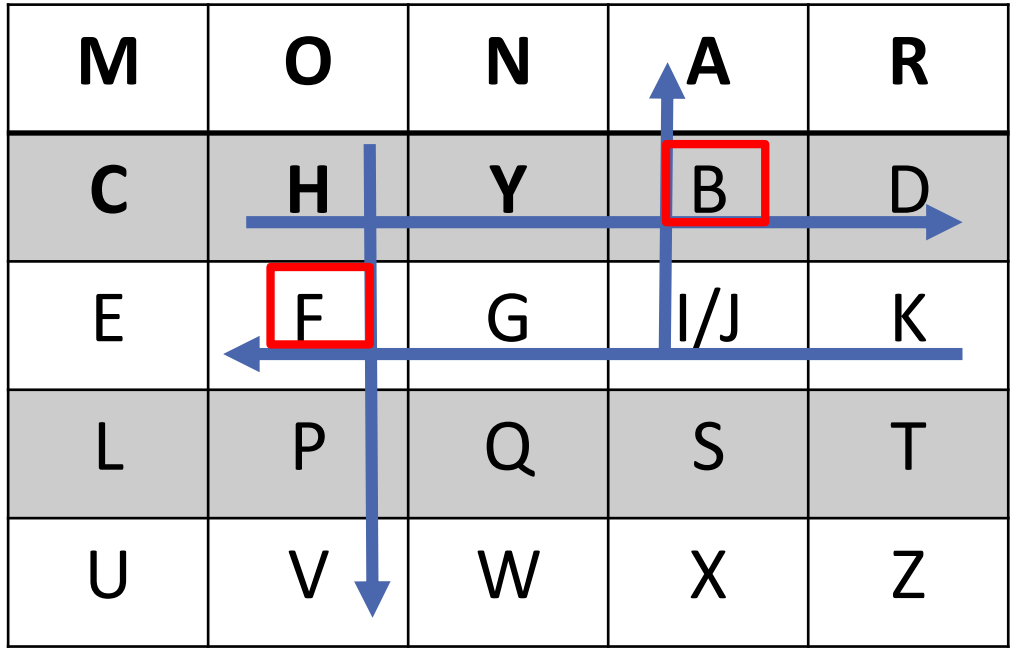
- ✓ 5X5 matrix
- ✓ keyword

Plain Text: hide the gold in the tree stump

HI DE TH EG OL DI NT HE TR EX ES TU MP

Cipher:

BF CK PD FI MP BK RQ CF ZD IU IL LZ OL



Exercise

Q 1: Keyword: PLAYFAIR

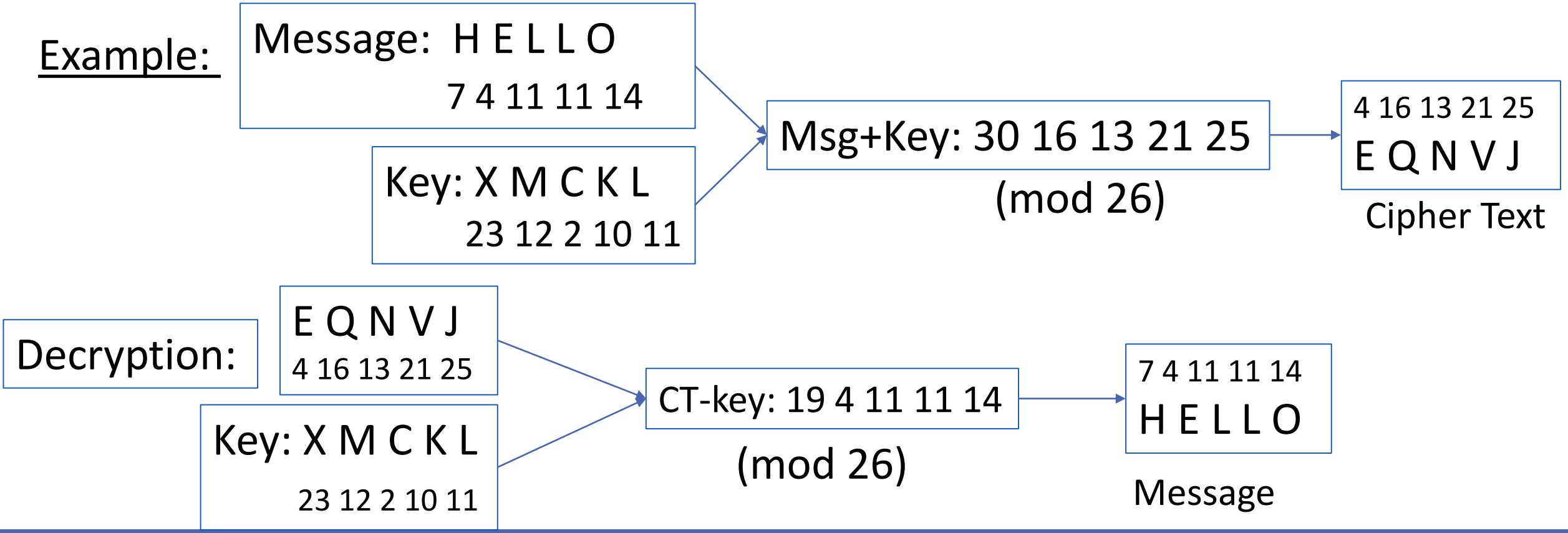
Plain Text: hide the gold in the tree stump

EB IM QM GH VR IR ON KG OD KU KN NZ EF

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

4.4 One-Time Pad

Once the key is used for encryption, it is never used again for any other message



Exercise

Q 1: PlainText: How are you

OneTimePad: NCBTZQARX

Cipher Text: UQXTQUYER

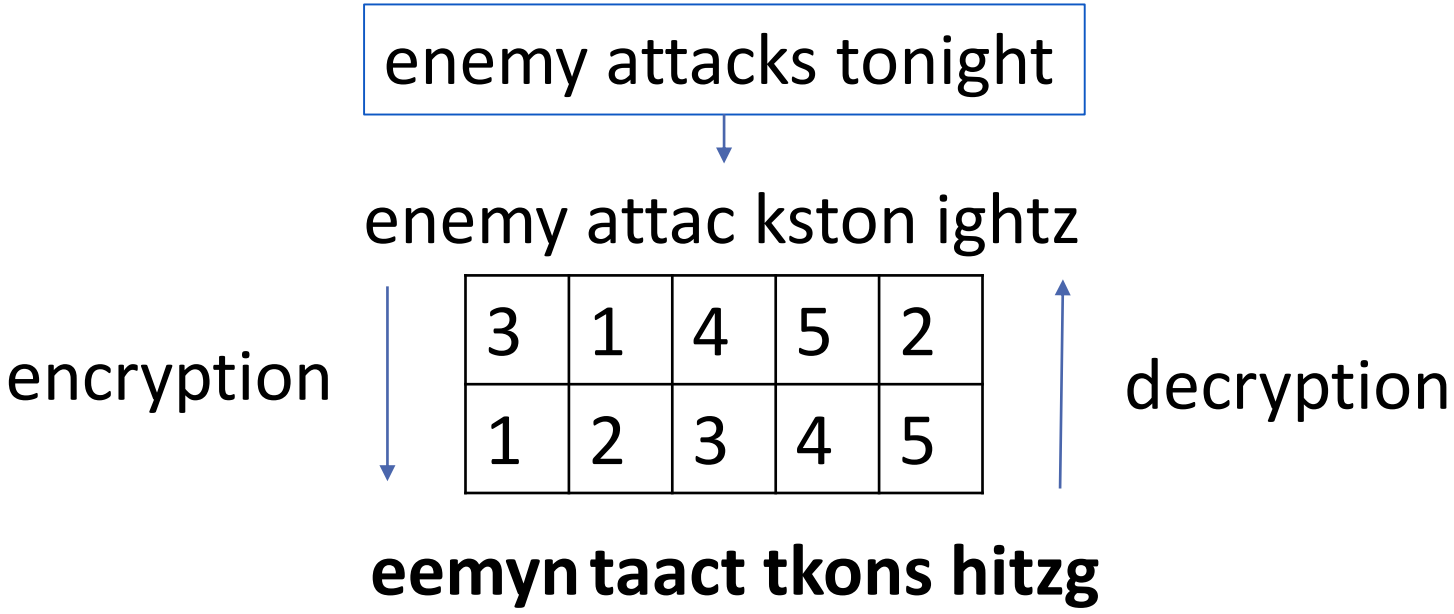
4.4.1 Drawbacks in One-Time Pad

- **Key generation and distribution:** Need for unlimited number of keys
- **Synchronization**

4.5 Transposition Ciphers

- Permutation ciphers
- Shuffle Plain Text without altering the actual letters used
- It doesn't substitute one symbol for another. Instead it changes the location of the symbol.

Example:



4.6 Data Encryption Standard

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

The fundamental building block of DES was designed by IBM.

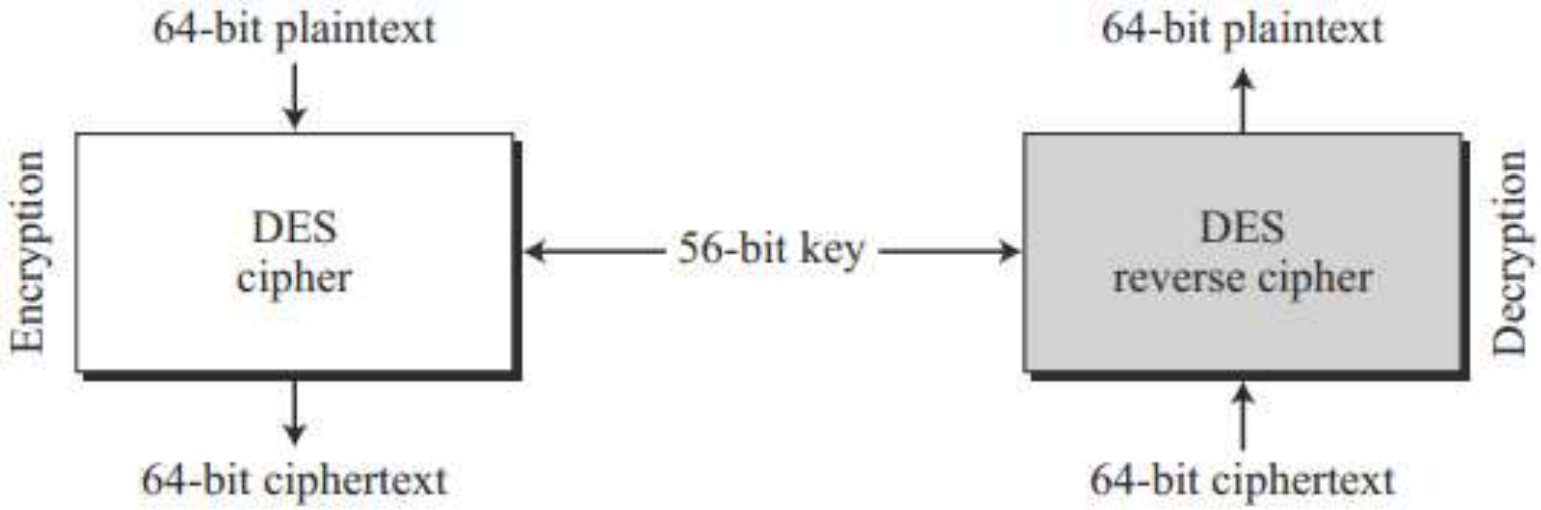


Figure 3: Encryption and Decryption with DES

4.6.1 Structure of DES

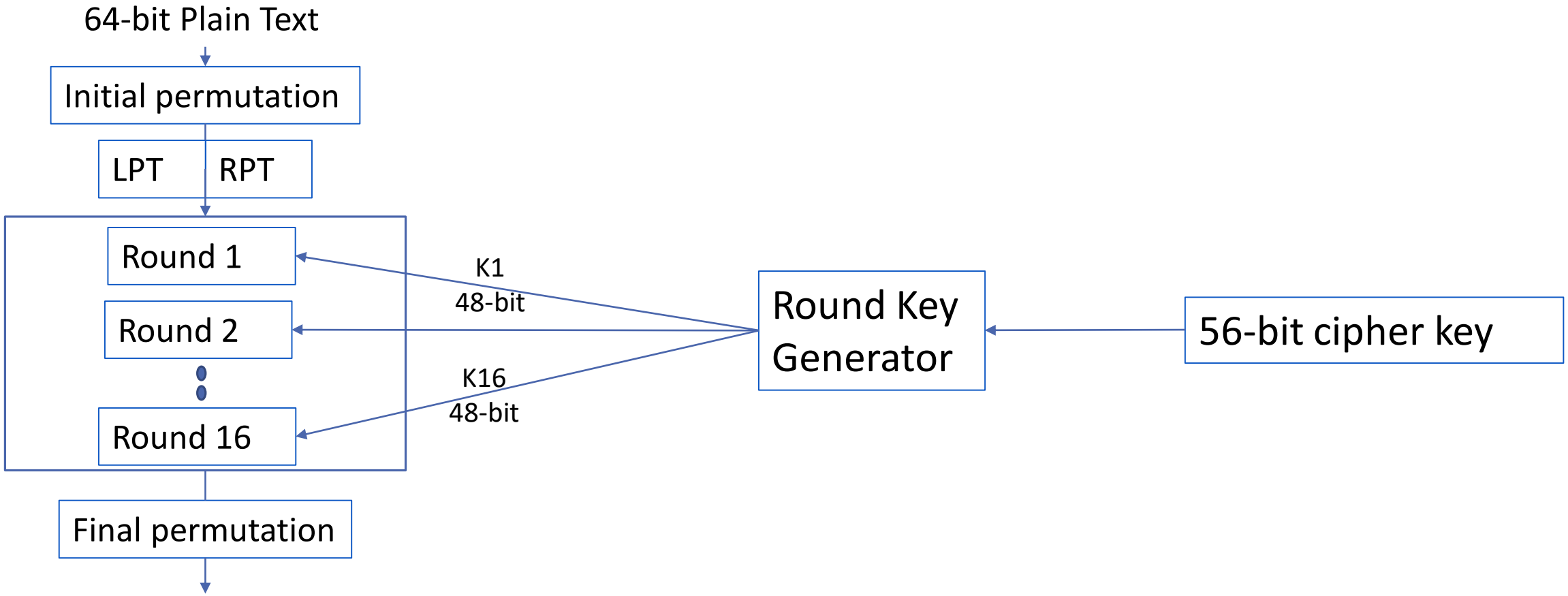
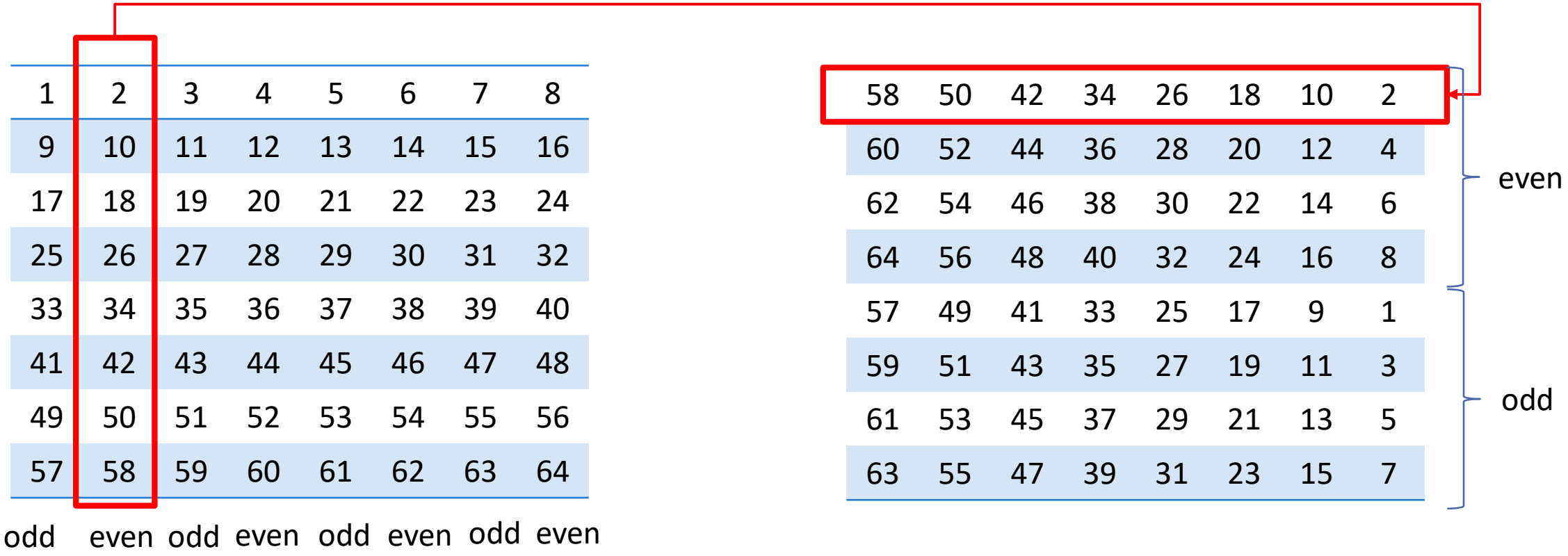


Figure 4: Structure of DES

4.6.1.1 Initial Permutation



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
odd	even	odd	even	odd	even	odd	even

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

even

odd

4.6.1.2 Rounds

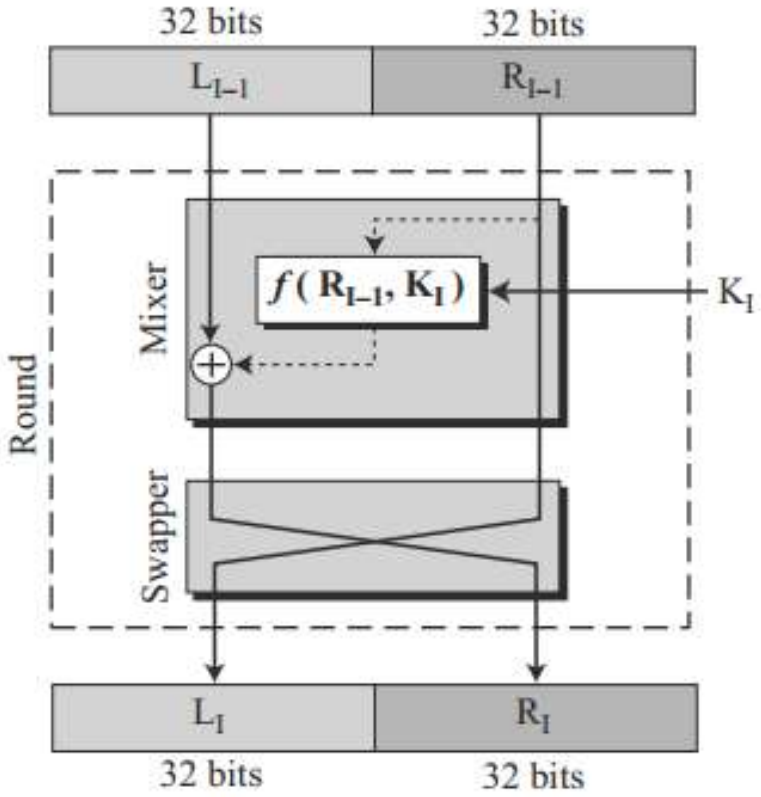


Figure 5: A round in DES

DES function

48 bit key to the rightmost 32 bits

Produce a 32-bit output

4.6.1.3 Function

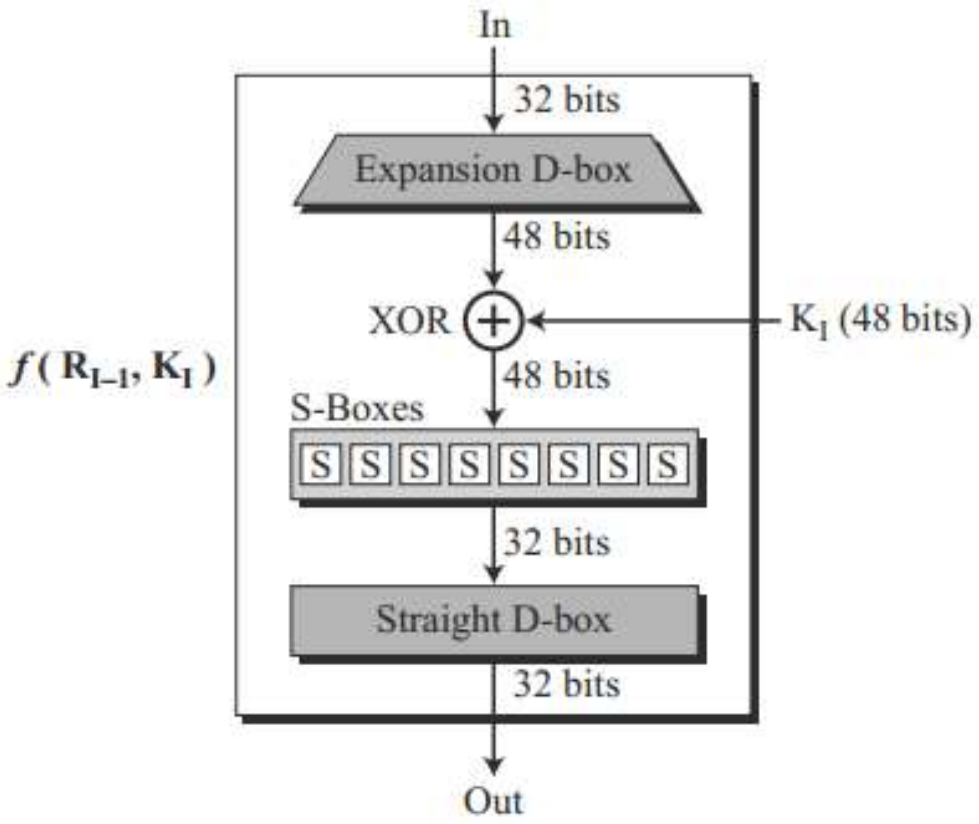
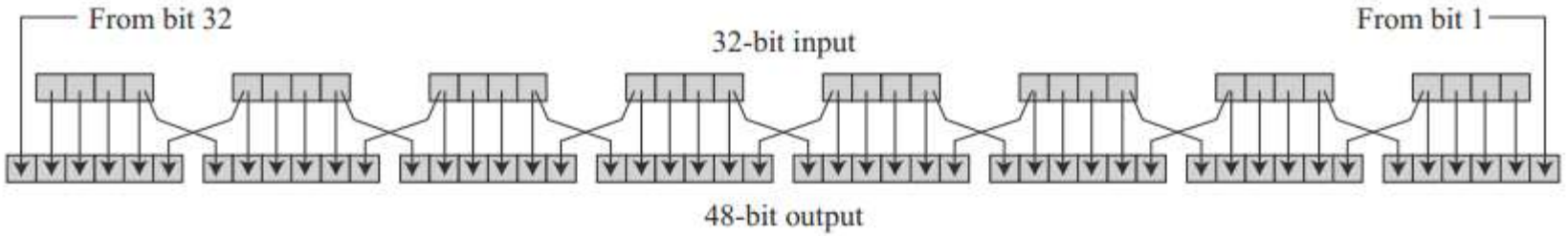


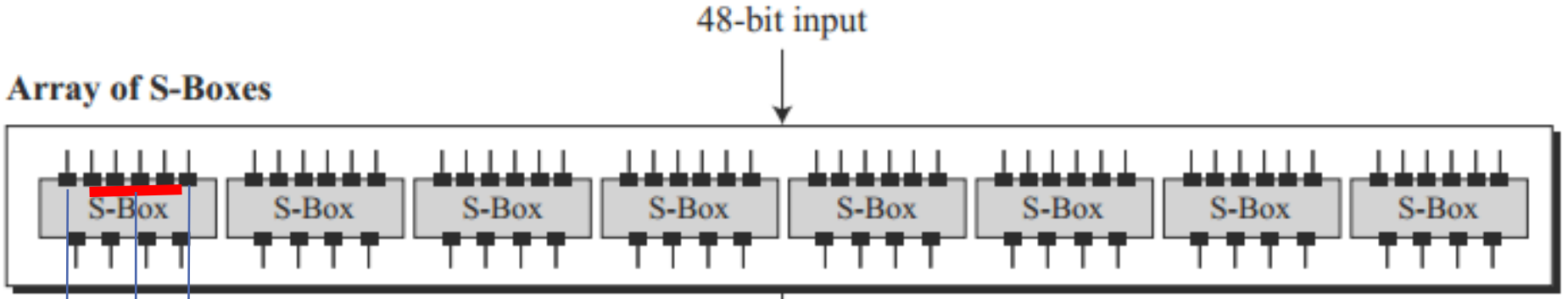
Figure 6: DES function

4.6.1.3 Function



32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

4.6.1.3 Function



0000 0th Column

11 3rd Row

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S-box 1

4.6.1.4 Straight Permutation

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

XOR with LPT

Swap LPT and RPT

Completion of 1st round

Note: 16th round don't have swapper (only mixer is there)

4.6.1.5 Final Permutation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Example **(STEP 1: LPT & RPT)**

M = 123456ABCD132536

M = 0001 0010 0011 0100 0101 0110 1010 1011 1100 1101 0001 0011 0010 0101 0011 0110

LPT = 0001 0100
1010 0111
1101 0110
0111 1000

RPT = 0001 1000
1100 1010
0001 1000
1010 1101

0	0	0	1	0	0	1	0
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	0
1	0	1	0	1	0	1	1
1	1	0	0	1	1	0	1
0	0	0	1	0	0	1	1
0	0	1	0	0	1	0	1
0	0	1	1	0	1	1	0

Example **(STEP 2: Expand RPT)**

0001 1000 1100 1010 0001 1000 1010 1101

10001**1** **1**1000**1** **0**1100**1** **0**1010**0** **0**0001**1** **1**1000**1** **0**1010**1** **0**1101**0**

Example **(STEP 3: XOR with Key and apply S-boxes)**

Key: 19 4C D0 72 DE 8C

100011 110001 011001 010100 000011 110001 010101 011010

000110 010100 110011 010000 011100 101101 111010 001100

2nd column

100101 100101 101010 000100 011111 011100 101111 010110

3rd row

S1	S2	S3	S4	S5	S6	S7	S8
1000	1010	1111	1110	0110	0101	0111	1110

Example **(STEP 4: Apply P-Boxes and XOR with LPT)**

1000	1010	1111	1110	0110	0101	0111	1110
1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32

0	1	0	0	1	1	1	0
1	1	0	1	1	1	1	0
0	0	1	1	0	1	0	1
1	1	1	0	1	1	0	0

⊕

0	0	0	1	0	1	0	0
1	0	1	0	0	1	1	1
1	1	0	1	0	1	1	0
0	1	1	1	1	0	0	0

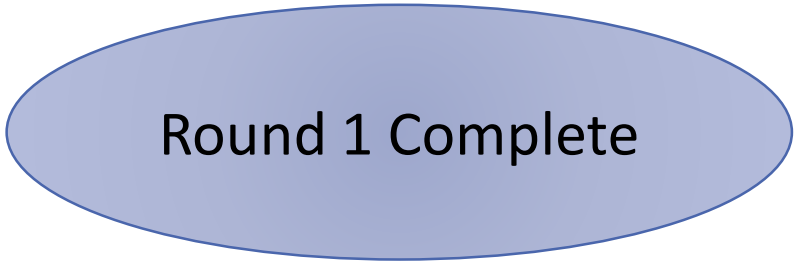
0101	1010	0111	1000	1110	0011	1001	0100
5	A	7	8	E	3	9	4

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Example **(STEP 5: Swapping)**

LPT: 18 CA 18 AD

RPT: 5A 78 E3 94

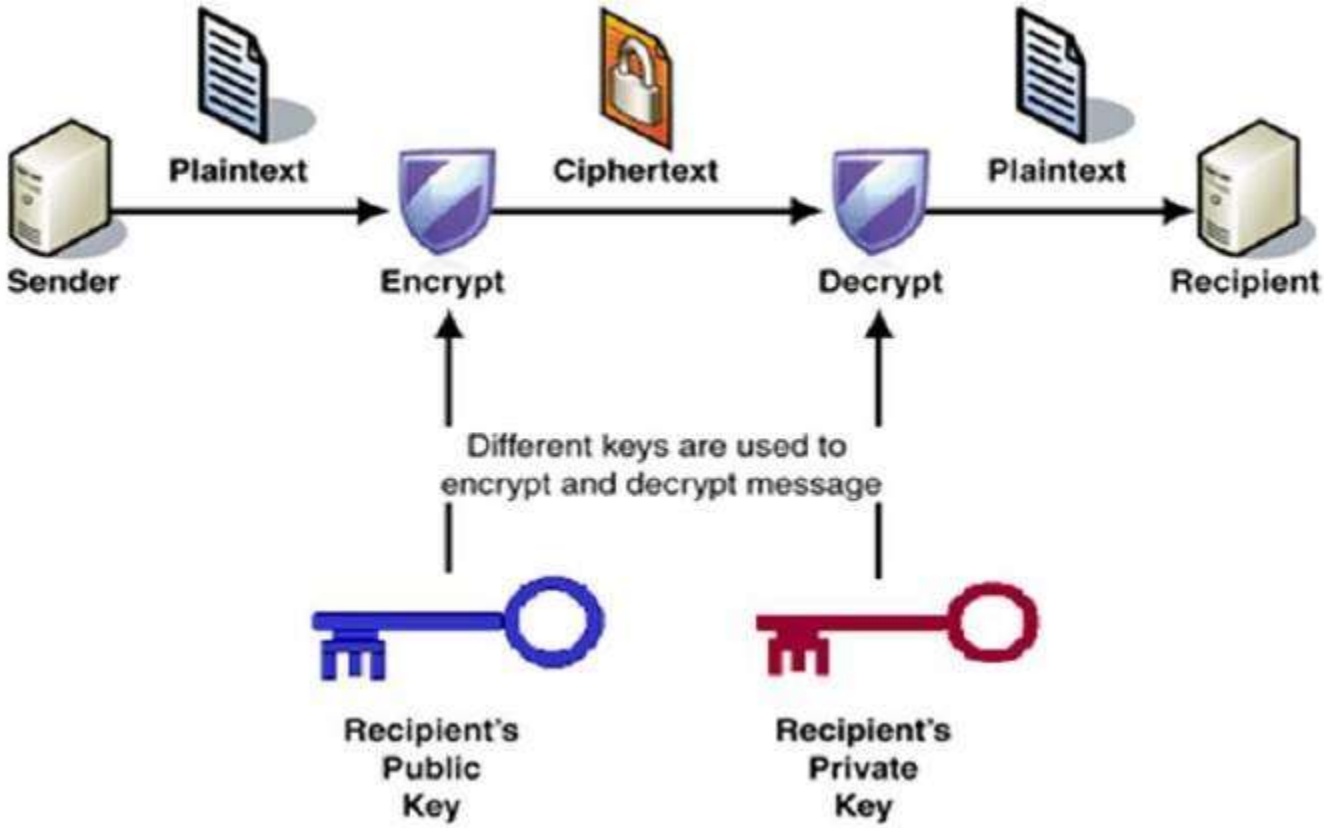


Code

des.c file

5. Asymmetric Key Cryptography

Also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.



5.1 RSA

Step 1: Choose 2 numbers p and q

example, p=7 q=11

Step 2: Find n= p*q

n=7*11=77

Step 3: Find ϕ(n)=(p-1)(q-1)

ϕ(n)=60

Step 4: e, d is public, private key pair

e d mode ϕ = 1 (Choose one value from e and d, then find another by hit and trial)

Choose value of e-> 1<e< ϕ

Suppose e=37

37*d mod ϕ = 1

37*13 mod 60 =1

(481) (e,d)= (37,31)

5.1 RSA

n=77, ϕ=60, e=37, d=13

Encrypted Data $C = P^e \pmod n$

$5^{37} \bmod 77 = 47$

Decrypted Data $P = C^d \pmod n$

$47^{13} \bmod 77 = 5$

Example

Bob chooses p=11, q=3. Now he chooses two keys 1 and d. If he chooses e=3, then d=7. Now imagine Alice sends the **Plaintext 7** to Bob. Calculate cipher text (c) sent by Alice. Also calculate plain text (p) calculated by Bob.

$$C = P^e \pmod{n} = 7^3 \bmod 33 = 13$$

$$P = C^d \pmod{n} = 13^7 \bmod 33 = 7$$

5.2 Diffie Hellman

Key exchange protocol

It is used to exchange key securely on calculation without passing the actual keys.

5.2 Diffie Hellman

g=7 p=23 (prime numbers)

g and p are public

Step 1: A B

Choose x and y (any number)

x=3 y=6

Step 2: R_1= g^x mod P R_2 =g^y mod P

7^3 mod 23 7^6 mod 23

21 4

Step 3: A will send R_1 to B and B will send R_2 to A.

Step 4: K=$R_2{}^x$ mod P K=$R_1{}^x$ mod P

4^3 mod 23 21^6 mod 23

18 18

Example

x=4 y=6 g=10 P=17

R_1=4
K=16

R_2=9
K=16


Thank you!!