Information Protection & Computer Security

Rajendra Kachhwaha
Email: rajendra1983@gmail.com

June 9, 2015

- Lecture 1.

  Topic Covered in Last Lecture(04 June 2015):

  Security Architecture

  Security Attacks

  Security Services

- Lecture 2-3.

  Today's Topic:

  Model for Network Security

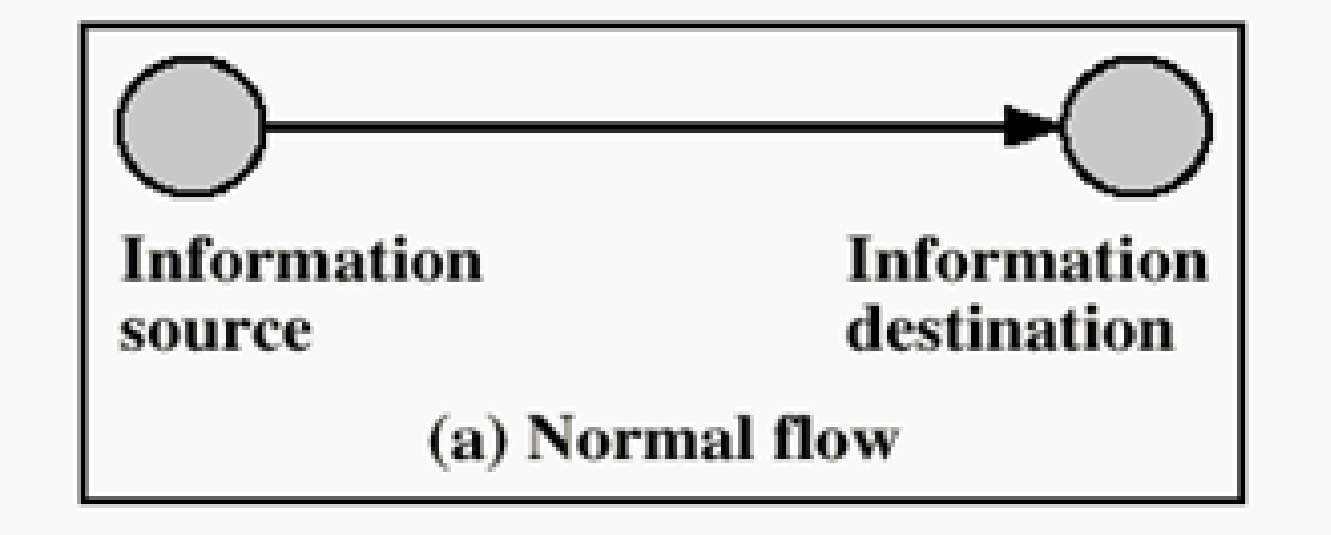
  Basic terms used in Cryptography

  Symmetric Cipher Model

  Substitution Techniques

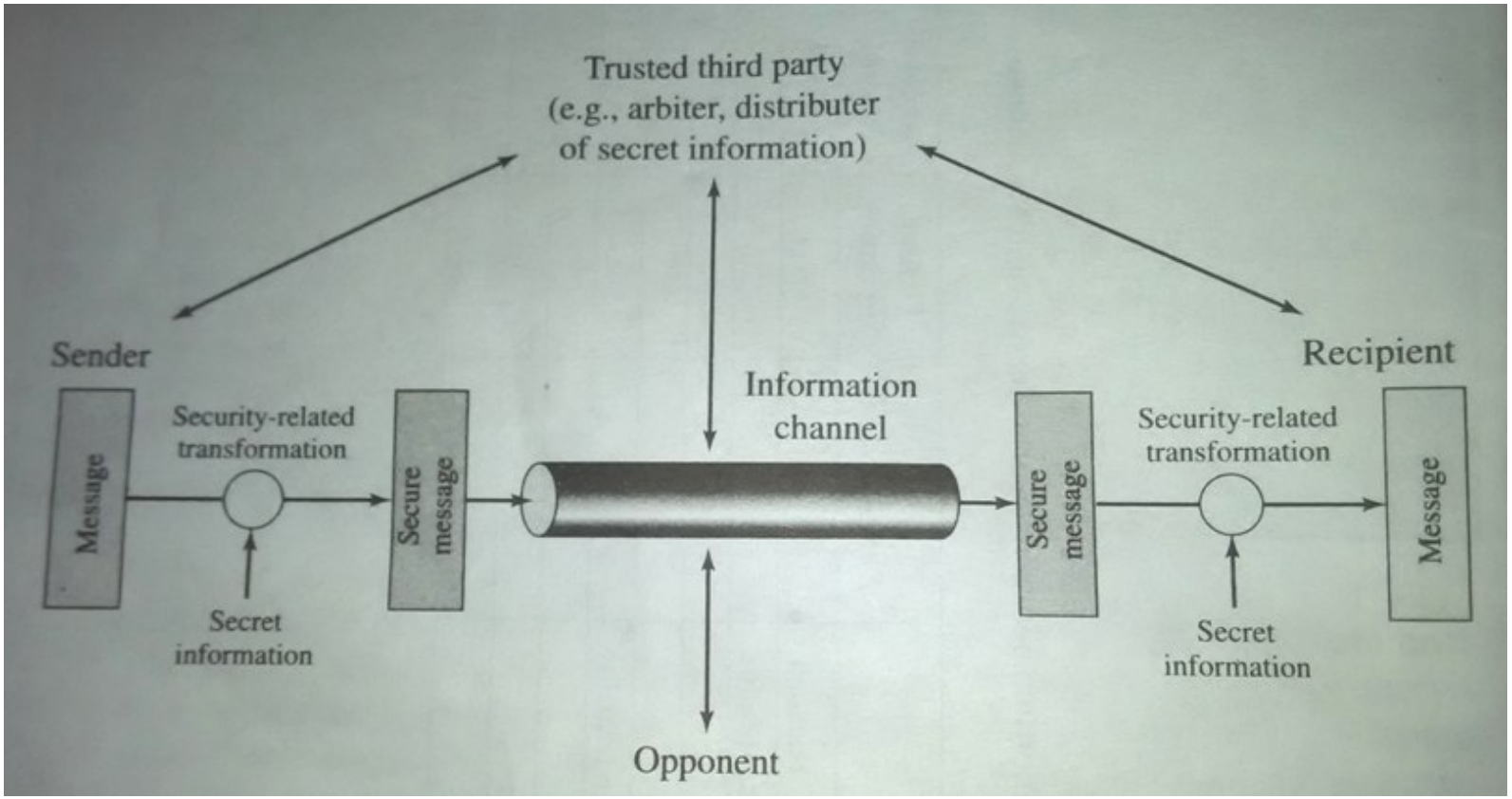
  Transpositions Techniques

- **Model for Network Security:**



1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used.(make use of security algorithm and the secret information)

- **Model for Network Security:**



- **Basic terms used in Cryptography:**

  Plaintext: Original message.

  Ciphertext: Coded message.

  Cipher: Algorithm for transforming plaintext to ciphertext.

  Key: Info used in cipher known only to sender/receiver.

  Encryption/ enciphering: Converting plaintext to ciphertext

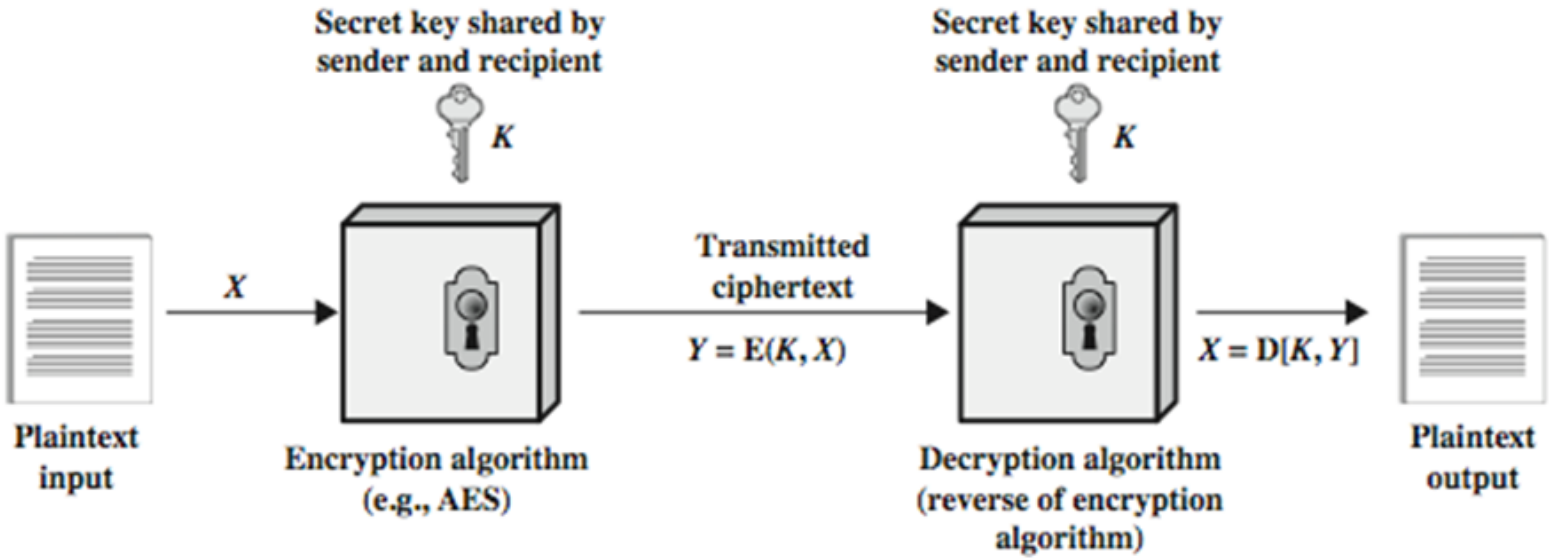
  Decryption/ deciphering: Recovering plaintext from ciphertext.

  Cryptography: Study of encryption principles/methods

  Cryptanalysis: Study of principles/methods of deciphering ciphertext without knowing key (breaking the code)

  Cryptology: The area of cryptography and cryptanalysis both.

- **Symmetric Cipher Model:**



Two requirements for secure use of symmetric encryption:

- a strong encryption algorithm
- a secret key known only to sender / receiver

Mathematically, we have:

- Y = E(K, X)
- X = D(K, Y)

- **Cryptographic systems are characterized by three independent dimensions:**

  The type of operations used for transforming plaintext to ciphertext:
  - Substitution: Each element in plaintext it mapped into another element.
  - Transposition: Elements in plaintext are rearranged.

  Number of keys used:
  - Symmetric: Both sender and receiver use the same key. (Single key/ Secret Key)
  - Asymmetric: Both sender and receiver use different keys. (Two-Key/ Public Key)

  The way in which the plaintext is processed:
  - Block Cipher: Processes the input one block of elements at a time.(Produces a block as output)
  - Stream Cipher: Processes the input elements continuously. (Produces one element as output)

- **Substitution Techniques:** It is a technique in which the letters of plaintext are replaced by other letters or by numbers or symbols.

  Caesar Cipher

  Monoalphabetic Cipher

  Playfair Cipher

  Hill Cipher

  One-Time Pad

  Vigenere Cipher

- **Substitution Techniques:**Caesar Cipher:

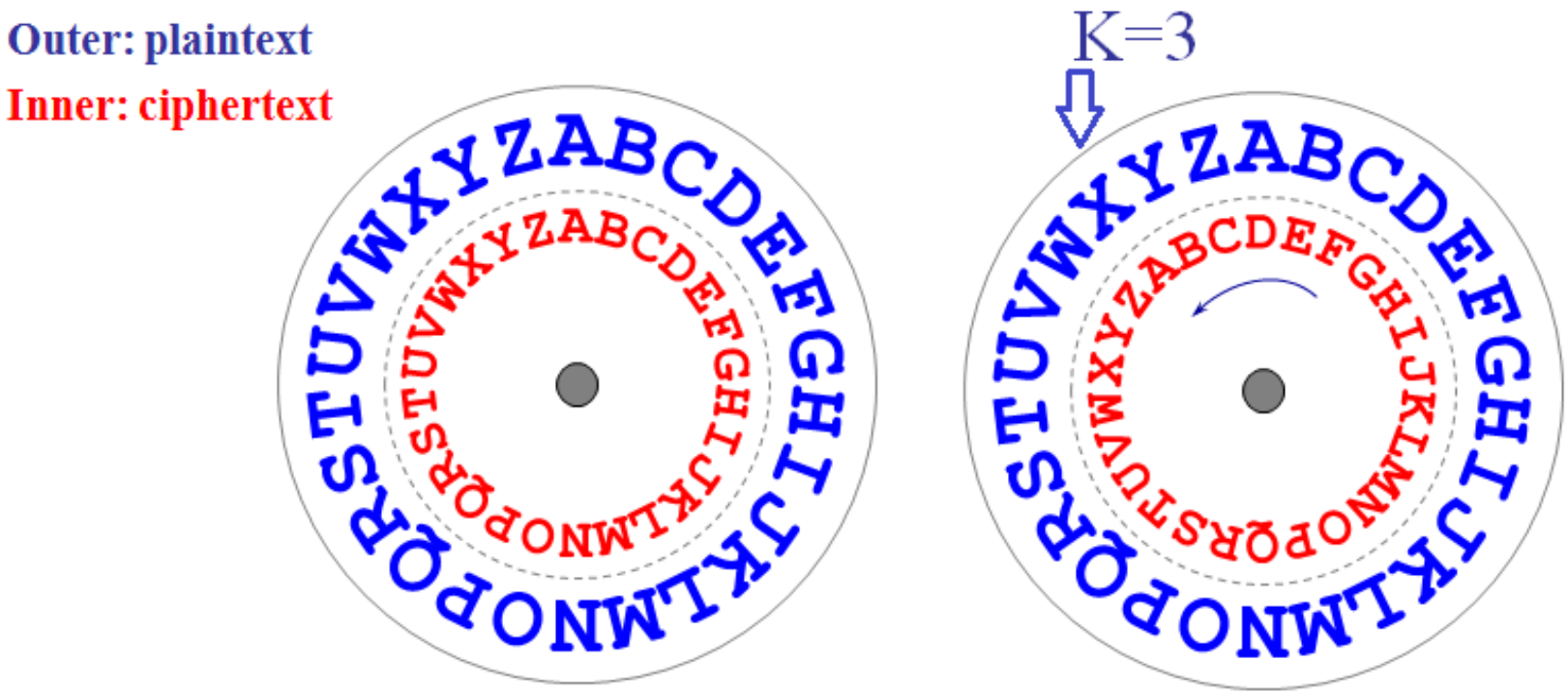
  Each letter is translated into the letter a fixed number of positions after it in the alphabet table.

  The fixed number of positions is a key both for encryption and decryption.

  For a key K=3,
  Plaintext letter: ABCDEF...UVWXYZ
  Ciphtertext letter: DEF...UVWXYZABC
  Example:
  Plaintext: IMPOSSIBLE
  Ciphtertext: LPSRVVLEOH

  Mathematically, we have:
  - $Y = E(K, X) = (X + K) \pmod{26}$
  - $X = D(K, Y) = (Y - K) \pmod{26}$

- **Substitution Techniques:** Caesar Cipher:



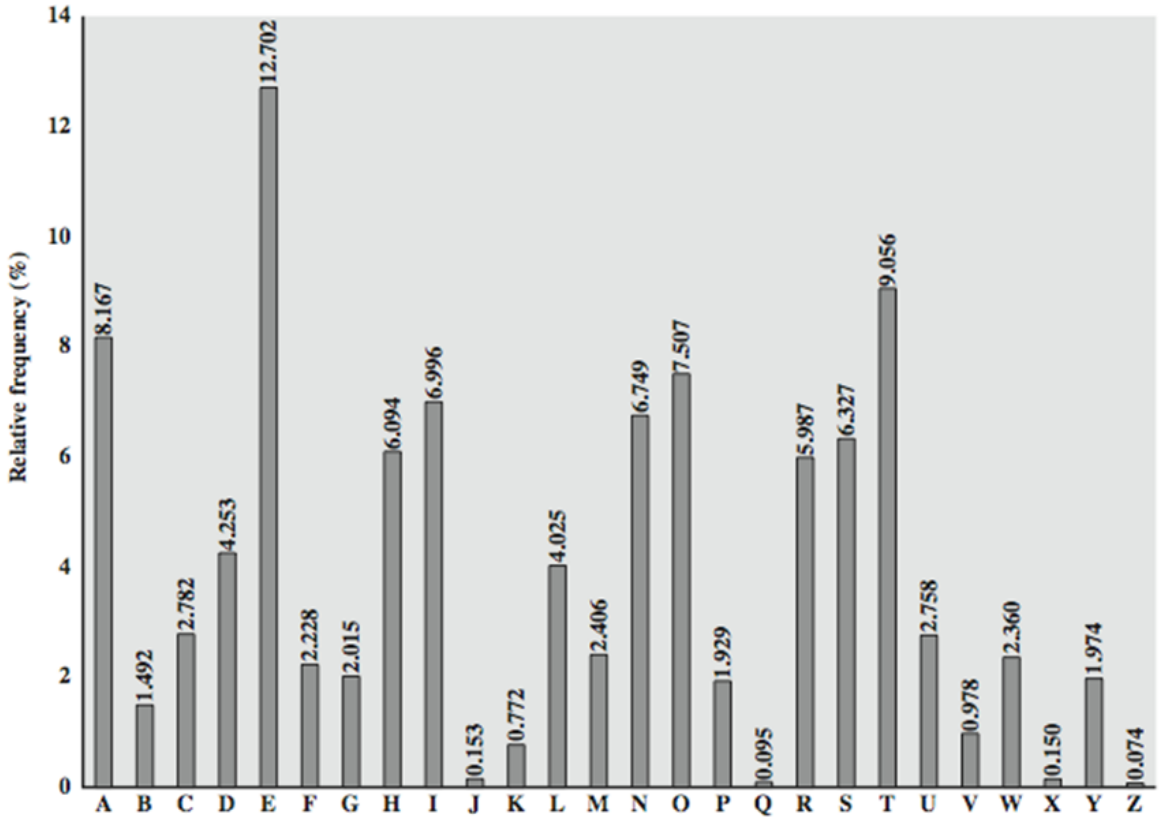
- **Substitution Techniques:**Caesar Cipher:
- Cryptanalysis of Caesar Cipher:

  Only have 26 possible ciphers−− >A maps to A,B,..Z−− >could simply try each in turn a brute force search−− >given ciphertext, just try all shifts of letters.

  Example 1: "welcome to jodhpur" with key=5, converted into "bjqhtrj yt otimuzw"

  Home work: "This is jodhpur national university" with key=4, converted into "xlmw mw nshltyv rexmsrep yrmzivwmxc"

- **Substitution Techniques:**Monoalphabetic Cipher:
  The cipher line can be any permutation of the 26 alphabetic characters. there are 26! or greater than $4x10^{26}$ possible keys.
  A single cipher alphabet(mapping from plain alphabet to cipher alphabet) is used per message.
  But Problem is language characteristics



- **Substitution Techniques:**Monoalphabetic Cipher:

  Example 1: "welcome to jodhpur" with key=ISYVKJRUXEDZQMCTPLOFNBWGAH, converted into "wkzycqk fc ecvutnl".

  Home work: Encryption of "hide the gold" with key=ISYVKJRUXEDZQMCTPLOFNBWGAH would be "uxvk fuk rczv".

- **Substitution Techniques:**Playfair Cipher:
  Not even the large number of keys in a Monoalphabetic cipher provides security.
  One approach to improving security was to encrypt multiple letters.
  Treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams.
  Based on the use of a 5x5 matrix of letters constructed using a keyword.
  The rules for filling in this 5x5 matrix are: L to R, top to bottom, first with keyword after duplicate letters have been removed, and then with the remain letters, with I/J used as a single letter.
  Example: Using the keyword "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

- **Substitution Techniques:**Playfair Cipher: Working

  If a pair is a repeated letter, insert a filler like 'X', eg. "balloon" encrypts as "ba lx lo on".

  If both letters fall in the same row, replace each with letter to right (wrapping back to start from end), eg. "AR" encrypts as "RM".

  If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. "MU" encrypts to "CM".

  Otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. "HS" encrypts to "BP", and "EA" to "IM" or "JM" (as desired).

  Example 1: "welcome to jodhpur" is converted into "ug ue no kl af rh fv zm"

  Home work: Encryption of "hide the gold" with the key of "hello world" would be "LF GE MW DN WO CV".

- **Substitution Techniques:**Hill Cipher:

  It is another multi-letter cipher

  The encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters.

  Use m linear equations in which each character is assigned a numerical value (a=0, b=1, c=2,....z=25).

  For m=3, the system can be described as follows:

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

This can be expressed in term of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

or

$$\mathbf{C} = \mathbf{KP} \bmod 26$$

where **C** and **P** are column vectors of length 3, representing the plaintext and ciphertext, and **K** is a 3×3 matrix, representing the encryption key. Operations are performed mod 26.

For example, consider the plaintext "paymoremoney" and use the encryption key

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

The first three letters of the plaintext are represented by the vector $\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$. Then $\mathbf{K}\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$ = LNS. Continuing in this fashion, the ciphertext for the entire plaintext is LNSHDLEWMTRW.

- **Substitution Techniques:**Hill Cipher:

  Example 1:plaintext: "welcome to jodhpur" with key=(3 2 3 1) (key is:top row, bottom row) is converted into "wsljocyfizwtzkqz".

  Home work: Encryption of "hide the gold" with the key=(3 2 3 1) would be "ldrntmysmbdg".

- **Substitution Techniques:** One-Time Pad:

the letters would first be converted to their numeric equivalents, as shown here.

V	E	R	N	A	M	C	I	P	H	E	R
21	4	17	13	0	12	2	8	15	7	4	17

Next, we must generate random numbers to combine with the letter codes. Suppose the following series of random two-digit numbers is generated.

76 48 16 82 44 03 58 11 60 05 48 88

The encoded form of the message is the sum mod 26 of each coded letter with the corresponding random number. The result is then encoded in the usual base-26 alphabet representation.

Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Numeric Equivalent	21	4	17	13	0	12	2	8	15	7	4	17
+ Random Number	76	48	16	82	44	3	58	11	60	5	48	88
= Sum	97	52	33	95	44	15	60	19	75	12	52	105
= mod 26	19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b

Thus, the message

VERNAM CIPHER

is encoded as

tahrsp itxmab

Homework: Formulate the decryption process.

- **Substitution Techniques:**Vigenere Cipher:

  The Vigenere Cipher is a substitution cipher.

  The Vigenere Cipher uses the table to encipher the plaintext.

  To encipher a message, repeat the key above the plaintext.

  Example 1:plaintext: "welcome to jodhpur" with key= "welcome" is converted into "siwecyipsuqrttqv".
  T: welcometojodhpur
  K: welcomewelcomewe
  C: siwecyipsuqrttqv

  Home work:Encryption of "hide the gold" with the key of "helloworld" would be "omophdsxzok".

- **Substitution Techniques:** Vigenere Cipher: vigenere table

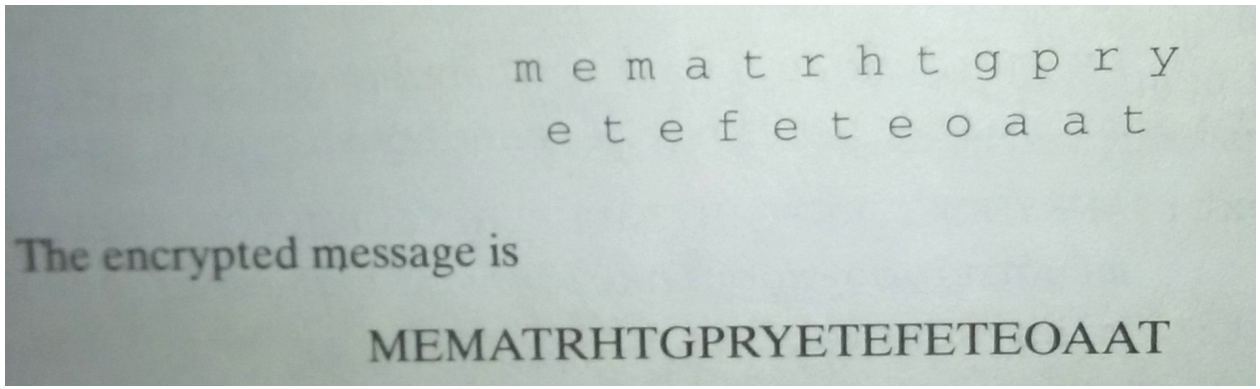
TABLE 2-1 Vigenère Tableau.

	0					5					10					15					20					25	
	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*	*m*
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	0
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	1
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	2
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	3
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	4
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	5
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	6
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	7
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	8
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	9
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	10
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	11
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	12
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	13
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	14
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	15
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	16
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	17
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	18
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	19
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	20
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	21
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	22
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	23
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	24
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	25

- **Transposition Techniques:**Elements in plaintext are rearranged OR Perform some sort of permutation on the plaintext letters.

  Rail Fence Cipher: Write message letters out diagonally over a number of rows then read off cipher row by row.

  Example: write message out as: "meet me after the toga party".



  Home work:plaintext: "welcome to jodhpur" with key=3 is converted into "woohecmtjdprleou".

  Home work:plaintext: "welcome to jodhpur" with key=5 is converted into "woetjrleoucmdpoh".

- **Rotor Machines:**

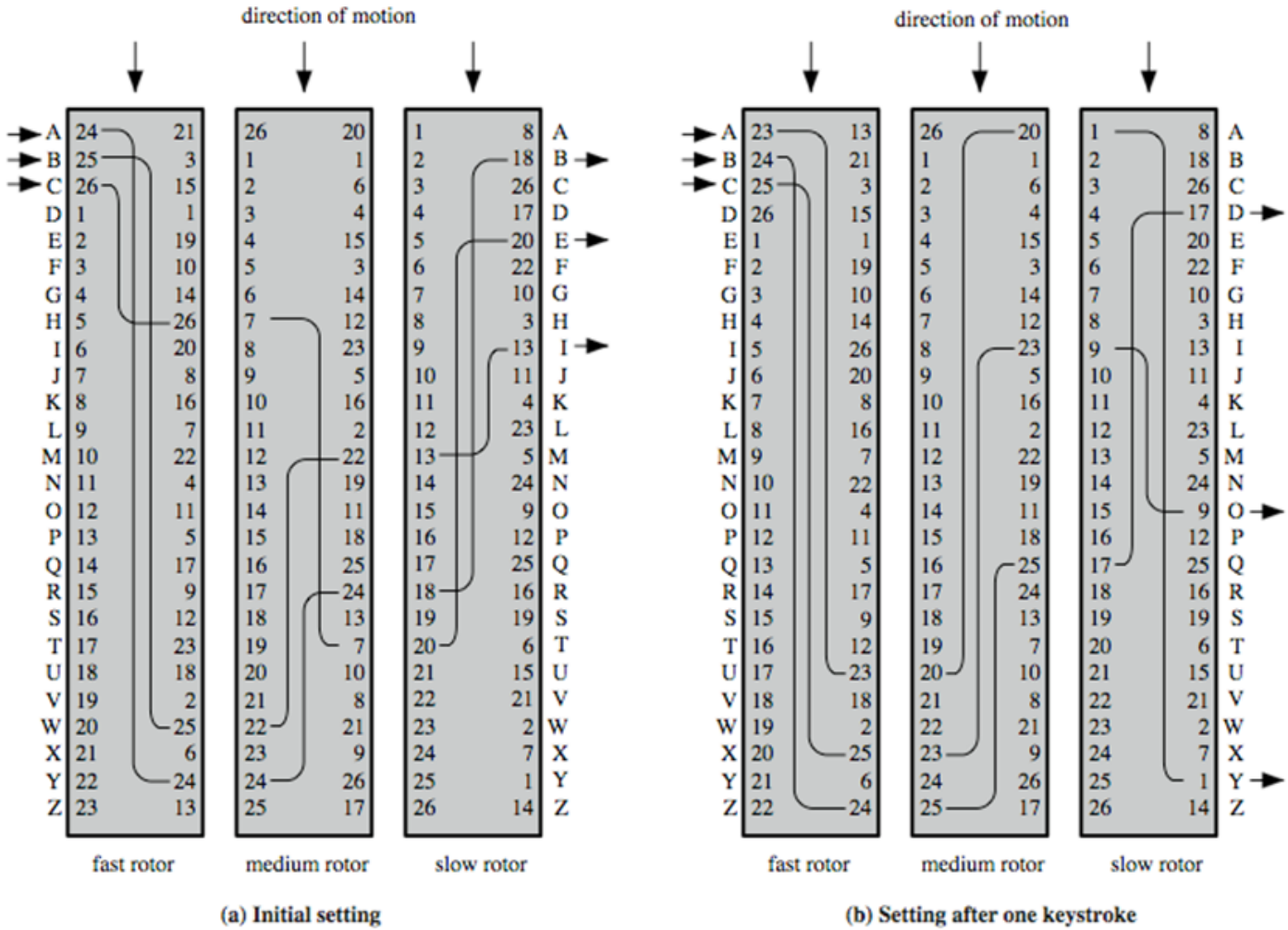
  The basic principle of the rotor machine:The machine consists of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin.

  If an operator depresses the key for the letter A, an electric signal is applied to the first pin of the first cylinder and flows through the internal connection to the twenty-fifth output pin.

  For every complete rotation of the inner cylinder, the middle cylinder rotates one pin position. Finally, for every complete rotation of the middle cylinder, the outer cylinder rotates one pin position.

  The result is that there are 26 x 26 x 26 = 17,576 different substitution alphabets used before the system repeats.

Rotor Machines:



(a) Initial setting

(b) Setting after one keystroke

- **Steganography:**

  Steganography is an alternative to encryption which hides the very existence of a message by some means.

  Hides existence of message by:
  Using only a subset of letters/words in a longer message marked in some way
  Using invisible ink
  Hiding in text in graphic image or sound file

  Steganography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information.