Introduction

- Shift cipher – shift the plaintext letter a fixed number of positions modulo 26 to the ciphertext letter
- Block or transposition cipher – break message into blocks and permute the letters in the block
- RSA Cryptosystem – create a key (n, e). To encrypt, convert the letters to two-digit positive integers, put integers into a block, raise the block to the power e modulo n. To decrypt, employ the key (n, d) found from the encryption key (n, e). Raise the enciphered message to the power d modulo n.

Classical Cryptography

Caesar cipher.

Encryption: $f(p) = (p + 3)$ **mod** 26, where A is replaced by 0, B replaced by 1, … Z replaced by 25.

Decryption: $f^{-1}(p) = (p - 3)$ **mod** 26, where 0 is replace by A, 1 replaced by B, … 25 replaced by Z.

EXAMPLE 1 What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

Solution:

1. First replace the letters in the message with numbers. Row 1 has the letters and row 2 has the corresponding numbers.
2. Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26 as shown in row 3.
3. Finally, translate the encrypted numbers to their corresponding letters as show in the bottom row.

M	E	E	T		Y	O	U		I	N
12	4	4	19		24	14	20		8	13
15	7	7	22		1	17	23		11	16
P	H	H	W		B	R	X		L	Q

T	H	E		P	A	R	K
19	7	4		15	0	17	10
22	10	7		18	3	20	13
W	K	H		S	D	U	N

Plaintext	M
Numbers	12
Encrypted numbers	15
Ciphertext	P

EXAMPLE 2 Encrypt the plaintext message "STOP GLOBAL WARMING" using the shift cipher with shift $k = 11$.

Solution:

- $f(p) = (p + k) \bmod 26$
- $f(p) = (p + 11) \bmod 26$

S	T	O	P		G	L	O	B	A	L
18	19	14	15		6	11	14	1	0	11
3	4	25	0		17	22	25	12	11	22
D	E	Z	A		R	W	Z	M	L	W

W	A	R	M	I	N	G
22	0	17	12	8	13	16
7	11	2	23	19	24	17
H	L	C	X	T	Y	R

Plaintext	S
Numbers	18
Encrypted numbers	3
Ciphertext	D

EXAMPLE 3 Decrypt the ciphertext message LEWLYPLUJL PZ H NYLHA A LHKOLY that was encrypted with the shift cipher with shift $k = 7$.

Solution:

L	E	W	L	Y	P	L	U	J	L	
11	4	22	11	24	15	11	20	9	11	
4	23	15	4	17	8	4	13	2	4	
E	X	P	E	R	I	E	N	C	E	

P	Z		H		N	Y	L	H	A	
15	25		7		13	24	11	7	0	
8	18		0		6	17	4	0	19	
I	S		A		G	R	E	A	T	

A	L	H	K	O	L	Y				
0	11	7	9	14	11	24				
19	4	0	2	7	4	17				
T	E	A	C	H	E	R				

Ciphertext	S
Encrypted Numbers	18
Plaintext numbers	3
Plaintext	D

EXAMPLE 4 What letter replaces the letter K when the function $f(p) = (7p + 3)$ **mod** 26 is used for encryption?
Solution:

K
10
$(7 \times 10 + 3)$ **mod** $26 = 21$
V

Plaintext	K
Numbers	10
Encrypted numbers	21
Ciphertext	V

EXAMPLE 5 Suppose that we intercepted the ciphertext message ZNK KGXRE HOXJ MKZY ZNK CUXS that we know was produced by a shift cipher. What was the original plain text message?
Solution:

The letter that occurs most frequently is K having a numeric value of 10. Solving for the shift value k and assuming that the letter K is the ciphertext encryption for the letter E, we find $10 = 4 + k$, where 4 represents the numeric value of the letter E and k is the shift value. We find $k = 6$ meaning letters are shifted six (6) positions toward the beginning of the alphabet or twenty (20) positions toward the end of the alphabet and, whether shifting toward the beginning or the end, we perform the operation modulo 26.

Z	N	K		K	G	X	R	E
25	13	10		10	6	23	17	4
19	7	4		4	0	17	11	24
T	H	E		E	A	R	L	Y

H	O	X	J		M	K	Z	Y
7	14	23	9		12	10	25	24
1	8	17	3		6	4	19	18
B	I	R	D		G	E	T	S

Z	N	K		C	U	X	S
25	13	10		2	20	23	18
19	7	10		22	20	23	18
T	H	E		W	O	R	M

Ciphertext	S
Encrypted Numbers	18
Plaintext numbers	3
Plaintext	D

EXAMPLE 6 Using the transposition cipher base on the permutation σ of the set {1,2,3,4} with $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4$, and $\sigma(4) = 2$.

(a) Encrypt the plaintext message PIRATE ATTACK
(b) Decrypt the ciphertext message SWUE TRAE OEHS, which was encrypted using this cypher

Solution (a):

1. Convert the message to blocks of four (4) letters

P	I	R	A	T	E	A	T	T	A	C	K

2. Encrypt the message.

1	2	3	4	1	2	3	4	1	2	3	4
P	I	R	A	T	E	A	T	T	A	C	K
I	A	P	R	E	T	T	A	A	K	T	C
3	1	4	2	3	1	4	2	3	1	4	2

Solution (B):

$$\sigma^{-1}(1) = 2, \sigma^{-1}(2) = 4, \sigma^{-1}(3) = 1, \sigma^{-1}(4) = 3$$

S	W	U	E	T	R	A	E	O	E	H	S
U	S	E	W	A	T	E	R	H	O	S	E

USE WATER HOSE