Basic Terminologies

- **Plain Text :** Data that can be read and understand without any special measure(original message).
- **Cipher Text:** Data that is transformed or converted by Encryption algorithm(coded message).
- **Encryption:** Algorithm for transforming plain text to cipher text.
- **Decryption:** Algorithm for transforming cipher text to plain text.
- **Key:** It is used for encryption and decryption of message.
- **Cryptography:** It is the science of using mathematics to encrypt and decrypt data

Objectives of Cryptography

- Confidentiality
- Integrity
- Non repudiation
- Authentication

Cont….

- **Confidentiality**
  - The protection of data from unauthorized disclosure.
  - Confidentiality is the protection of transmitted data from passive attacks
- **Integrity**
  - The assurance that data received are exactly as sent by authorized entity
  - Data integrity is the protection of transmitted data from active attacks

Cont. …

- **Non-repudiation**
  - Non-repudiation prevents either sender or receiver from denying a transmitted message.
- **Authentication**
  - It is concerned with assuring that a communication is authentic, i.e. assure the recipient message is from the source that it claims to be.

Types of Cryptography

- **Followings are the Types of Cryptography:**
  - Symmetric cipher
  - Asymmetric cipher

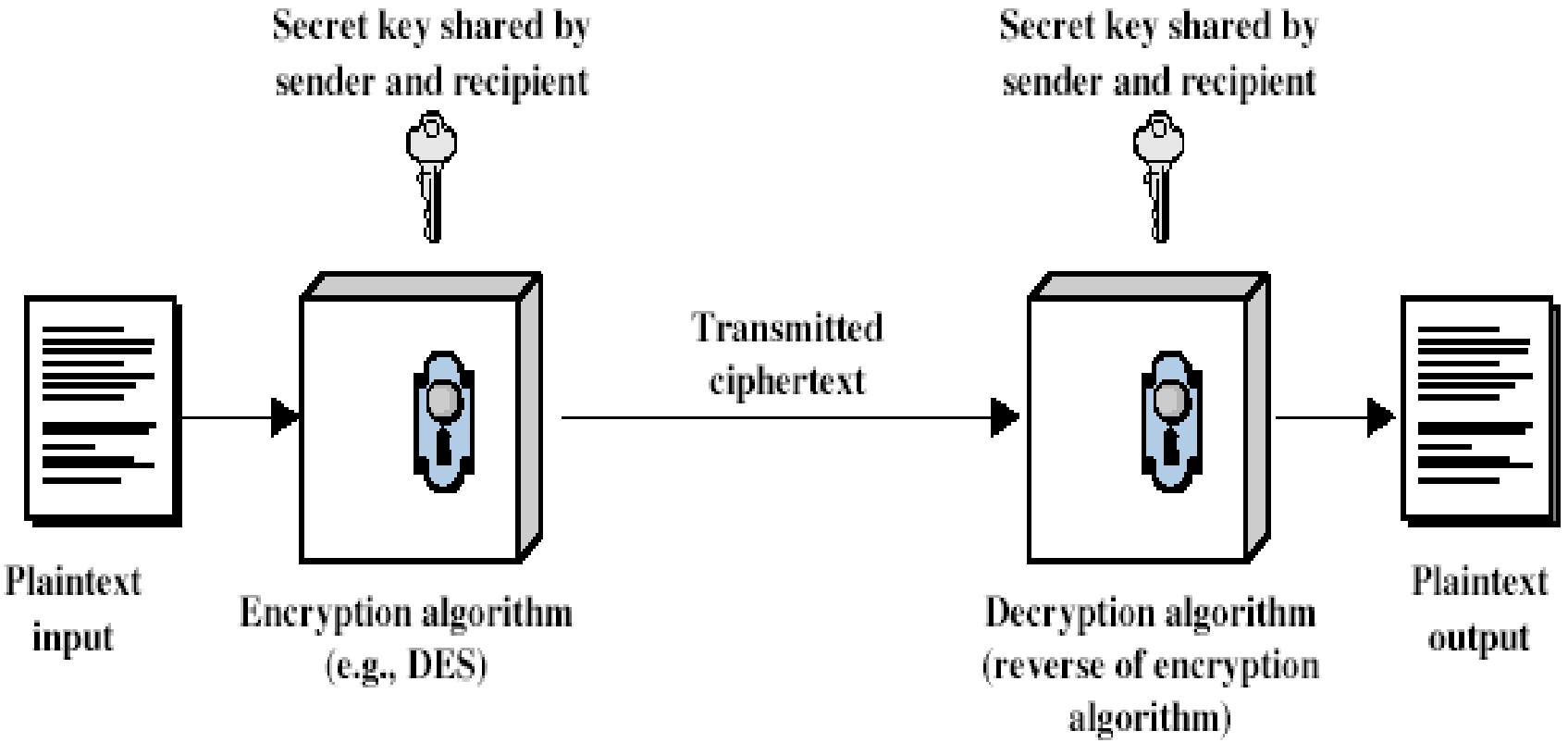
Cont….

- **VIRUS:**
  - A computer virus is a malicious program that self-replicates via copying itself to another program. In different phrases, the computer
  - virus spreads with the aid of itself into other executable code or documents.
  - Almost all viruses are connected to an executable document, which means the virus may also exist on your pc but it surely cannot infect your computer unless you run or open the malicious program.
  - It is important to note that a virus cannot be spread without a human action(such as running an infected program).

Symmetric cipher

- Both sender and receiver use single same key for Encryption and Decryption
- It is also known as Conventional Cryptography/Secret Key /Private Key
- Example :DES

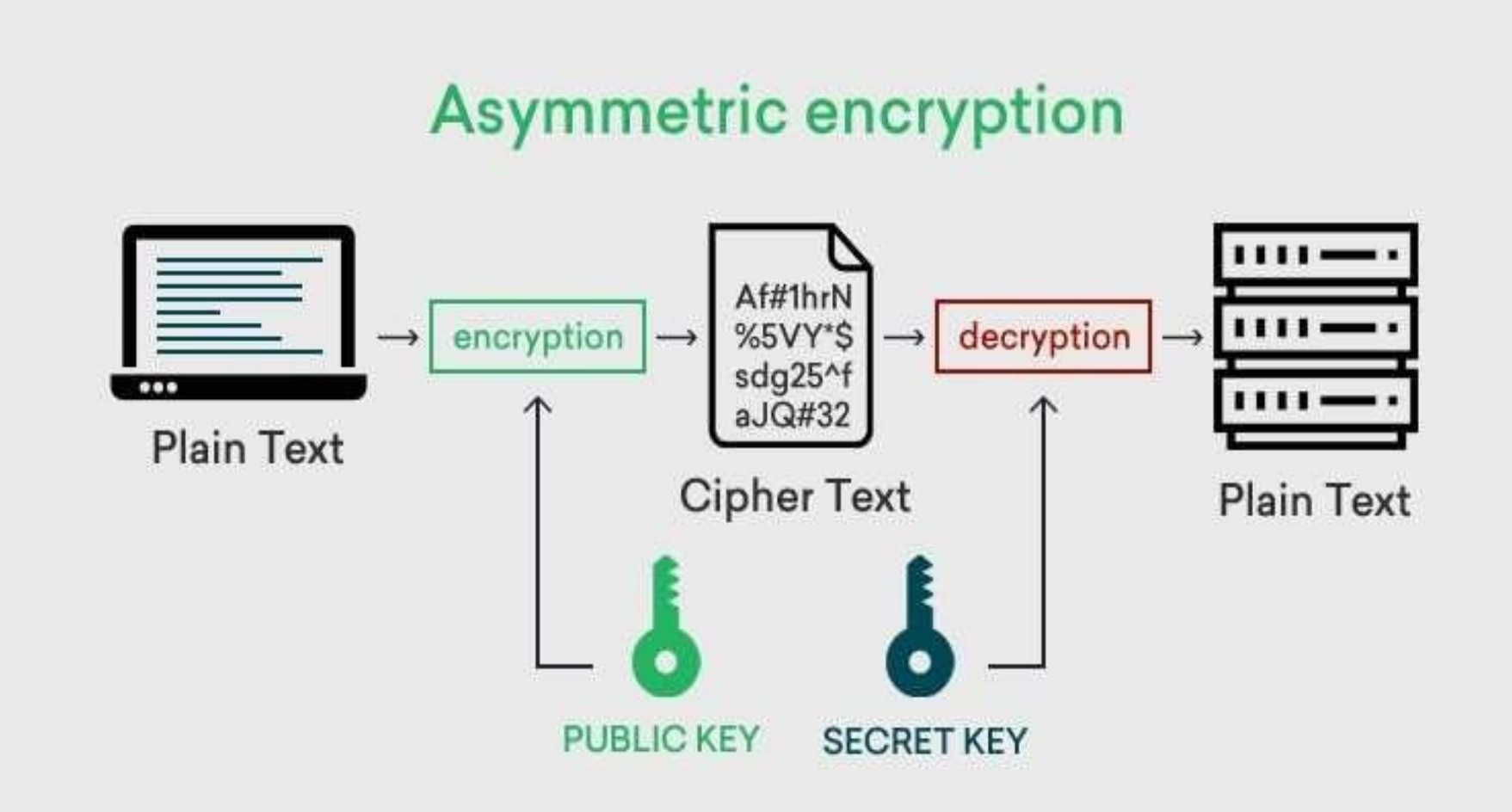
Symmetric Cipher Model



Asymmetric Cipher Model

- **Asymmetric cryptography,** also known as public-key cryptography.
- It is a process that uses a pair of related keys one public key and one private key to encrypt and decrypt a message and protect it from unauthorized access or use.
- **A private key** also known as a secret key is shared only with key's initiator.
- **Example:** RSA algorithm

Asymmetric Cipher Model



Encryption Algorithm

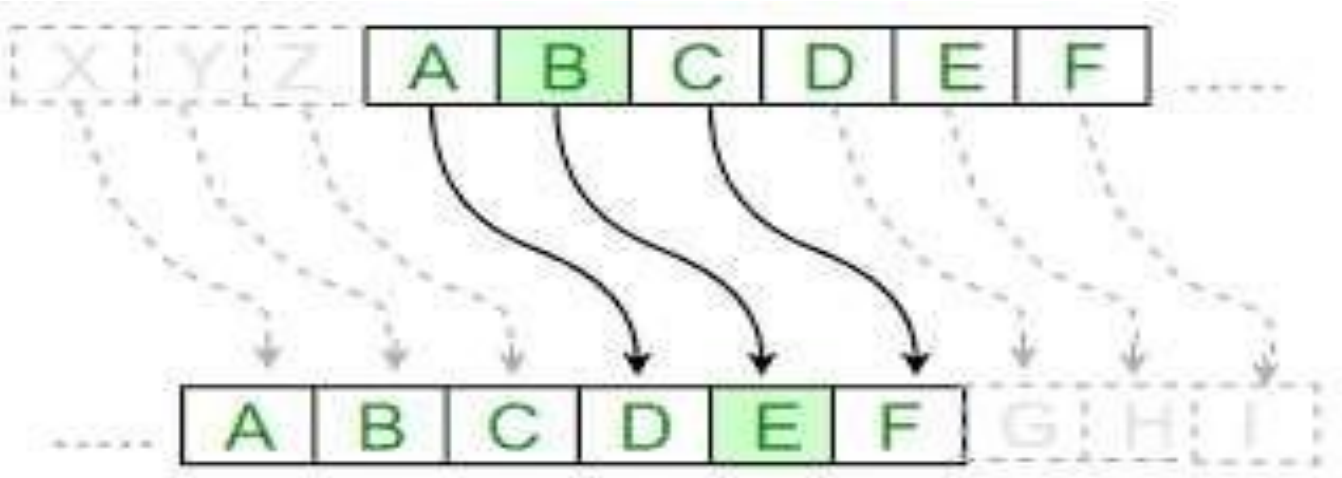
- **Type of operation used**
  1. Substitution : Elements of plaintext are mapped into another element
  2. Transposition : Elements of plaintext are rearranged
- **Some of the Substitution Techniques are**
  - Caesar cipher
  - Playfair cipher
  - Hill cipher
  - Vigenere cipher (Auto-key system)
  - Vernam cipher or One time pad

Caesar cipher

- In cryptography, a Caesar cipher, also known as a Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques.
- It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 2, A would be replaced by C, B would become D, and so on.
- **For Encryption,** $C=E(P)=(P+K) \bmod 26$
- **For Decryption,** $P=D(C)=(C-k) \bmod 26$

Cont….

- **Example of Caesar cipher:**

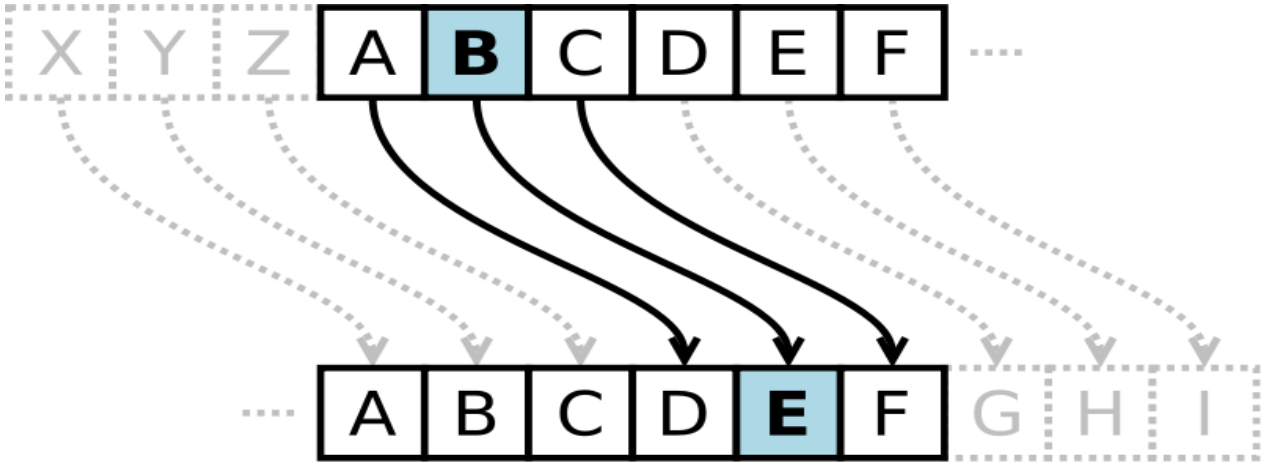


Cont….

- **Example of Caesar cipher:**
- **Plain text** :: meet me after
- Key :: 3
- **Cipher text** :: phhw ph diwhu
- **EX.**
  - **Plain text** :: Good morning friends welcome to piet
  - Key :: 4

Caesar Cipher

- In cryptography, a **Caesar cipher**, also known as a **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most widely known encryption techniques.
- It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- For example, with a shift of 3, A would be replaced by D, B would become E, and so on.



Caesar Cipher (Conti…)

- The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.
- Encryption of a letter by a shift *n* can be described mathematically as

$$E_n(x) = (x + n) \mod 26.$$

- Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

PLAYFAIR CIPHER

- The Playfair cipher uses a 5 by 5 table containing a key word or phrase.
- To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order
- To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD", and map them out on the key table.

RULES

- If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.

- If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).

- If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).

- If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same **row** as the first letter of the plaintext pair.

EXAMPLE(5x5 MATRIX)

- Key phrase: KEYWORD

K	E	Y	W	O
R	D			

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

EXAMPLE

- Plain text: why don’t you
- WH YD ON TY OU

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

- Cipher text: YI EA ES VK EZ

EXAMPLE

- Plain text: IMPOSSIBLE
- IM PO SS IB LE
- Regrouping: IM PO SX SI BL EX

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

- Cipher text: QF YS ZQ LQ IC UW
- Plain text : IM PO SX SI BL EX

Transposition techniques

- **Transposition techniques** systematically transpose the position of plaintext elements.

- **Rail Fence Technique**
- In this technique text is written down as a sequence of diagonals and then read of as sequence of rows.

Transposition techniques (Conti…)

- Plain text: meet at five pm behind p lab.
- Written as rail fence of depth 2:

m		e		a		f		v		p		b		h		n		p		a	
	e		t		t		i		e		m		e		i		d		l		b

- Encrypted as: mea fvp bhn pae tti eme idl b

Transposition techniques (Conti…)

- With rail fence of depth 3:

- Encrypted as: mtf ebi pbe aip enl xet vmh dax

M			T			F			E			B			I			P			B		
	E			A			I			P			E			N			L			X	
		E			T			V			M			H			D			A			X

Transposition techniques (Conti…)

- A more complex scheme is to write a message in a rectangle (square matrix), row-by-row and read it off, column.
- Pain text: meet at five pm behind p lab.

m	e	e	t	a
t	f	i	v	e
p	m	b	e	h
i	n	d	p	l
a	b	x	x	x

- Encrypted text: mtpiaefmnbeibdxtvepxaehlx

Transposition techniques (Conti…)

- Alternatively, a key can also be defined to permute the order of the column, e.g. encryption key (41523) defines write in a row-by-row, read it off: 4^{th} column first, 1^{st} column second, 5^{th} column third, followed by 2^{nd} and 3^{rd} column, and prepare encrypted text.

HILL CIPHER

- This multi-letter cipher is developed by the mathematician lester hill in 1929.

- An n-gram substitution may define using an invertible nxn matrix A= aij as the key to map an n-character plaintext m1,m2,…mn to a cipher text n-gram

- $C=E_K(X)=KX \bmod 26$
- $X=D_K(C)= K^{-1}C \bmod 26$

- For n=3
- $C1= (k_{11}x_1+k_{12}x_2+k_{13}x_3) \bmod 26$
- $C2= (k_{21}x_1+k_{22}x_2+k_{23}x_3) \bmod 26$
- $C3= (k_{31}x_1+k_{32}x_2+k_{33}x_3) \bmod 26$

HILL CIPHER (Conti…)

- Example: encrypt ‘meet b’ using 2x2 hill cipher with the key k= $\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$
- $K^{-1}= \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$
- Plain text will be written as ME ET BX
- Letters with there numerical values are as follows

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

- Numerical values for plain text letters are 12 4, 4 19, 1 23

HILL CIPHER (Conti…)

- **ENCRYPTION**
- $\begin{pmatrix} c1 \\ c2 \end{pmatrix} = \begin{pmatrix} k11 & k12 \\ k21 & k22 \end{pmatrix} x \begin{pmatrix} x1 \\ x2 \end{pmatrix} \bmod 26$
- $\begin{pmatrix} c1 \\ c2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} X \begin{pmatrix} 12 \\ 4 \end{pmatrix} \bmod 26$

- C1=(36+4) mod 26 = 14 = o
- C2=(60+8) mod 26 = 16 = q
- C3=(12+19) mod 26 = 5 = f
- C4=(20+38) mod 26 = 6 = g
- C5=(3+23) mod 26 = 0 = a
- C6=(5+46) mod 26 = 25 = z
- Encrypted text is : ‘oq fg az’

HILL CIPHER (Conti…)

- **DECRYPTION**
- $\begin{pmatrix} X1 \\ X2 \end{pmatrix} = \begin{pmatrix} k11 & k12 \\ k21 & k22 \end{pmatrix} x \begin{pmatrix} C1 \\ C2 \end{pmatrix} \bmod 26$
- $\begin{pmatrix} x1 \\ x2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} X \begin{pmatrix} 14 \\ 16 \end{pmatrix} \bmod 26$

- x1=(28-16) mod 26 = 12 = m
- x2=(-70+48) mod 26 = 4 = e
- x3=(10-6) mod 26 = 4 = e
- x4=(-25+18) mod 26 = 19 = t
- x5=(0-25) mod 26 = 1 = b
- x6=(0+75) mod 26 = 23 = x
- Decrypted text is : ‘me et bx’

HILL CIPHER (Conti…)

- Encrypt a message “CIPHER” using 3x3 hill cipher with key=[{2,1,1}, {1,1,2}, {1,0,-2}]

- K= 2 1 1
- 1 1 2
- 1 0 -2

- K^{-1}= 2 -2 -1
- -4 5 3
- 1 -1 -1

- Pain text: CIP HER
- Cipher text: BOY JIP

VIGENERE CIPHER

- In a Caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E and so on.
- The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values.
- To encrypt, a table of alphabets can be used, termed a tabula recta, *Vigenère square*, or *Vigenère table*
- It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.

VIGENERE CIPHER (Conti…)

- Plain text: ATTACKATDAWN
- Key: LEMON

A	T	T	A	C	K	A	T	D	A	W	N
L	E	M	O	N	L	E	M	O	N	L	E

	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

- Cipher text :LXFOPVEFRNHR

VIGENERE CIPHER (Conti…)

- Plaintext: information security
- Key: confidential
- Encryption: KBSTZPEGBWNDGQHWQWC

- Plaintext: crypto is for cryptography
- Key: abcdef
- Encryption: CSASXTITHRVHRZRWSLRBRKC

VIGENERE CIPHER (Conti…)

- Vigenère can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25, and addition is performed modulo 26, then Vigenère encryption can be written,

$$C_i \equiv (P_i + K_i) \pmod{26}$$

- Decryption

$$P_i \equiv (C_i - K_i) \pmod{26}$$

VERNAM CIPHER

- Gilbert vernam in 1918 devised a system that works on binary data rather than letters.

Encryption : $c_i = m_i \oplus k_i \qquad i = 1,2,3,...$

m_i : plain-text bits.

k_i : key (key-stream) bits

c_i : cipher-text bits.

Decryption : $m_i = c_i \oplus k_i \qquad i = 1,2,3,...$

- Vernam proposed the use of running tape that eventually repeated the key, so that the system can work with a very but repeating keys

ONE-TIME PAD

- Major joseph mauborgne-an army signal corp. officer, invented it by proposing improvement in vernam cipher.
- A one-time pad (OTP) is a large no repeating set of truly random key letters, written on sheet of paper, and glued together in a pad.
- The sender uses each key letter on the pad to encrypt exactly one plain text character.
- The sender encrypts the message and then destroys the used pages of the pad.
- The receiver has an identical pad and uses each letter on the pad, in turn, to decrypt each letter of cipher text.
- The receiver destroys the same used pages of the pad after decrypting the message.
- It produces random output that bears no statistical relationship to the plaintext so there is no way to break the code.