Unit I

Cryptography,

Definitions

- Cryptography
  - is the study or science of secret communication,
- Encryption
  - is simply a component of that science.
  - Encryption is the process of hiding information, through the use of ciphers,
- Cryptanalysis
  - is the art of decrypting or obtaining plain text from hidden messages over an insecure channel. It is also known as code cracking.
- Cryptology
  - Study of the mathematics behind encryption/decryption

Conventional Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
    - Original message
  - Encryption algorithm
    - For various transformation and substitution
  - Secret Key
    - How to do transformation and substitution depends on key
  - Cipher text
    - The scrambled message
  - Decryption algorithm
    - The encryption algorithm in reverse on the cipher text to obtain the original message

Conventional Encryption Principles

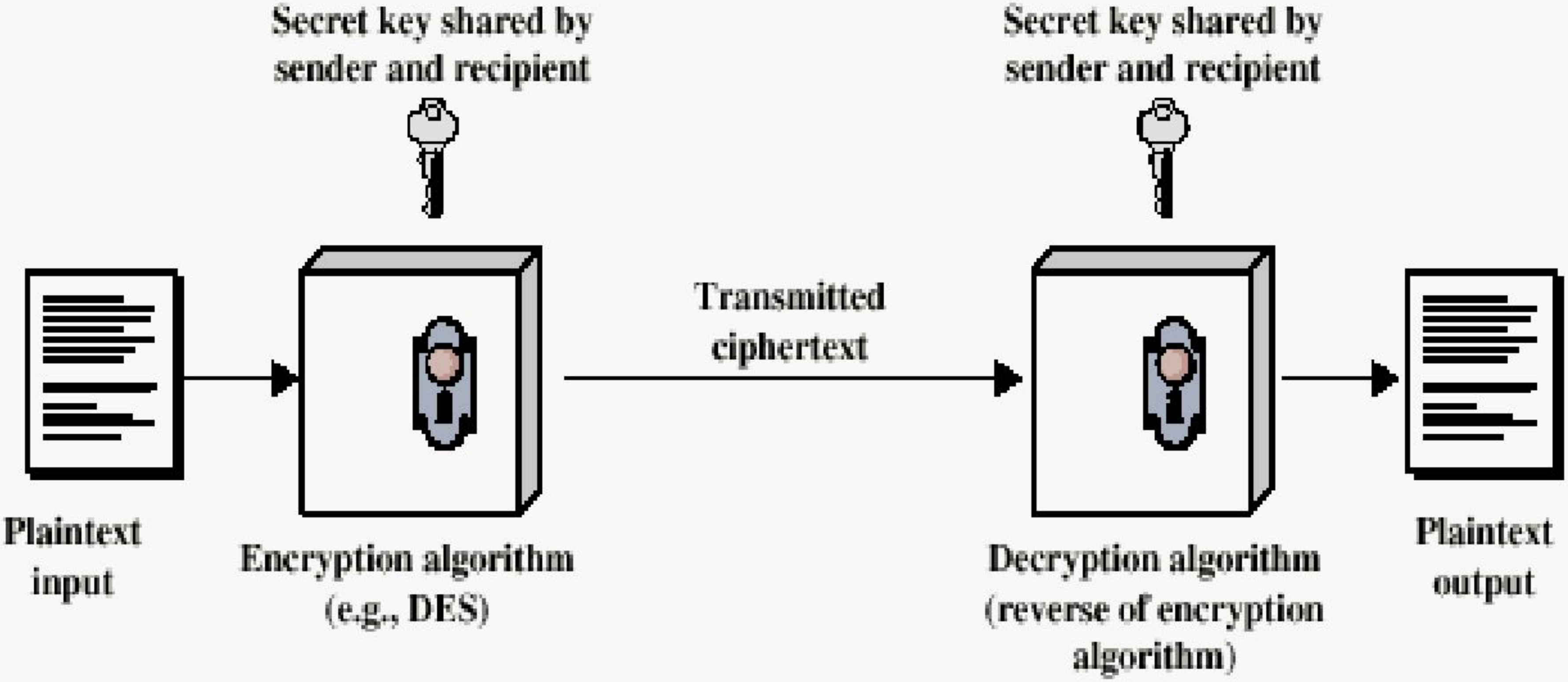
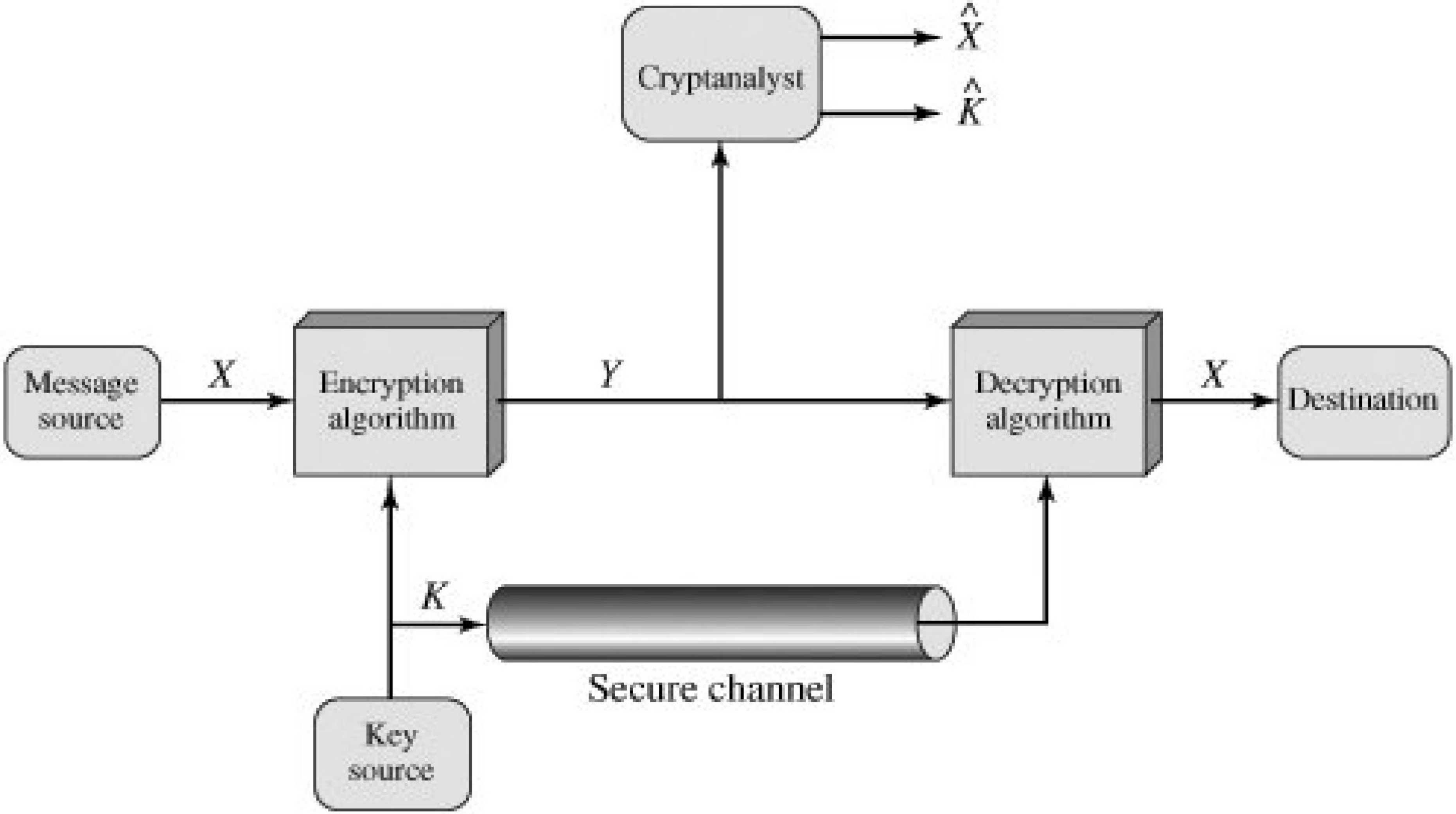

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Conventional Encryption

Model for conventional Cryptosystem



Cryptography Techniques

There are three Techniques

- Secret key or Symmetric Cryptography – it uses same key for encryption and decryption
- Public-key or Asymmetric Cryptography, and – it uses one key for encryption and another for decryption
- Hash functions – it makes use of a mathematical transformation to encrypt the information in an irreversible manner.

Cryptography

Cryptographic systems are classified along three independent dimensions

The type of operations used for transforming plaintext to ciphertext.

Substitution: An element in plaintext is mapped into another element

Transposition: Elements in the plaintext are rearranged.

>>Fundamental requirements: **all operations be reversible**.

>> Most systems use a combination of substitution and transposition

The number of keys used:

Symmetric (single key used by both the sender and receiver)

Asymmetric (two keys or public key, sender and receiver use different keys

The way the plaintext is processed.

block cipher process

Stream cipher process

Types of Attacks

- Ciphertext-only attack – In this case, the attacker has only the cipher text to reach plaintext, and thus he makes guess about the plaintext.
- Known-plaintext attack – In this case, the attacker tries to guess the plaintext by analyzing some part of the cipher text. Eg. A postscript
- Chosen-plaintext attack – the cryptanalyst can choose plaintexts and obtain their corresponding cipher texts. The aim is to choose the plaintexts such that the resulting pairs of plaintext and cipher texts makes easy for deducing the encryption key.
- Man in the middle attack – the person will intercept the signals sent by sender and receiver. He will pose to them as the other party and will exchange keys with both of them separately.

Steganography

- Means covered writing
- Steganography is data hidden within data.
- Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.
- Steganography techniques can be applied to images, a video file or an audio file.
- The hiding of a message within another so that the presence of the hidden message is indiscernible
- The key concept behind steganography is that the message to be transmitted is not detectable to the casual eye.

Steganography

- The difference between steganography and cryptography is that in cryptography, one can tell that a message has been encrypted, but he cannot decode the message without knowing the proper key.
- In steganography, the message itself may not be difficult to decode, but most people would not detect the presence of the message
- When combined, steganography and cryptography can provide two levels of security.
- Computer programs exist which encrypt a message using cryptography, and hide the encryption within an image using steganography.

Table 2.2. Average Time Required for Exhaustive Key Search

Key size (bits)	Number of alternative keys	Time required at 1 decryption/*m*s	Time required at 10^6 decryption/*m*s
32	$2^{32} = 4.3 \times 10^9$	2^{31} *ms* = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} *ms* = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} *ms* = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} *ms* = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	26! = 4×10^{26}	2×10^{26} *ms* = 6.4×10^{12} years	6.4×10^6 years

Classical Encryption techniques

CES:

Substitution: The letters of plaintext are replaced by other letters or by numbers or by symbols

Transposition: Different kind of mapping is achieved by performing some sort of permutation on the plaintext letters

Substitution Techniques

Types of Cipher

1) Caesar Cipher
2) Monoalphabetic Cipher
3) Playfair Cipher
4) Hill Cipher
5) Polyalphabetic Cipher

Caesar Cipher (Julias Caesar)

- The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example:

- plain: meet me after the toga party
- cipher: PHHW PH DIWHU WKH WRJD SDUWB

$(c+k) \bmod 26 =$ $(c-k) \bmod 26 =$

$(c*k) \bmod 26$ $(c*i/k) \bmod 26$

$\gcd(k,26) = 1$

Key = 7 (7,26)

Hello

…..

23*

Caesar Cipher (Julias Caesar)

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

Caesar Cipher (Julias Caesar)

Let us assign numerical to each letter

a	b	c	d	e	f	g	h	I	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- **The algorithm can be expressed as:**

$$C = E(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is

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

where *k takes on a value in the range 1 to 25.*

The decryption algorithm is simply

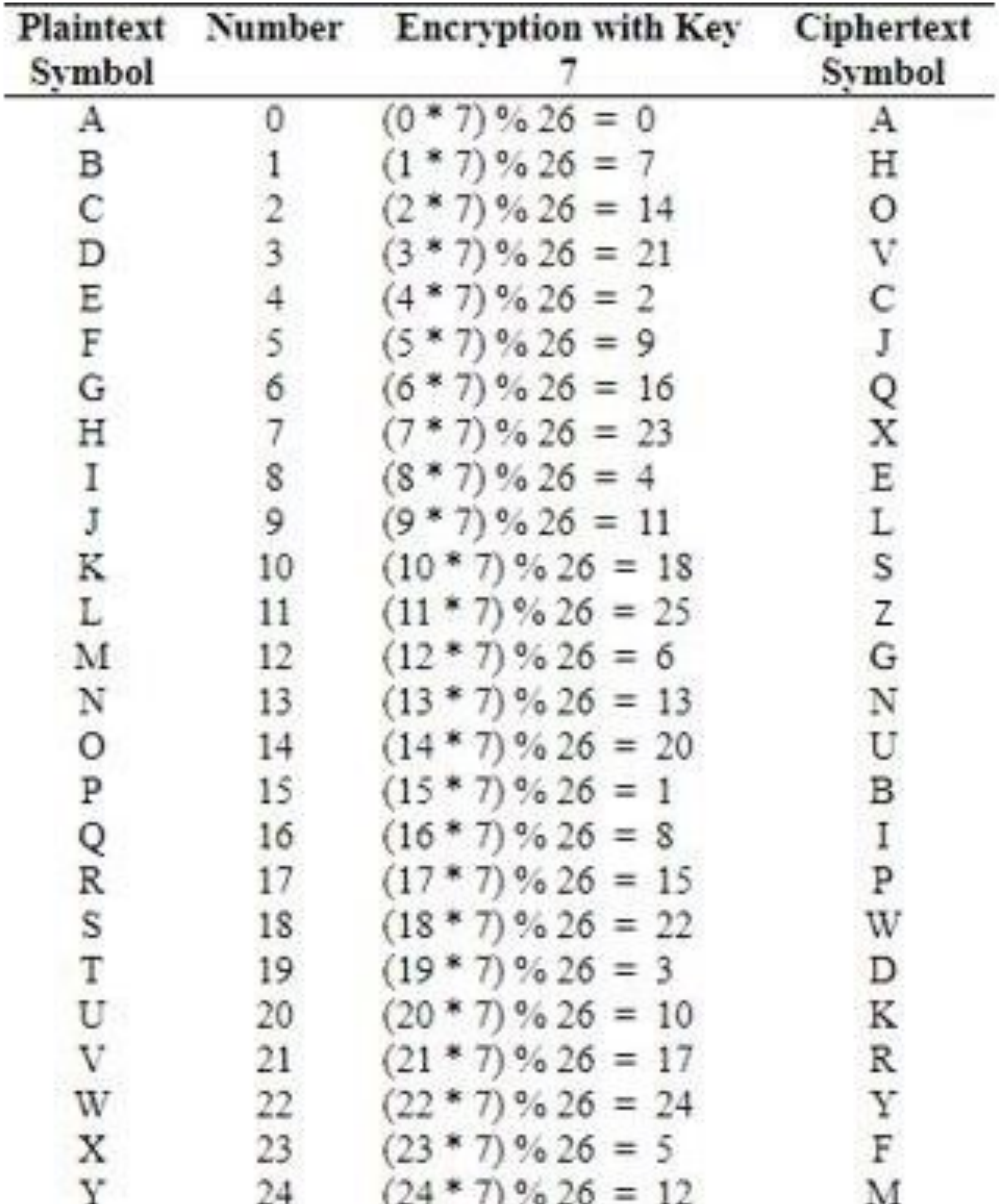
$$p = D(k, C) = (C - k) \bmod 26$$

Drawbacks of Caesar Cipher

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

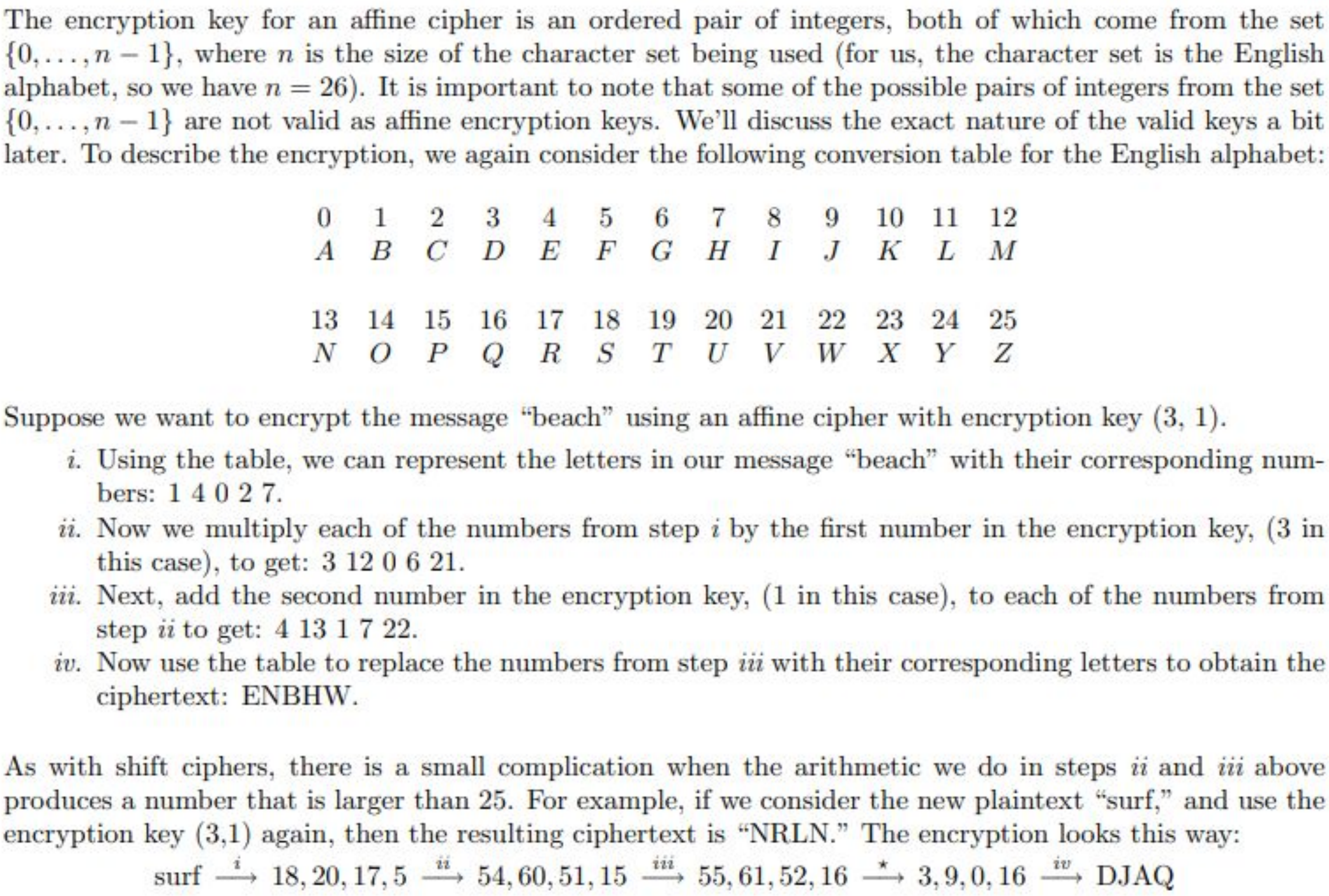
N

A



Plaintext Symbol	Number	Encryption with Key 7	Ciphertext Symbol
A	0	(0 * 7) % 26 = 0	A
B	1	(1 * 7) % 26 = 7	H
C	2	(2 * 7) % 26 = 14	O
D	3	(3 * 7) % 26 = 21	V
E	4	(4 * 7) % 26 = 2	C
F	5	(5 * 7) % 26 = 9	J
G	6	(6 * 7) % 26 = 16	Q
H	7	(7 * 7) % 26 = 23	X
I	8	(8 * 7) % 26 = 4	E
J	9	(9 * 7) % 26 = 11	L
K	10	(10 * 7) % 26 = 18	S
L	11	(11 * 7) % 26 = 25	Z
M	12	(12 * 7) % 26 = 6	G
N	13	(13 * 7) % 26 = 13	N
O	14	(14 * 7) % 26 = 20	U
P	15	(15 * 7) % 26 = 1	B
Q	16	(16 * 7) % 26 = 8	I
R	17	(17 * 7) % 26 = 15	P
S	18	(18 * 7) % 26 = 22	W
T	19	(19 * 7) % 26 = 3	D
U	20	(20 * 7) % 26 = 10	K
V	21	(21 * 7) % 26 = 17	R
W	22	(22 * 7) % 26 = 24	Y
X	23	(23 * 7) % 26 = 5	F
Y	24	(24 * 7) % 26 = 12	M

Affine cipher



The encryption key for an affine cipher is an ordered pair of integers, both of which come from the set $\{0, \ldots, n-1\}$, where n is the size of the character set being used (for us, the character set is the English alphabet, so we have $n = 26$). It is important to note that some of the possible pairs of integers from the set $\{0, \ldots, n-1\}$ are not valid as affine encryption keys. We'll discuss the exact nature of the valid keys a bit later. To describe the encryption, we again consider the following conversion table for the English alphabet:

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*

Suppose we want to encrypt the message "beach" using an affine cipher with encryption key (3, 1).

i. Using the table, we can represent the letters in our message "beach" with their corresponding numbers: 1 4 0 2 7.

ii. Now we multiply each of the numbers from step *i* by the first number in the encryption key, (3 in this case), to get: 3 12 0 6 21.

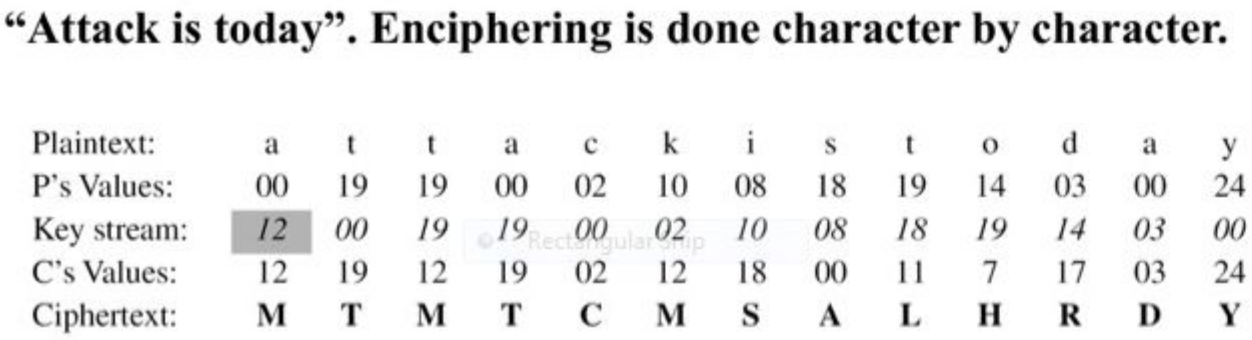
iii. Next, add the second number in the encryption key, (1 in this case), to each of the numbers from step *ii* to get: 4 13 1 7 22.

iv. Now use the table to replace the numbers from step *iii* with their corresponding letters to obtain the ciphertext: ENBHW.

As with shift ciphers, there is a small complication when the arithmetic we do in steps *ii* and *iii* above produces a number that is larger than 25. For example, if we consider the new plaintext "surf," and use the encryption key (3,1) again, then the resulting ciphertext is "NRLN." The encryption looks this way:

$$\text{surf} \xrightarrow{i} 18, 20, 17, 5 \xrightarrow{ii} 54, 60, 51, 15 \xrightarrow{iii} 55, 61, 52, 16 \xrightarrow{\star} 3, 9, 0, 16 \xrightarrow{iv} \text{DJAQ}$$

Auto Key Cipher



"Attack is today". Enciphering is done character by character.

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

Mono-alphabetic Cipher

- Instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4 x 10^{26} possible keys.
- This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis.
- Such an approach is referred to as a **mono alphabetic substitution cipher, because a single cipher alphabet (mapping f**rom plain alphabet to cipher alphabet) is used per message.

Mono-alphabetic Cipher

- They are easy to break because they reflect the frequency data of the original alphabet
- A counter measure is to provide multiple substitutes known as homophones

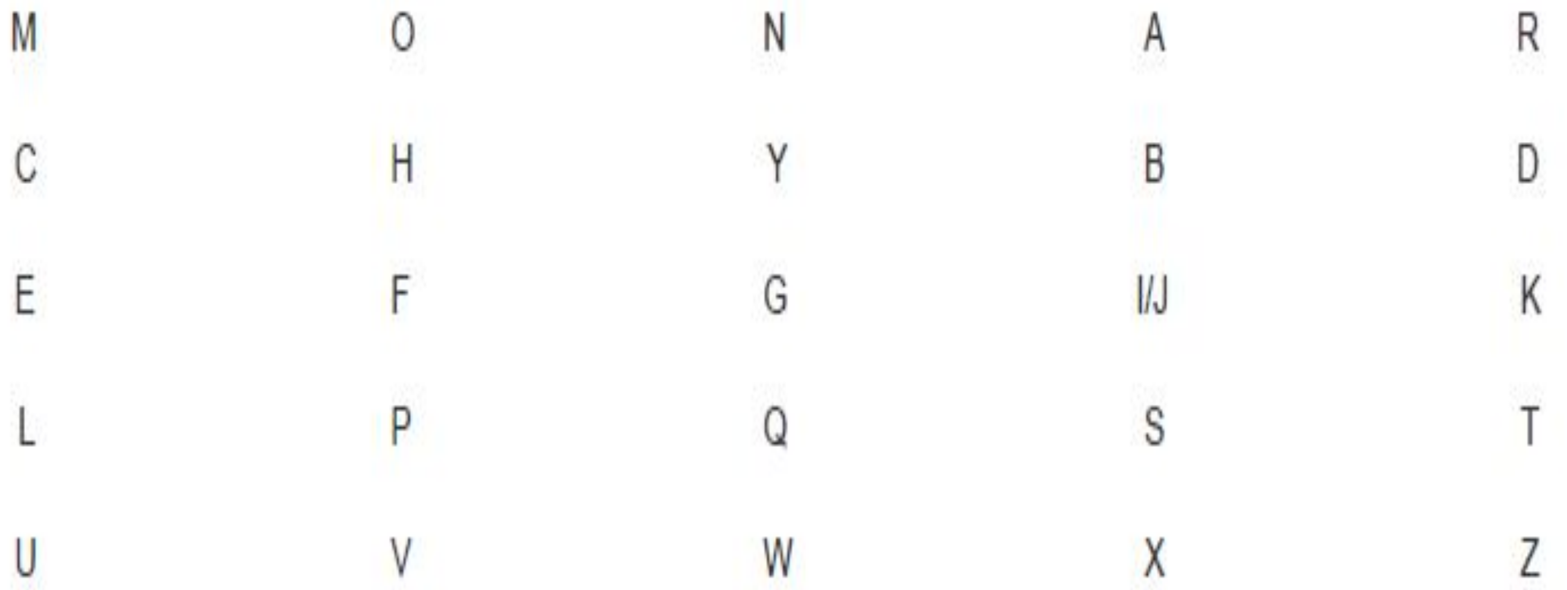
Plain letters with rounded %-frequency	Assigned cipher numbers	Plain letters with rounded %-frequency	Assigned cipher numbers
e - 12	00,06,13,32,52,53,71,72,83,93,94	m - 3	33,51,80
t - 10	14,16,30,31,43,58,73,79,84	p - 2	12,50
o - 8	11,15,25,41,42,57,78,85	y - 2	49,68
i - 8	03,10,34,35,54,56,77,86	f - 2	24,45
a - 8	18,19,20,36,55,62,76,87	g - 2	01, 96
n - 7	02,37,38,59,61,69,70	w - 2	81,98
r - 6	09,26,39,60,75,88	b - 2	48,97
s - 6	17,28,63,74,89	v - 1	99
h - 5	04,08,27,64	k - 1	67
l - 4	21,40,65,82	x - 1	47
d - 3	05,29,66	j - 1	95
u - 3	07,22,91	q - 1	90
c - 3	23,44,92	z - 1	46

Mono-alphabetic Cipher with homophones

- Verify that the sender encodes cryptography to 440968123085962655122 749.
- The sender and the recipient share the above table as a key. As a recipient, decode 792793 087851785004116993 923512649360 922069 9772 66932342663205 .

Playfair Cipher

- The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.
- Example: 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

Encrypting and Decrypting

There are three rules: Plaintext is encrypted two letters at a time.

- 1) If the two letters are in the same row, they are each encoded using the letter to their right. (AR goes to RM). If there is no such letter, because you are at the end of the row, then use the first letter instead
- 2) If the two letters are in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last. So mu as RM.
- 3) Otherwise, each plain text letter is replaced by the letter that lies own row and column occupied by the other plaintext letter. Thus, HS becomes BP and EA becomes IM.

Example

- Encrypt the following using playfair cipher
- WE ARE DISCOVERED SAVE YOURSELF

WE AR ED IS CO VE RE DS AV EY OU RS EL FX

UG RM KC SX HM UF MK BT OX GC MV AT LU IV

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

ESTATE

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

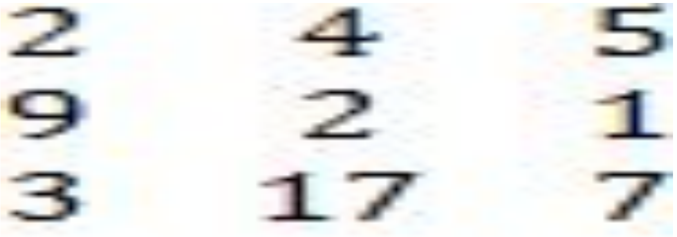
WE ARE GOING TO MALL

WE AR EG OI NG TO MA LL

VS GY AC VO MH EQ RG LL

Hill Ciphers

- This example will rely on some linear algebra and some number theory. The *key* for a hill cipher is a matrix. Here the matrix size is 3x3. But it can be any size



2	4	5
9	2	1
3	17	7

Assume the message is ATTACK AT DAWN

- To encipher this, we need to break the message into chunks of 3. We now take the first 3 characters from our plaintext, ATT and create a vector that corresponds to the letters (replace A with 0, B with 1 ... Z with 25 etc.) to get: [0 19 19] (this is ['A' 'T' 'T']).

Hill Ciphers

- To get our cipher text we perform a matrix multiplication

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \\ 19 \end{bmatrix} = \begin{bmatrix} 171 \\ 57 \\ 456 \end{bmatrix} \pmod{26} = \begin{bmatrix} 15 \\ 5 \\ 14 \end{bmatrix} = \text{'PFO'}$$

Hill Ciphers

Now for the tricky part, the decryption. We need to find an inverse matrix modulo 26 to use as our 'decryption key'. i.e. we want something that will take 'PFO' back to 'ATT'. If our 3 by 3 key matrix is called K, our decryption key will be the 3 by 3 matrix K^{-1}, which is the inverse of K.

$$K^{-1}\begin{bmatrix} 15 \\ 5 \\ 14 \end{bmatrix} \pmod{26} = \begin{bmatrix} 0 \\ 19 \\ 19 \end{bmatrix} = \text{'ATT'}$$

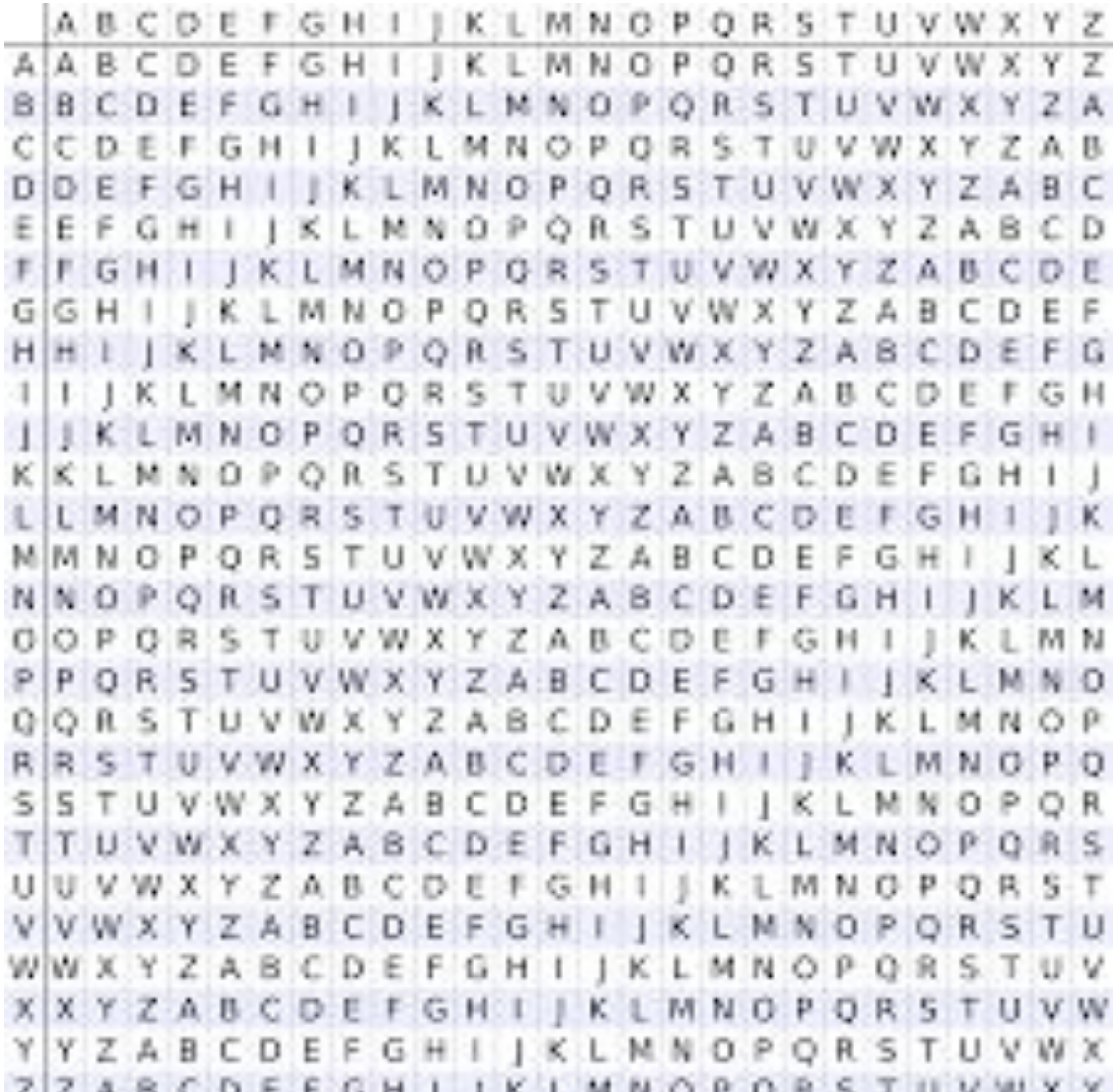
How to find K^{-1}?

- Take as an exercise for decryption

Polyalphabetic Ciphers Vigenere Ciphers

- Pick a keyword (for our example, the keyword will be "MEC").
- Write your keyword across the top of the text you want to encipher, repeating it as many times as necessary.
- For each letter, look at the letter of the keyword above it (if it was 'M', then you would go to the row that starts with an 'M'), and find that row in the Vigenere table.
- Then find the column of your plaintext letter (for example, 'w', so the twenty-third column).

Vigenere Table



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

Example – Vigenere Cipher

Keyword: M E C M E C M E C M E C M E C
M E C M E C M

Plaintext: w e n e e d m o r e s u p p l
i e s f a s t

Ciphertext: I I P Q I F Y S T Q W W B T N
U I U R E U F

Transposition Cipher
1. Rail Fence cipher

- Example:

Meet me after the toga party

- We can write the message: (rail fence technique is)

```
m   e   m   a   t   r   h   t   g   p   r   y
  e   t   e   f   e   t   e   o   a   a   t
```

- The Encrypted message is

```
MEMATRHTGPRYETEFETEOAAT
```

2. Row Transposition Ciphers

- A more complex scheme
- Transposition cipher writes the message into a rectangle by rows and reads it out by columns
- Write letters of message out in rows over a specified number of columns
- Then reorder the columns according to some key before reading off the rows
- **Attack postponed until two am**

```
Key:        4 3 1 2 5 6 7
Plaintext:  a t t a c k p
            o s t p o n e
            d u n t i l t
            w o a m x y z (See column wise 12356)
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Exercise

Playfair cipher
Use the word KEYWORD as keyword and encode
“Come to the window”

Affine Cipher
Use additive cipher key as 15 and multiplicative cipher key as 17
Decode the same string

Hill Cipher
Input : Plaintext: ACT
Key: GYBNQKURP