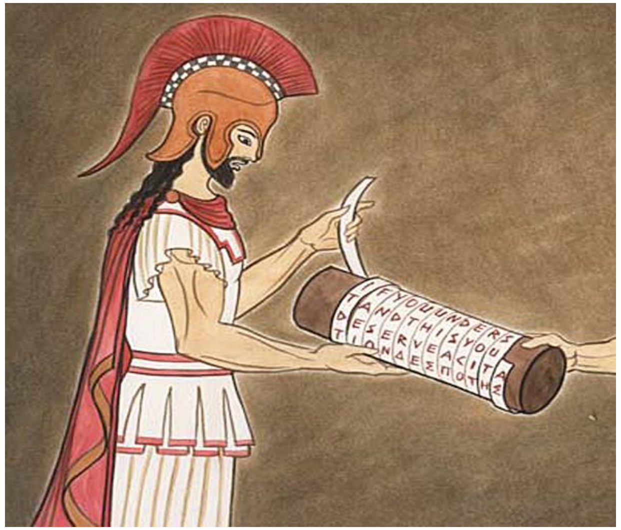
Alberti Disc

The Enigma Rotor machine

Classical Encryption Techniques

Scytale



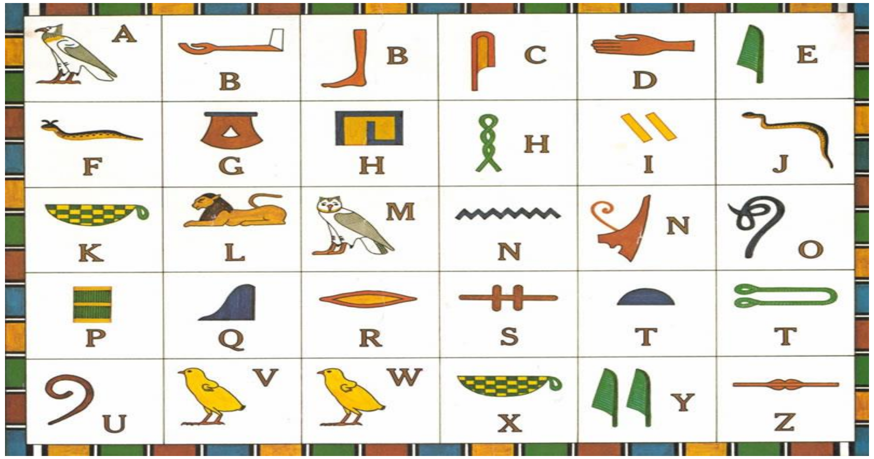
Mukesh Chinta

Assistant Professor

Department of CSE

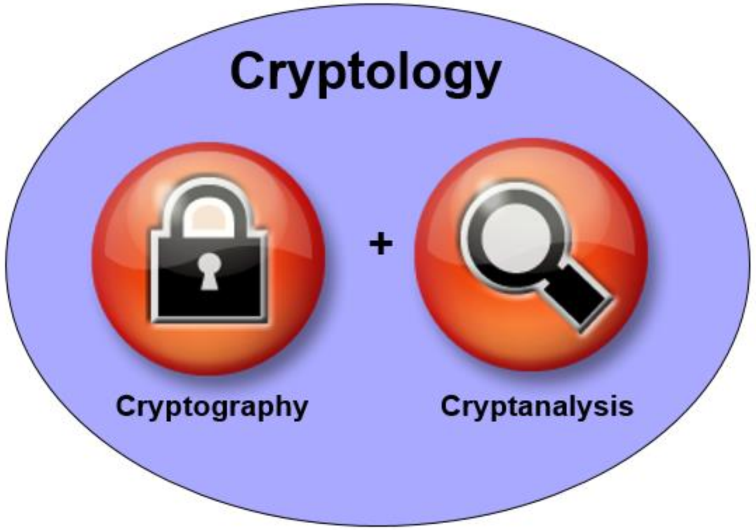
VRSEC

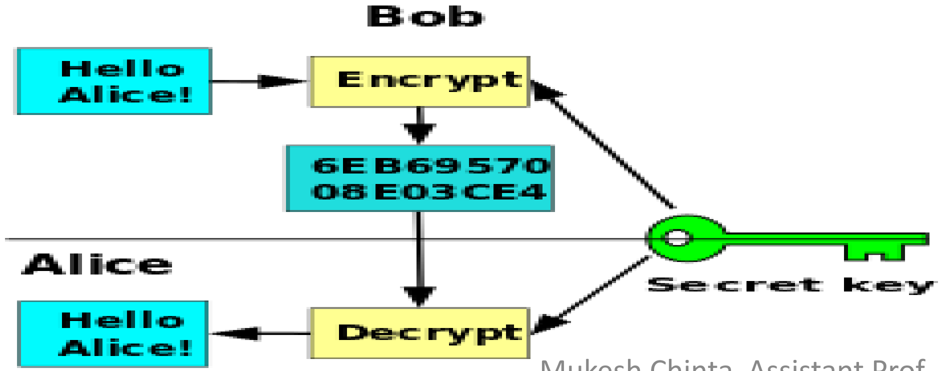
Hieroglyphics

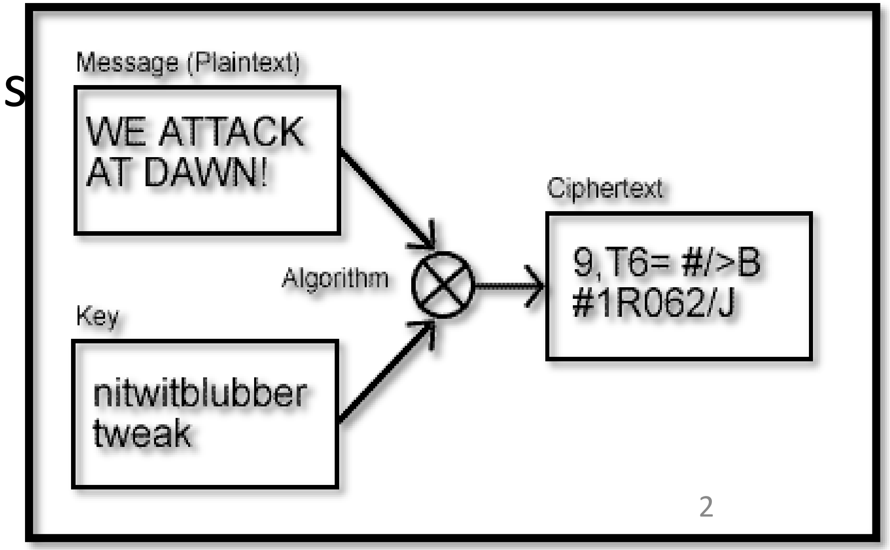


Basic Terminology

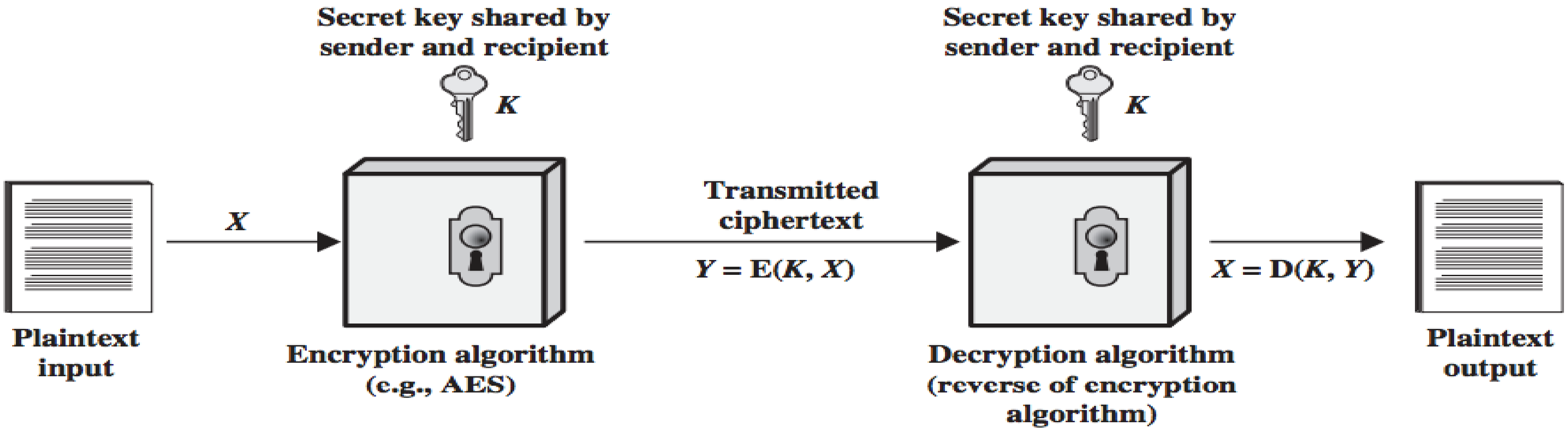
- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis







Symmetric encryption Model


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

1. ***Plain Text***: This is the original message or data which is fed into the algorithm as input.
2. ***Encryption Algorithm***: This encryption algorithm performs various substitutions and transformations on the plain text.
3. ***Secret Key***: The key is another input to the algorithm. The substitutions and transformations performed by algorithm depend on the key.
4. ***Cipher Text***: This is the scrambled (unreadable) message which is output of the encryption algorithm. This cipher text is dependent on plaintext and secret key. For a given plaintext, two different keys produce two different cipher texts.
5. ***Decryption Algorithm***: This is the reverse of encryption algorithm. It takes the cipher text and secret key as inputs and outputs the plain text.

Two main requirements are needed for secure use of conventional encryption:

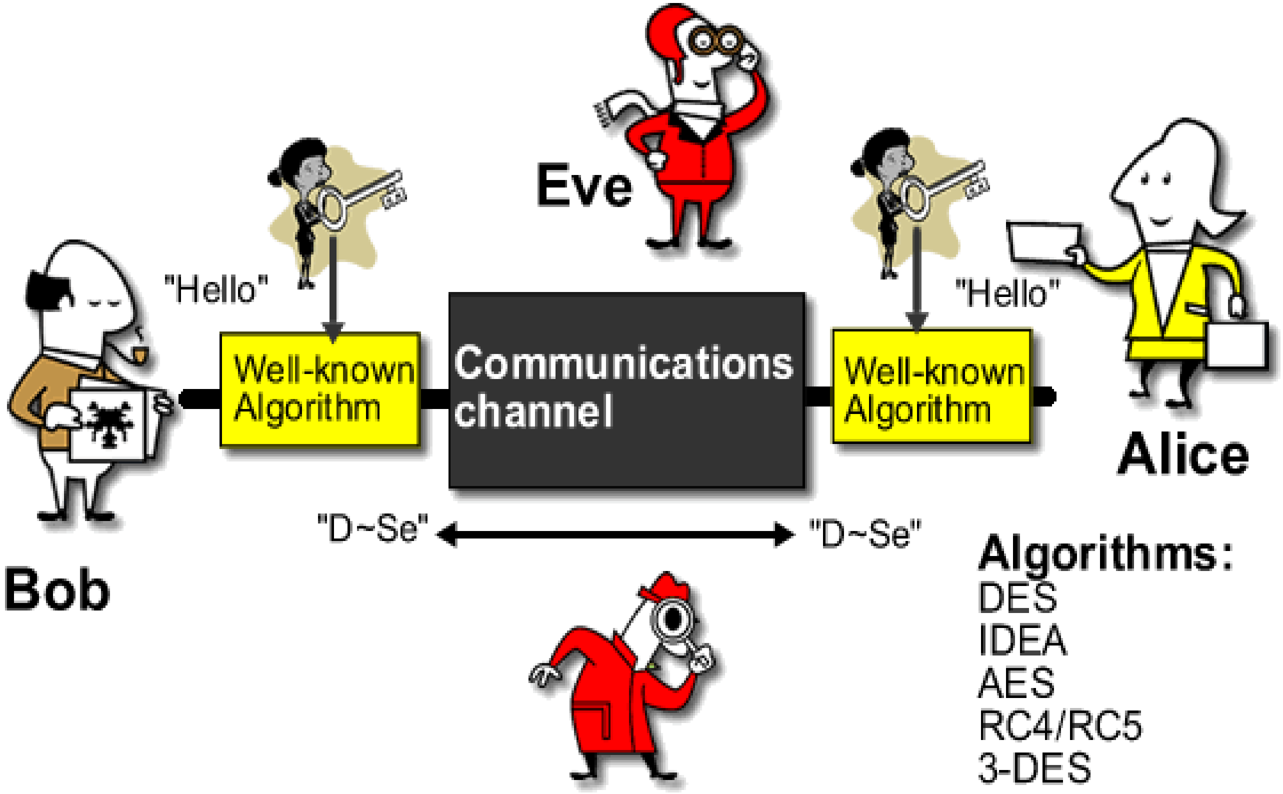
- A strong encryption algorithm is needed. It is desirable that the algorithm should be in such a way that, even the attacker who knows the algorithm and has access to one or more cipher texts would be unable to decipher the ciphertext or figure out the key.
- The secret key must be distributed among the sender and receiver in a very secured way. If in any way the key is discovered and with the knowledge of algorithm, all communication using this key is readable.

$$Y = E(K, X)$$

This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key.

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D(K, Y)$$



Algorithms:
DES
IDEA
AES
RC4/RC5
3-DES

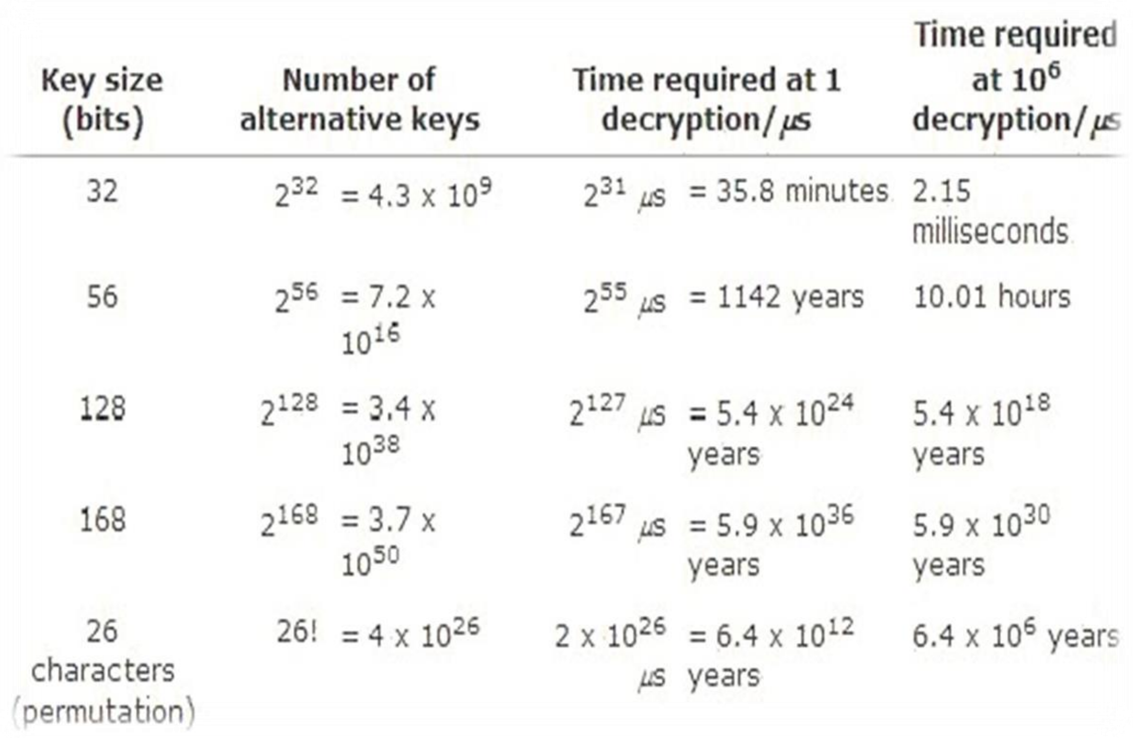
Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Cryptographic systems are classified along three independent dimensions:

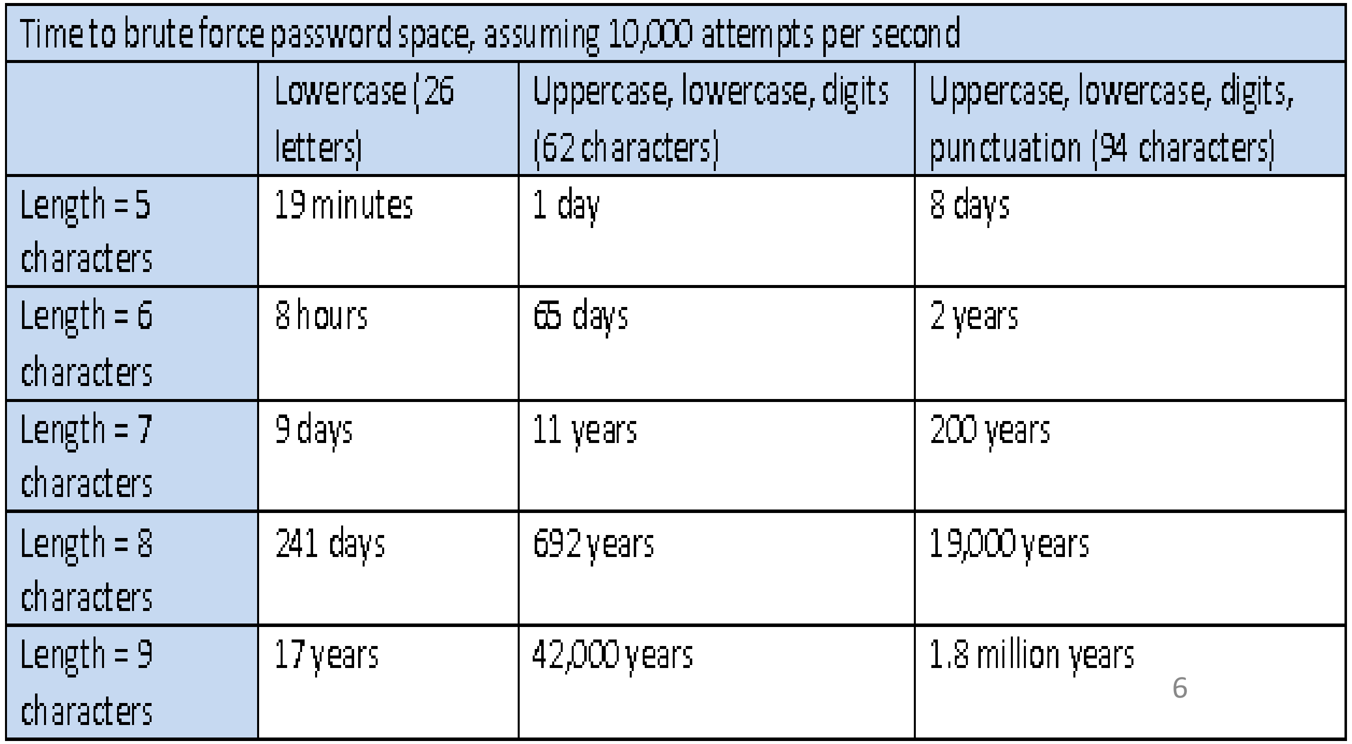
- ***The type of operations used for performing plaintext to ciphertext***
  - ❖**Substitution**: Method by which units of plaintext are replaced with ciphertext according to a regular system.
  - ❖**Transposition**: Here, units of plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged.
- ***The number of keys used***
  - ❖If single key is used by both sender and receiver, it is called **symmetric**, single-key, secret-key or conventional encryption
  - ❖If sender and receiver each use a different key, then it is called **asymmetric**, two-key or public-key encryption.
- ***The way in which plaintext is processed***
  - ❖A **block cipher** process the input as blocks of elements and generated an output block for each input block.
  - ❖**Stream cipher** processes the input elements continuously, producing output one element at a time as it goes along.

Cryptanalysis

- **The process of attempting to discover the plaintext or key is known as cryptanalysis.** It is very difficult when only the ciphertext is available to the attacker as in some cases even the encryption algorithm is not known.
- The most common attack under these circumstances is the **brute-force** approach of trying all the possible keys. This attack is made impractical when the key size is considerably large.



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

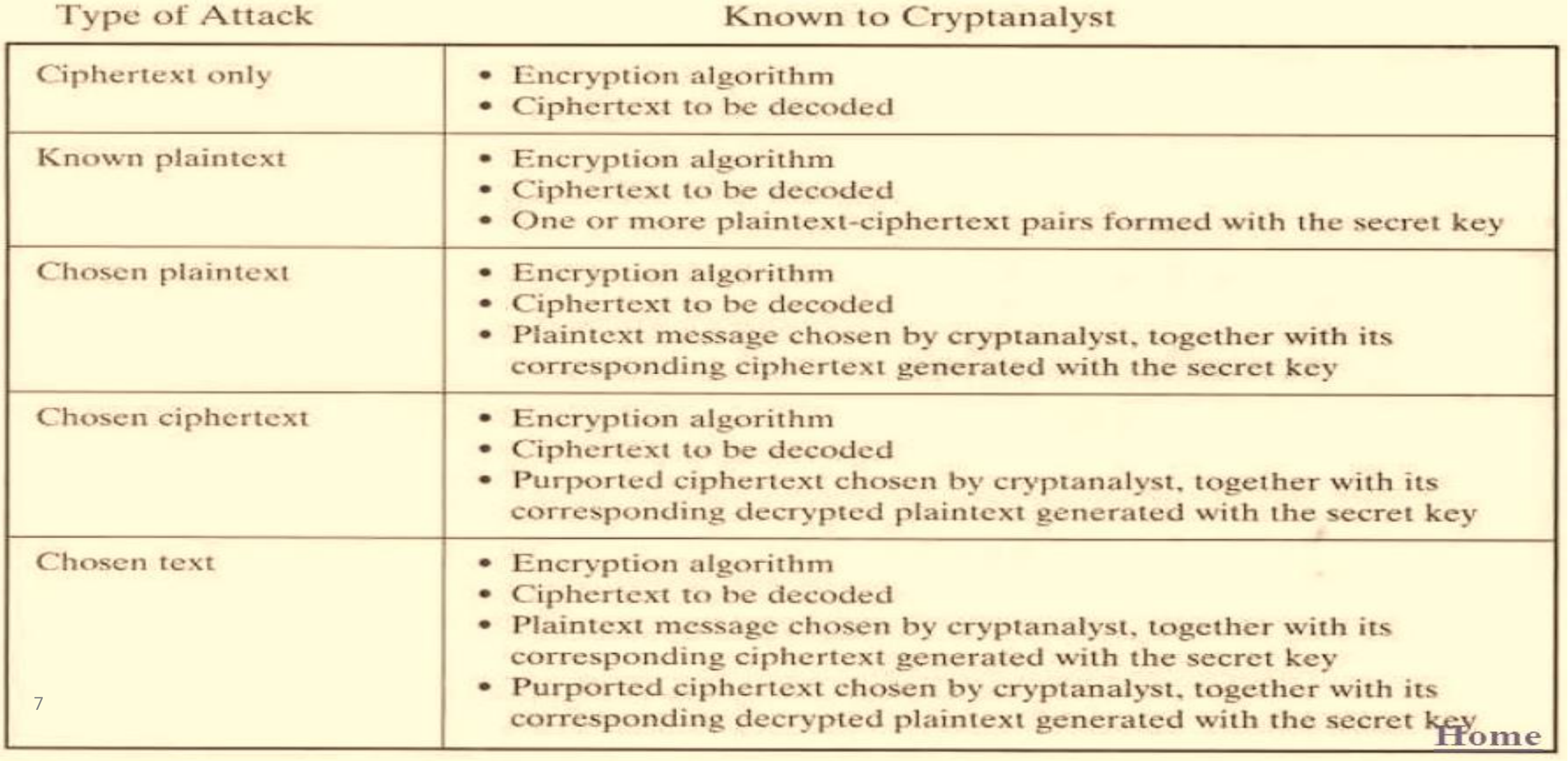


Time to brute force password space, assuming 10,000 attempts per second

	Lowercase (26 letters)	Uppercase, lowercase, digits (62 characters)	Uppercase, lowercase, digits, punctuation (94 characters)
Length = 5 characters	19 minutes	1 day	8 days
Length = 6 characters	8 hours	65 days	2 years
Length = 7 characters	9 days	11 years	200 years
Length = 8 characters	241 days	692 years	19,000 years
Length = 9 characters	17 years	42,000 years	1.8 million years

Attacks on Encrypted Messages

Cryptanalytic attacks may be classified by how much information needed by the attacker



Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext to be decoded
Known plaintext	• Encryption algorithm • Ciphertext to be decoded • One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Encryption algorithm • Ciphertext to be decoded • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Home

- An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext and time is available to the opponent. Example for this type is **One-time Pad**.
- An encryption scheme is **computationally secure** if the ciphertext generated by the scheme meets the following criteria:
  - Cost of breaking cipher exceeds the value of the encrypted information.
  - Time required to break the cipher exceeds the useful lifetime of the information.

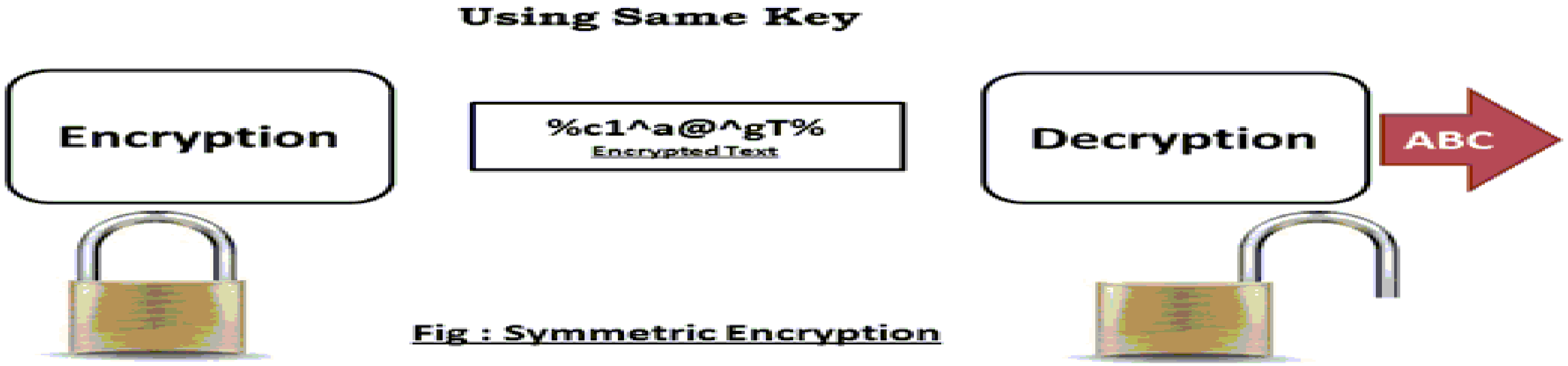


Fig : Symmetric Encryption

Substitution Encryption Techniques

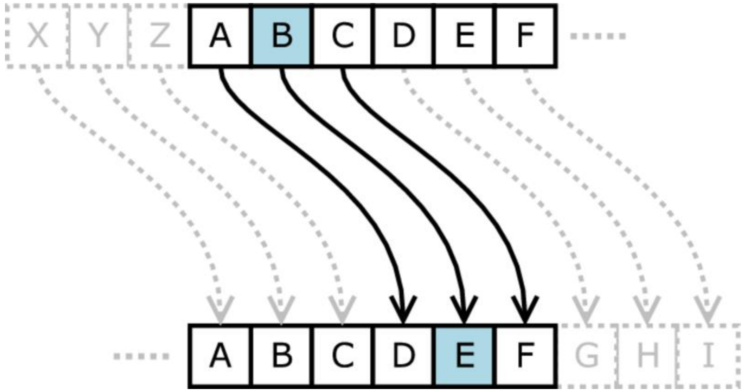
- Substitution ciphers form the first of the fundamental building blocks. The core idea is to replace one basic unit (letter/byte) with another. Whilst the early Greeks described several substitution ciphers, the first attested use in military affairs of one was by Julius Caesar, described by him in *Gallic Wars*. Hence the name **Caesar Cipher**.
- Each letter is replaced by the letter three positions further down the alphabet.

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

- example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```



- Mathematically, map letters to numbers:

```
a, b, c, ..., x,  y,  z
0, 1, 2, ..., 23, 24, 25
```

- Then the general Caesar cipher is:

$$c = \mathrm{E}_K(p) = (p + k) \bmod 26$$

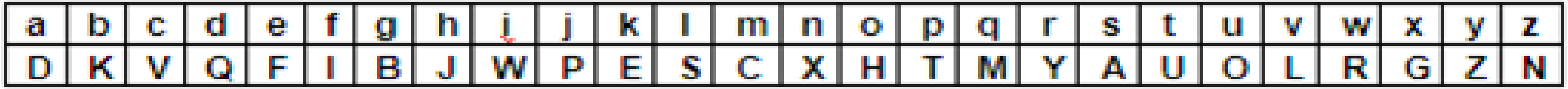
$$p = \mathrm{D}_K(c) = (c - k) \bmod 26$$

- This mathematical description uses **modulo (clock) arithmetic**. Here, when you reach Z you go back to A and start again. Mod 26 implies that when you reach 26, you use 0 instead (ie the letter after Z, or 25 + 1 goes to A or 0). Can be generalized with any alphabet.
- With only 25 possible keys, the Caesar cipher is far from secure. Brute force search can yield the key in seconds.

For Example, try to break the ciphertext "GCUA VQ DTGCM"

Mono-alphabetic Cipher

- A dramatic increase in the key space of the Caesar cipher can be achieved by a Mono-alphabetic Cipher, where the substitution alphabet can be any permutation of the 26 alphabetic characters.
- The idea is rather than just shifting the alphabet, shuffle (jumble) the letters arbitrarily generating a key space of 26! (4 x 10^{26} keys).



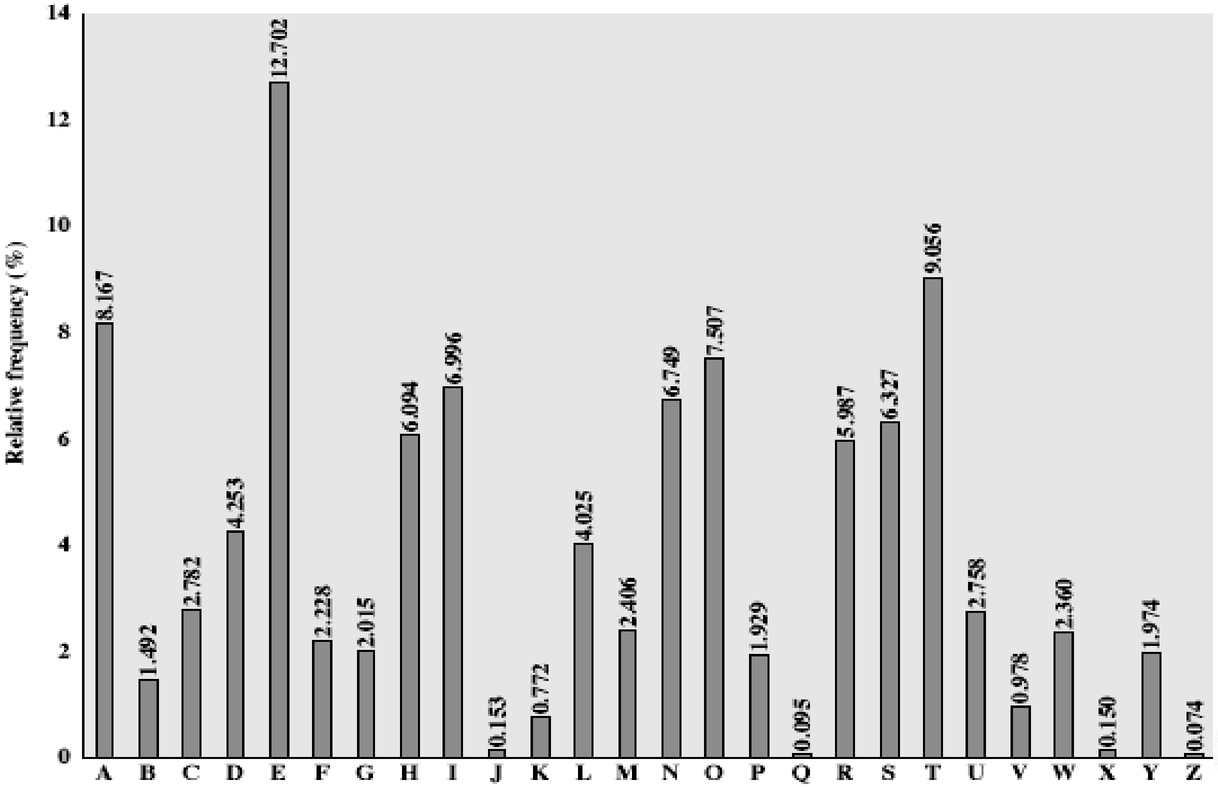
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

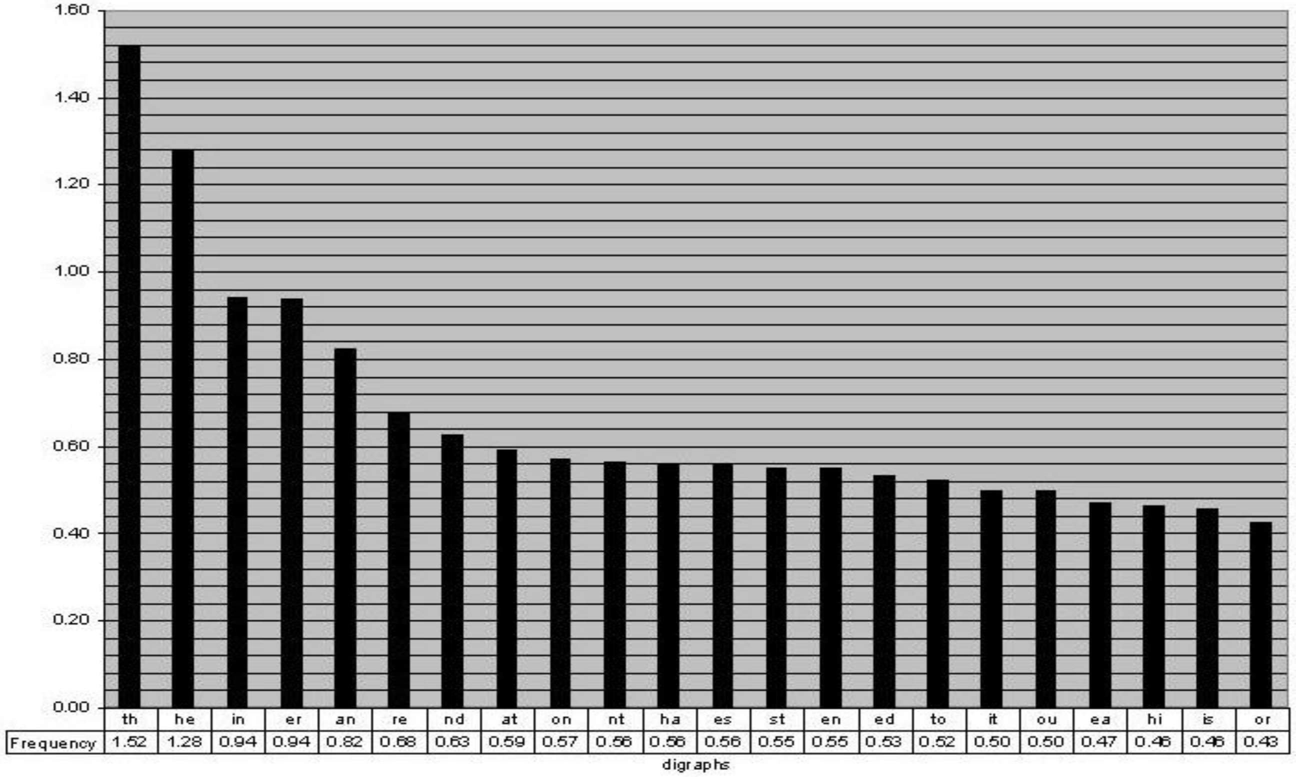
Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Now the Brute Force attack on this cipher requires exhaustive search of 26! = 4 x 10^{26} keys, but the cryptanalysis makes use of the language characteristics, the Letter that is commonly used in English is the letter ***E*** , then ***T,R,N,I,O,A,S;*** other letters are fairly rare ***Z,J,K,Q,X*** There are tables of single, double & triple letter frequencies.

- The problem with Mono-alphabetic cipher are the **language characteristics**. Human languages are not random, all the letters are not equally frequent.
- Mono-alphabetic substitution do not change relative letter frequencies, which the cryptanalysts could use and enable them to break the cipher easily.





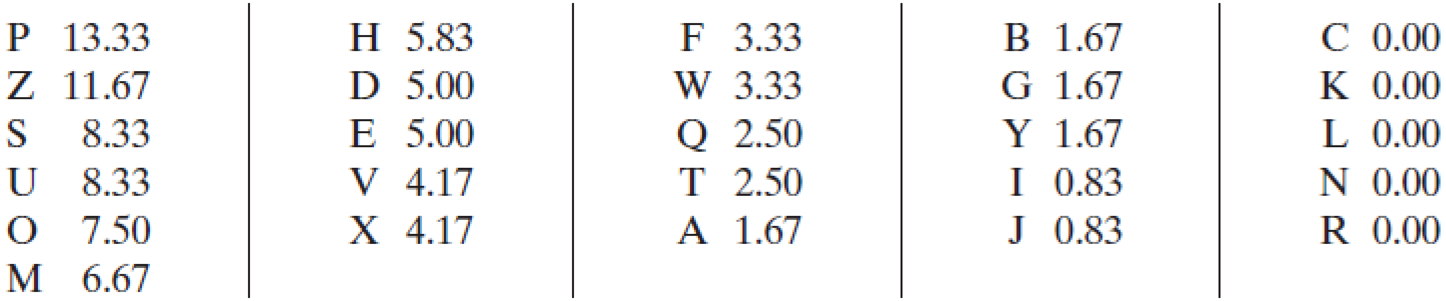
The simplicity and strength of the mono-alphabetic substitution cipher meant it dominated cryptographic use for the first millennium AD. It was broken by Arabic scientists in 9th Century.

Cryptanalysis of Mono-alphabetic cipher

- The ciphertext to be solved is

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

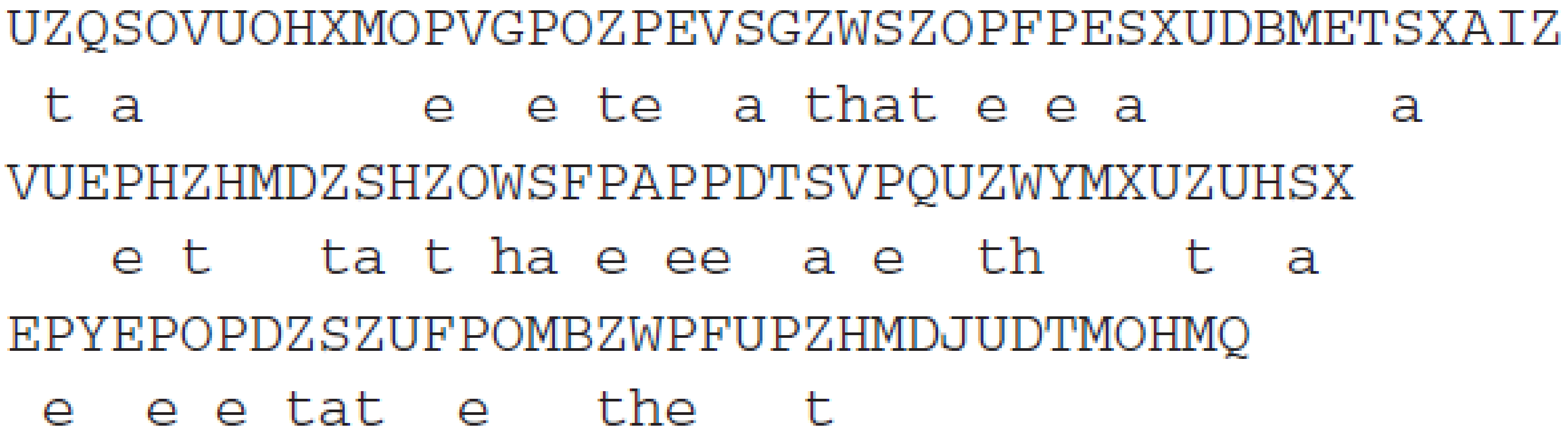
- As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English



P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

- Comparing this breakdown, it seems likely that cipher letters ***P*** and ***Z*** are the equivalents of plain letters e and t, but it is not certain which is which. The letters ***S, U, O, M, and H*** are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}. The letters with the lowest frequencies (namely***, A, B,G, Y, I, J***) are likely included in the set {b, j, k, q, v, x, z}.
- Next sensible thing to do is to compare the digram frequency. The most common such digram is ***th***. In our ciphertext, the most common digram is ***ZW,*** which appears three times. So we make the correspondence of Z with t and W with h.
- The sequence ***ZWP*** appears in the ciphertext, and we can translate that sequence as "***the***". This is the most frequent trigram (three-letter combination)in English.

- Notice the sequence ***ZWSZ*** in the first line. We do not know that these four letters form a complete word, but if they do, it is of the form th_t. If so, S equates with a.
- So far, then, we have



```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

Only four letters have been identified, but already we have quite a bit of the message. Continued analysis of frequencies plus trial and error should easily yield a solution from this point. The complete plaintext, with spaces added between words, follows:

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

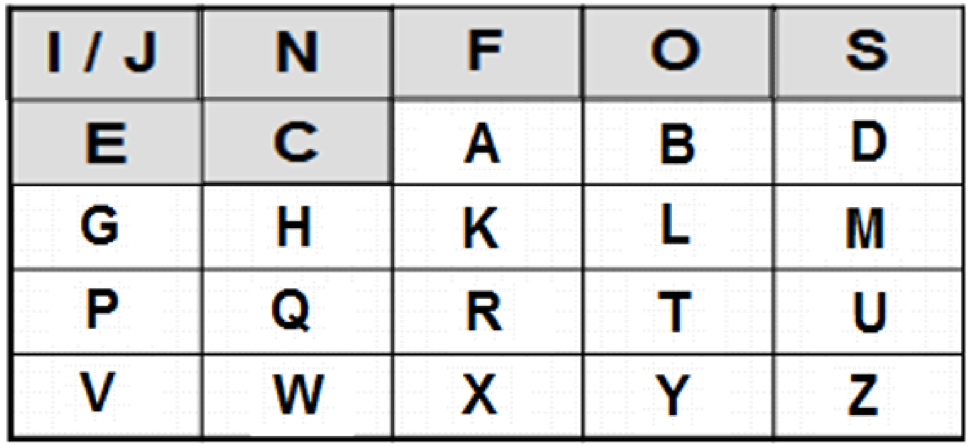
Playfair Cipher

- Not even the large number of keys in a mono-alphabetic cipher provides security. One approach to improving security is to **encrypt multiple letters at a time**.
- The **Playfair Cipher** is the best known such cipher. It is invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair. It treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- The Playfair algorithm is 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

Using the Key word **INFOSEC**



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

- Plaintext is encrypted two letters at a time, according to the rules as shown.
  1. if a pair is a repeated letter, insert a filler like 'X', eg. "balloon" encrypts as "ba lx lo on"
  2. 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"
  3. 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"
  4. 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)

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

Plaintext: Wireless

Wi re le sx sz

Cipher Text: XG MK UL XA TX

Decrypting of course works exactly in reverse.

- Playfair security is much improved over mono-alphabetic since have 26 x 26 = 676 digrams. One would need a 676 entry frequency table to analyse and lots of cipher text.
- It was widely used for many years (eg. US & British military in WW1). It can also be broken since still has much of plaintext structure

Hill Cipher

- **Hill cipher** is a polygraphic substitution **cipher** based on linear algebra. Invented by Lester S. **Hill** in 1929. It involves substitution of '*m*' ciphertext letters for '*m*' successive plaintext letters. For substitution purposes using '*m*' linear equations, each of the characters are assigned a numerical values i.e. a=0, b=1, c=2, d=3,…….z=25.
- It uses one matrix to encrypt, one to decrypt. Must be n x n, invertible matrices. Decryption matrix must be modular inverse of encryption matrix in Mod 26.
- Thus, C = KP *mod26,* where C= Column vectors of length 3, P = Column vectors of length 3

  K = 3x3 encryption key matrix.
- For decryption process, inverse of matrix **K** i.e. $\mathbf{K}^{-1}$ is required which is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the identity matrix that contains only 0's and 1's as its elements. Plaintext is recovered by applying K^{-1} to the cipher text. It is expressed as

$$C = E_K(P) = KP \; mod26$$

$$P = D_K(C) = K^{-1}C \; mod26.$$

$$= K^{-1}KP = IP = P$$

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

- For our purposes, we will illustrate the cipher with n=2. Consider the following key: $\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}$
- To encrypt a plaintext, group the plaintext in pairs: "**MA**" and "**TH**", for example. Convert each letter to its numerical equivalent, mod 26, and write it in a nx1 matrix as follows: $\begin{pmatrix} 12 \\ 0 \end{pmatrix}$
- Now, multiply the encryption key by the plaintext and reduce mod 26 to get the ciphertext:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 36 \\ 72 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix} \bmod 26$$

which corresponds to the ciphertext **KU**

- Here is the encryption of "TH":

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} 64 \\ 149 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 19 \end{pmatrix} \bmod 26$$

which corresponds to the ciphertext **MT**

- To decrypt, you need the inverse matrix. Although it's beyond the scope of this class, here's the derivation of the inverse matrix:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 26$$

which results in the inverse matrix $\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}$

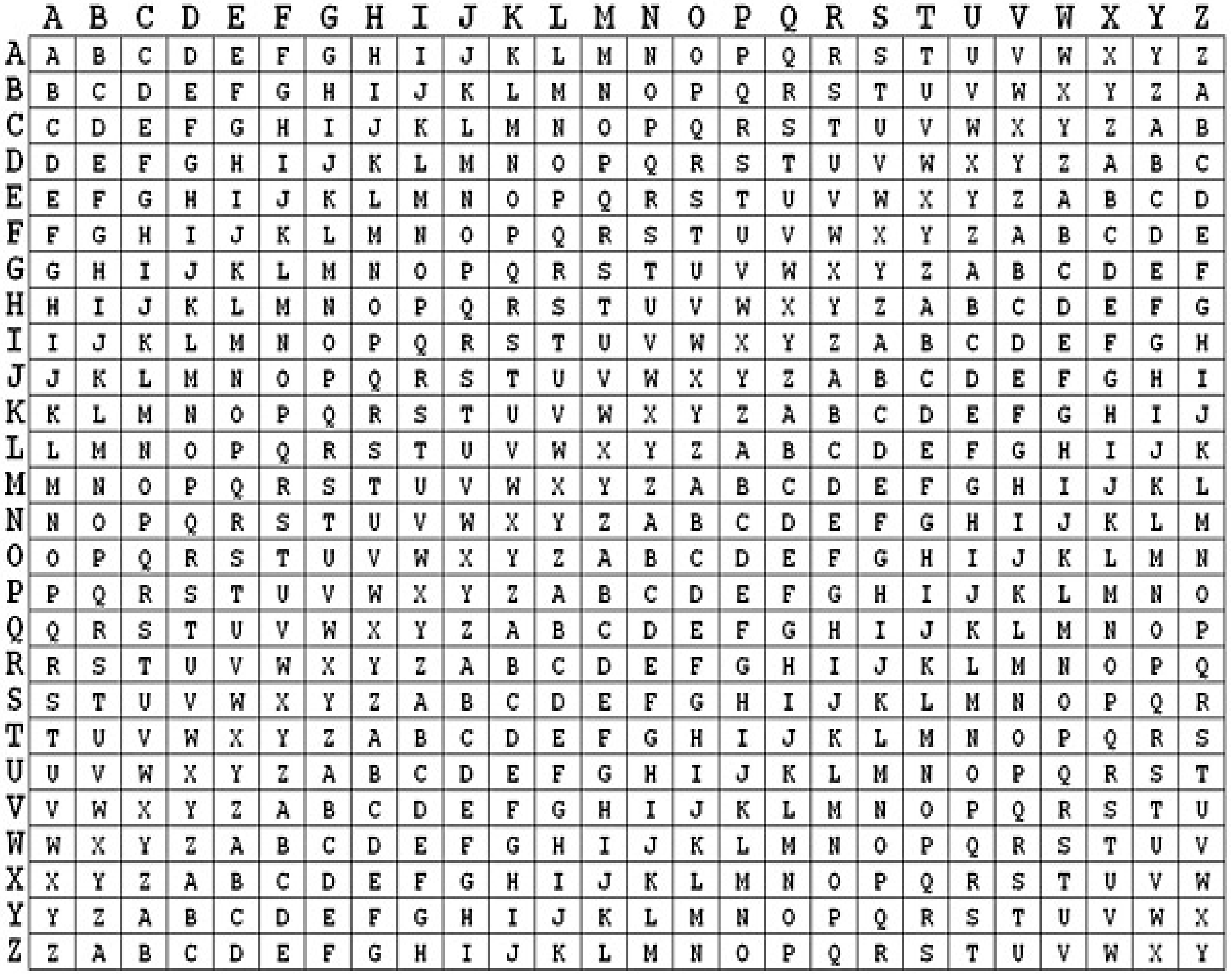
- Now, we can corroborate that this is the case by decrypting the example above

$$\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}\begin{pmatrix} 10 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 610 \\ 260 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 0 \end{pmatrix} \bmod 26 \qquad \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}\begin{pmatrix} 12 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 617 \\ 267 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 7 \end{pmatrix} \bmod 26$$

- **The main advantages of hill cipher is that it perfectly hides single-letter frequencies.**
- **Strong enough against the attacks made only on the cipher text. But, it still can be easily broken if the attack is through a known plaintext.**

Vigenère Cipher

- The **Vigenere cipher** is a polyalphabetic cipher based on using successively shifted alphabets, a different shifted alphabet for each of the 26 English letters. The procedure is based on the tableau shown below and the use of a keyword.

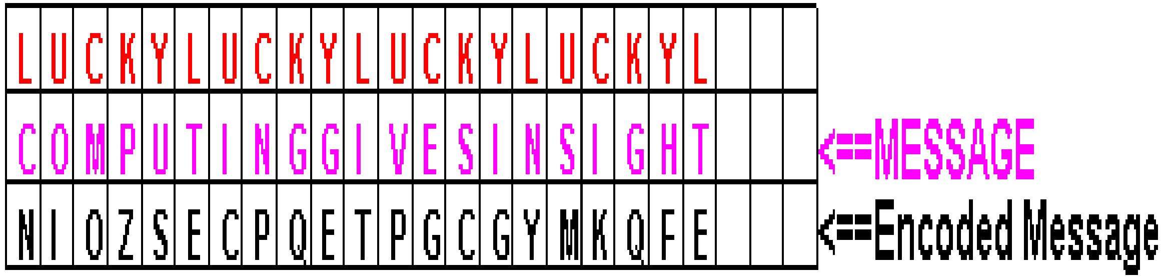


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

For the message COMPUTING GIVES INSIGHT and keyword LUCKY we proceed by repeating the keyword as many times as needed above the message, as follows.

L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L
C	O	M	P	U	T	I	N	G	G	I	V	E	S	I	N	S	I	G	H	T

Encryption is simple: Given a key letter x and a plaintext letter y, the ciphertext letter is at the intersection of the row labeled *x* and the column labeled *y*; so for L, the ciphertext letter would be N. So, the ciphertext for the given plaintext would be given as:



L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L				
C	O	M	P	U	T	I	N	G	G	I	V	E	S	I	N	S	I	G	H	T				<==MESSAGE
N	I	O	Z	S	E	C	P	Q	E	T	P	G	C	G	Y	M	K	Q	F	E				<==Encoded Message

Transposition Ciphers

- A Transposition Cipher is a cipher in which the plaintext message is rearranged by some means agreed upon by the sender and receiver.
  - *In transposition ciphers, no new alphabet is created. The letters of the plaintext are just rearranged in some fashion…*

Transposition Cipher Types

1. **Rail Fence Cipher** - involves writing messages so that alternate letters are written on separate upper and lower lines
2. **Route Cipher** - the plaintext is first written out in a grid of given dimensions, then read off in a pattern given in the key.
3. **Simple Columnar Cipher** - This cipher technique simply arranges the plain text as a sequence of rows of a rectangle that are read in columns.
4. **Keyword Columnar Cipher** - This cipher technique simply arranges the plain text as a sequence of rows of a rectangle that are read in columns according to the keyword.

Plain text: meet me after the toga party

Row 1: m e m a t r h t g p r y

Row 2: e t e f e t e o a a t

Cipher text: m e m a t r h t g p r y e t e f e t e o a a t

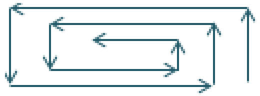
Plain Text: HELLO WORLD **Key =** 3 Columnar

Column 1	Column 2	Column 3
H	E	L
L	O	W
O	R	L
D	X	X

Cipher Text: HLODEORXLWLX

Plain Text: meet me after the toga party at seven clock

Key = 5 Rows &



(35 letters " 35 / 5 = 7")

Row 1:	m	e	r	o	r	s	c
Row 2:	e	a	t	g	t	e	l
Row 3:	e	f	h	a	y	v	o
Row 4:	t	t	e	p	a	e	c
Row 5:	m	e	t	a	t	n	k

Cipher Text: kcolcsroremeetmetatnevetgtaftepayah

Plain Text: defend the east wall of the castle **Keyword =** GERMAN

1st Step

G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e	x	x

2nd Step

A	E	G	M	N	R
n	e	d	e	d	f
a	h	t	e	s	e
l	w	t	l	o	a
c	t	f	e	a	h
x	t	s	e	x	l

Cipher Text: nalcxehwttdttfseeleedsoaxfeahl

Modern Block Ciphers

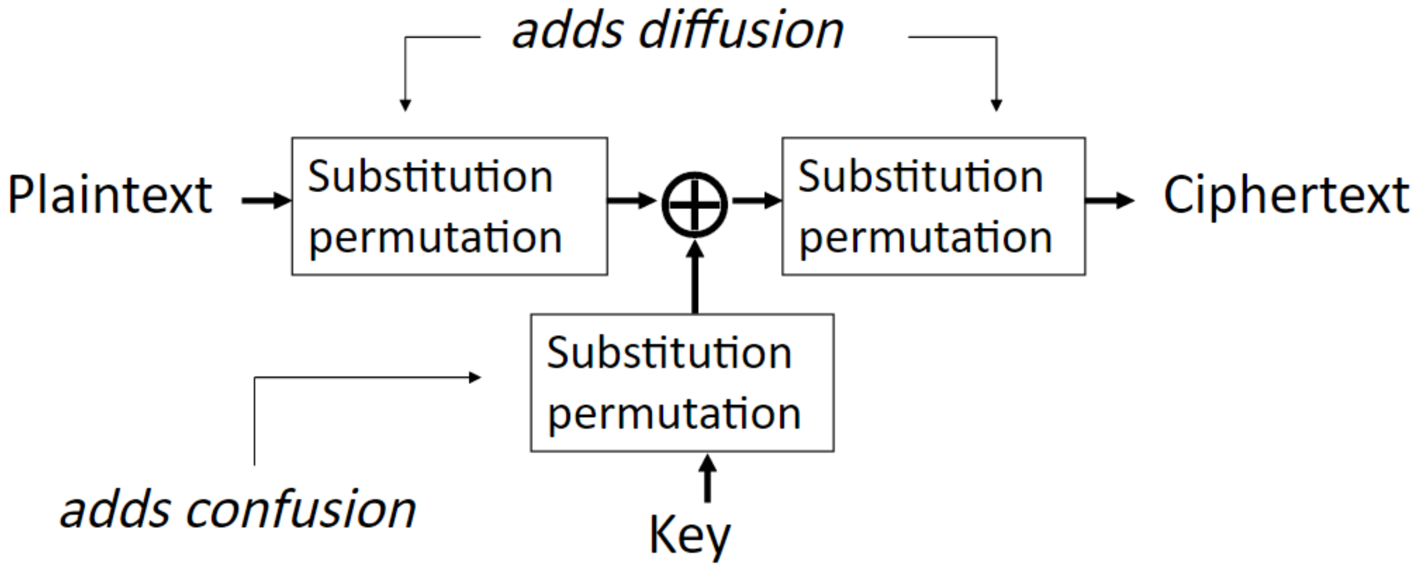
- Modern block ciphers are widely used to provide encryption of quantities of information, and/or a cryptographic checksum to ensure the contents have not been altered.

- Block ciphers work a on block / word at a time, which is some number of bits. All of these bits have to be available before the block can be processed. Stream ciphers work on a bit or byte of the message at a time, hence process it as a “stream”. Block ciphers are currently better analysed, and seem to have a broader range of applications.

- Most symmetric block encryption algorithms in current use are based on a structure referred to as a **Feistel block cipher**. A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits.

- Claude Shannon’s 1949 paper has the key ideas that led to the development of modern block ciphers. Critically, it was the technique of layering groups of S-boxes separated by a larger P-box to form the S-P network, a complex form of a product cipher. He also introduced the ideas of *confusion* and *diffusion*, notionally provided by S-boxes and P-boxes

- Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key.
- The mechanism of **diffusion** seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.
- **Confusion** seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key.



Feistel Cipher Structure

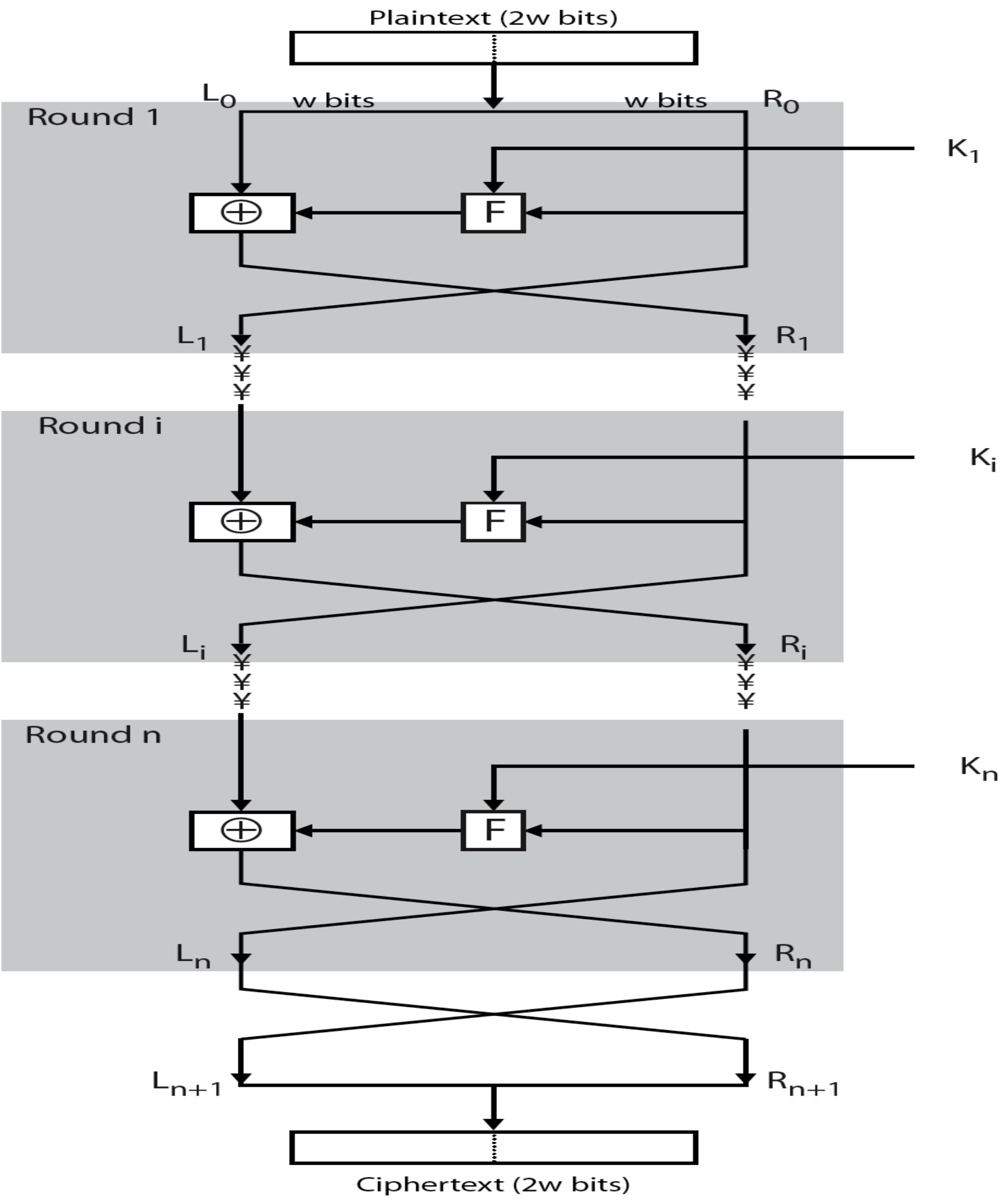
- Horst Feistel, working at IBM Thomas J Watson Research Labs devised a suitable invertible cipher structure in early 70's. First described by Fiestel in 1973, it forms the basis for almost all conventional encryption schemes

- It is depends on the choice of the following parameters
  - **Block size:** larger block sizes mean greater security (typical size is 64 bits)
  - **Key Size:** larger key size means greater security (typical size is 128 bits)
  - **Number of rounds:** multiple rounds offer increasing security but slows down the cipher (N = 16)
  - **Subkey generation algorithm:** greater complexity will lead to greater difficulty of cryptanalysis.
  - **Round Function (F):** Greater complexity in this algorithm means greater resistance
  - **Fast software encryption/decryption:** the speed of execution of the algorithm becomes a concern.
  - **Ease of Analysis:** Though the algorithm is made as difficult as possible to cryptanalyze, it should be easy to analyze.

One of Feistel's main contributions was the invention of a suitable structure which adapted Shannon's S-P network in an **easily inverted structure**. It partitions input block into two halves which are processed through multiple rounds which perform a substitution on left data half, based on round function of right half & subkey, and then have permutation swapping halves. Essentially the same h/w or s/w is used for both encryption and decryption, with just a slight change in how the keys are used.

Steps:

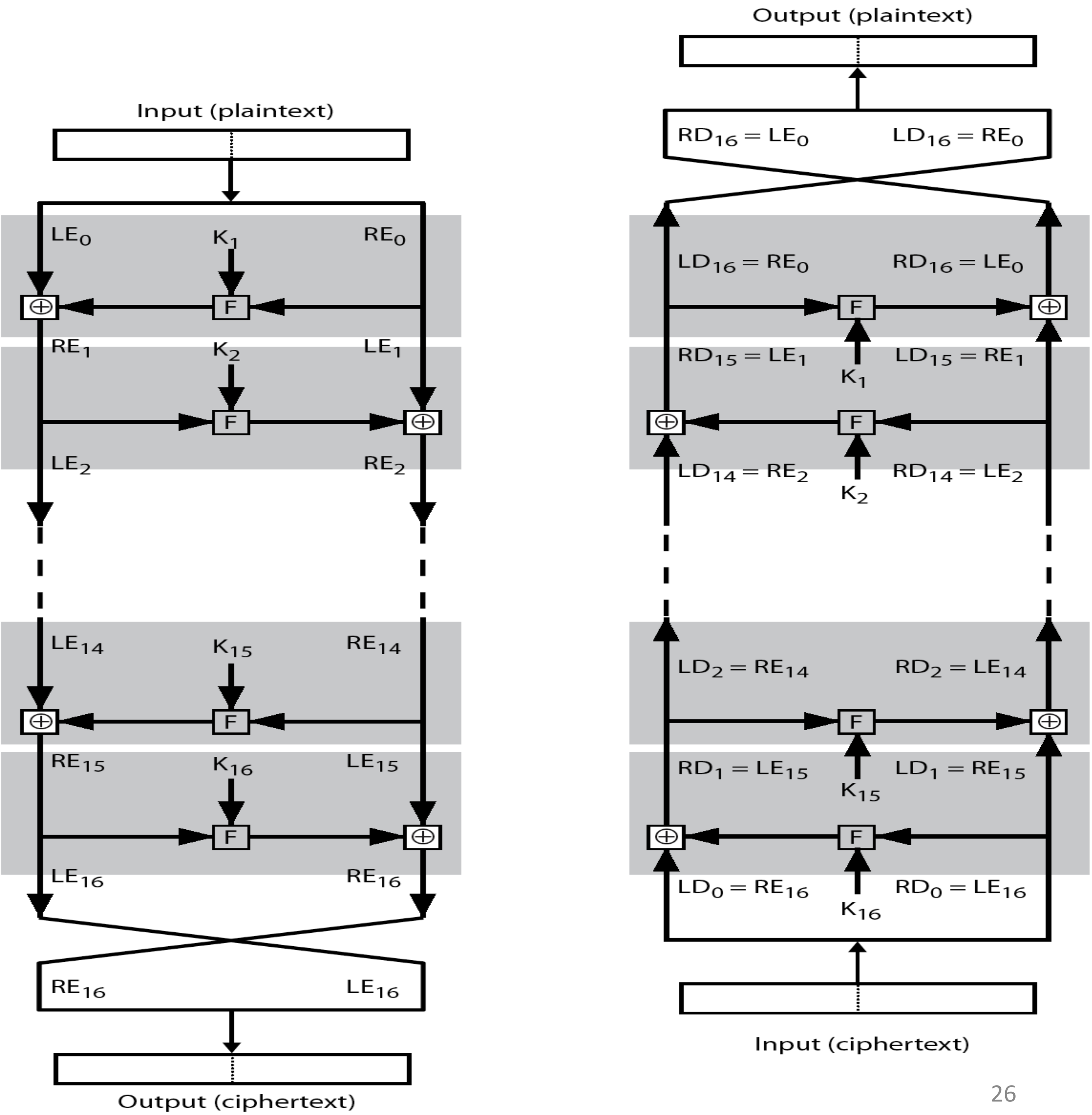
- Input of plaintext with length 2w bits and key K.
- Plaintext is divided into two halves L**0** and R**0**.
- These two halves pass through N rounds of processing to produce CipherText block.
- The key K is derived from subkey generation algorithm.
- These two halves combine by applying a round function '**F**' on right half of data and then taking XOR operation of the output of **F** with left half of data.
- A permutation is performed which swaps the two halves of data forming a substitution – permutation network (SPN) as proposed by Shannon.



- The process of decryption with a Feistel cipher, is essentially the same as the encryption process.

- The rule is as follows: Use the ciphertext as input to the algorithm, but use the subkeys *Ki* in reverse order. That is, use *Kn* in the first round, *Kn*–1 in the second round, and so on until *K*1 is used in the last round.

- This is a nice feature because it means we need not implement two different algorithms, one for encryption and one for decryption.



Input (plaintext)
LE_0
K_1
RE_0
F
⊕
RE_1
K_2
LE_1
LE_2
RE_2
LE_{14}
K_{15}
RE_{14}
RE_{15}
K_{16}
LE_{15}
LE_{16}
RE_{16}
RE_{16}
LE_{16}
Output (ciphertext)
Output (plaintext)
$RD_{16} = LE_0$
$LD_{16} = RE_0$
$LD_{16} = RE_0$
$RD_{16} = LE_0$
$RD_{15} = LE_1$
K_1
$LD_{15} = RE_1$
$LD_{14} = RE_2$
K_2
$RD_{14} = LE_2$
$LD_2 = RE_{14}$
$RD_2 = LE_{14}$
$RD_1 = LE_{15}$
K_{15}
$LD_1 = RE_{15}$
$LD_0 = RE_{16}$
K_{16}
$RD_0 = LE_{16}$
Input (ciphertext)