Information Security

PREPARED BY: DR. REEMA PATEL

Security Basics

- The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T)
  - Provides some security secrecy and some mechanisms to implement those services

- ITU-T Recommendation X.800, Security Architecture for OSI
  - defines such a systematic approach of defining and providing security requirements

Security Basics

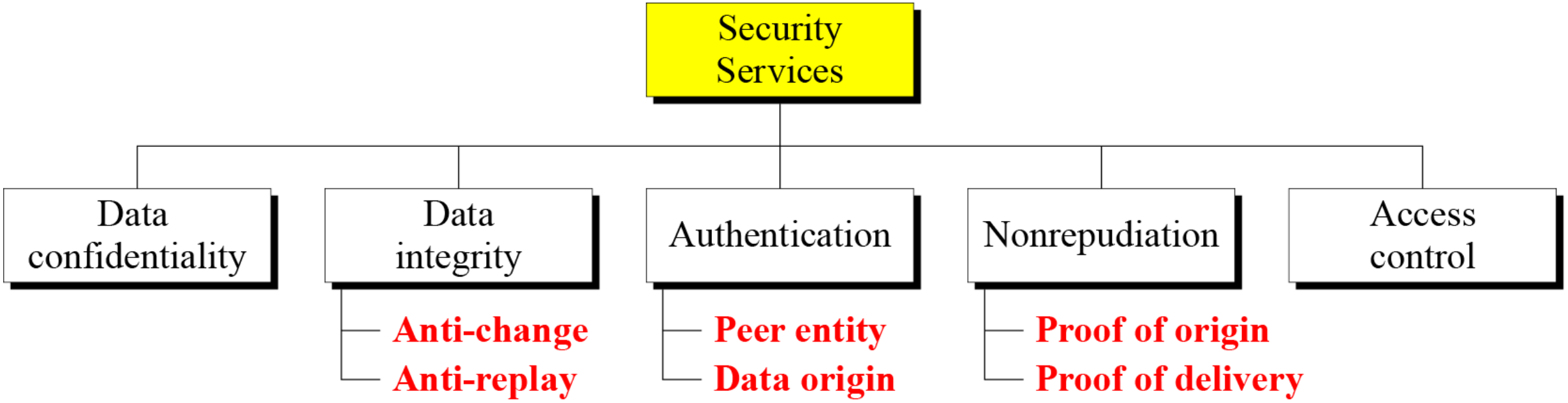
- X.800 focuses on three aspects of information security

1. Security service
   - properties which any security solution should satisfy e.g. ……

2. Security mechanism
   - tools and techniques by which, the security services can be achieved e.g.

3. Security attack
   - actions that are attempts at violating the security rules.

Security Services



Security Services - X.800 objectives

- **Authentication** : assurance that the communicating entity is the one claimed
- **Access Control** : prevention of the unauthorized use of a resource
- **Data Confidentiality :** protection of data from unauthorized disclosure
- **Data Integrity** : assurance that data received are exactly as sent by an authorized entity
- **Non-Repudiation** : protection against denial by one of the parties in a communication

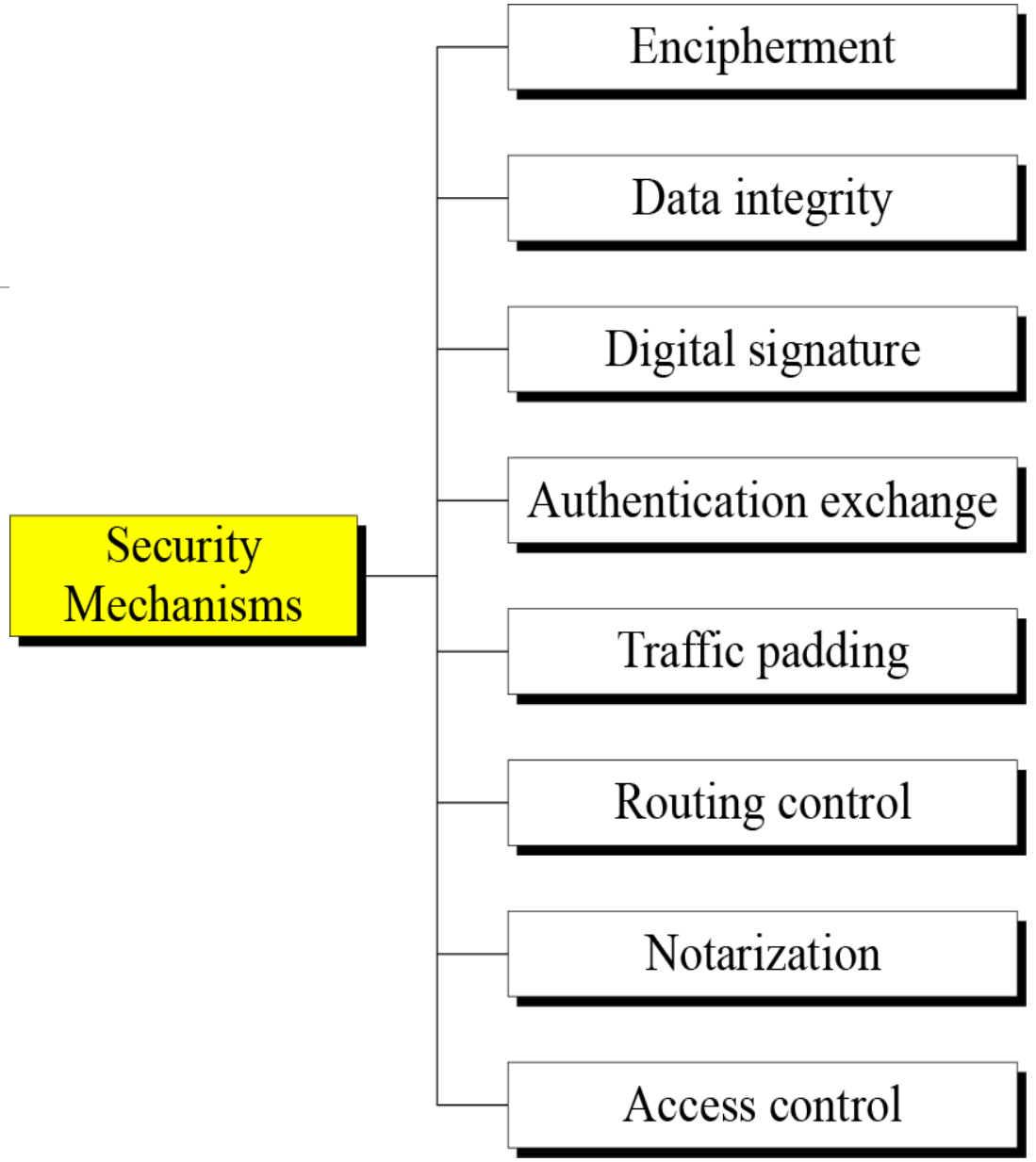
Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack

- No single mechanism that will support all services required

These are the tools used to provide security, such as:Encryption – Converting data into a coded format.Firewalls – Blocking unauthorized access to networks.Antivirus – Detecting and removing malicious software.
No single mechanism is enough; multiple layers of security are needed.

Security Mechanism



Security Services and Security Mechanisms

- Relation between Security Services and Security Mechanisms

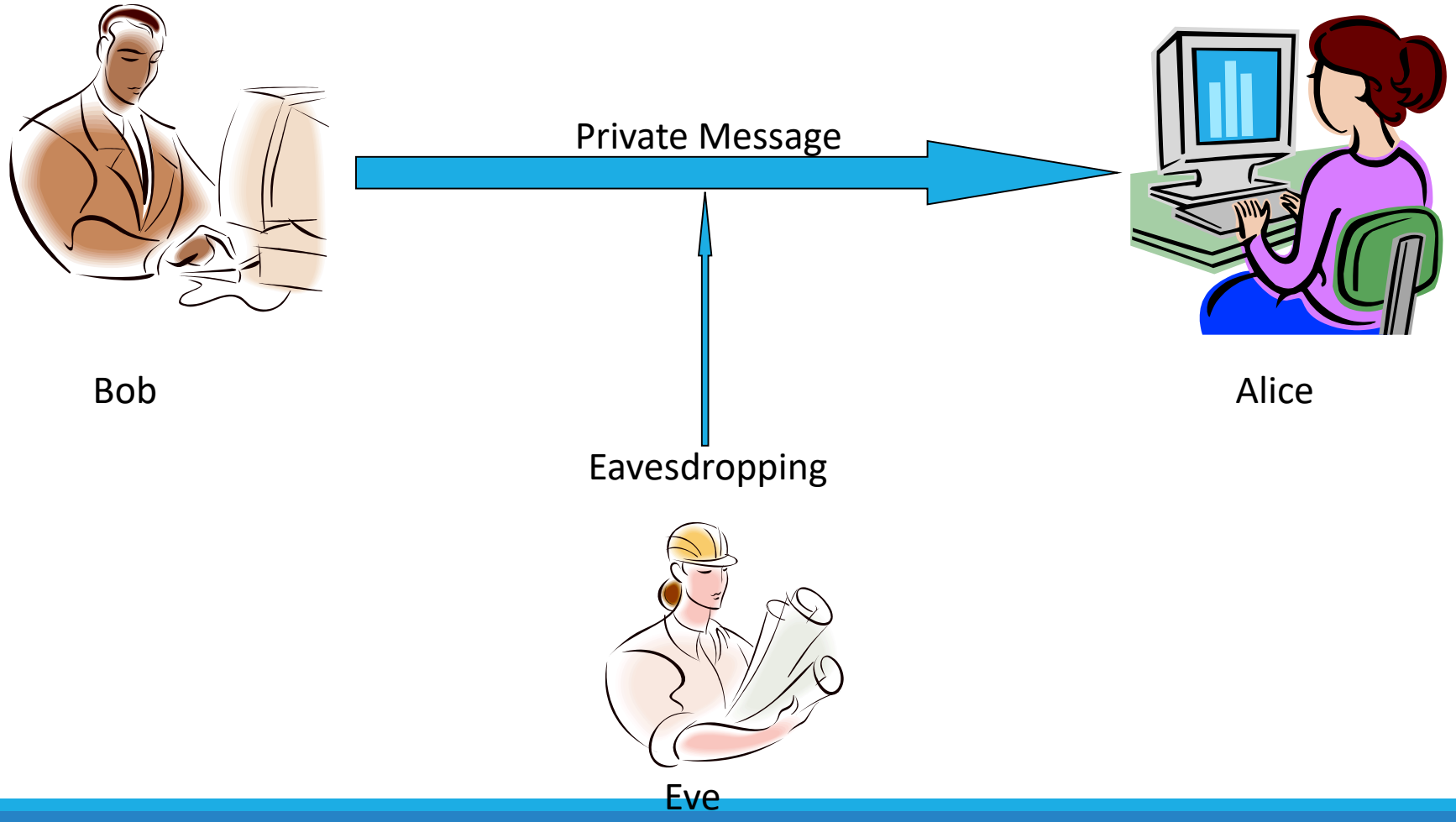
Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Cryptography

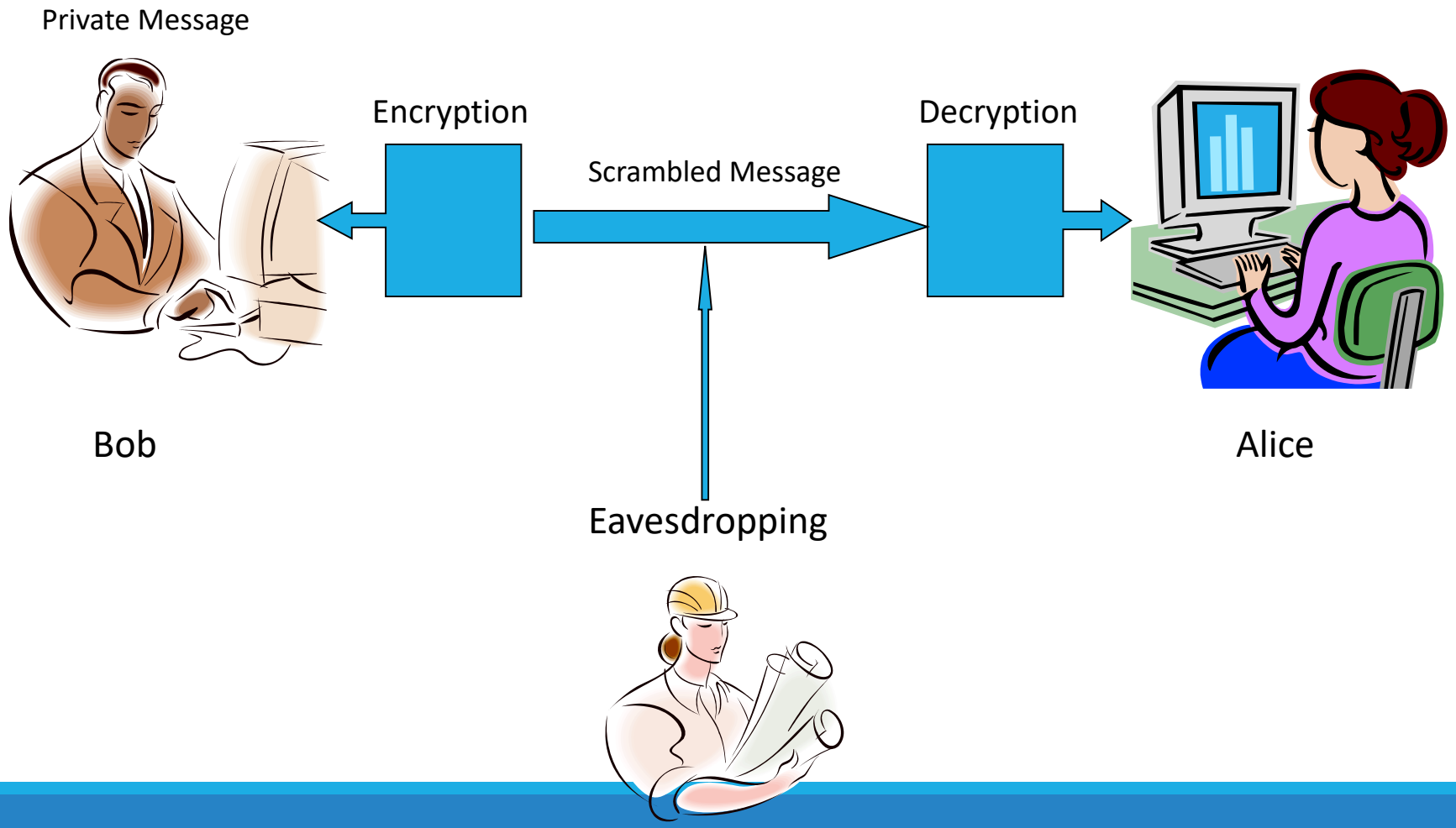
- kryptos – “hidden”
- grafo – “write”

- Keeping messages secret
  - Usually by making the message unintelligible to anyone that intercepts it

Problem



Solution


Private Message
Encryption
Scrambled Message
Decryption
Bob
Alice
Eavesdropping

Basic Terminology

- **plaintext** - original message
- **ciphertext** - 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)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Ciphers

- Symmetric cipher: same key used for encryption and decryption
- Block cipher:
  - encrypts a block of plaintext at a time (typically 64 or 128 bits)
- Stream cipher:
  - encrypts data one bit or one byte at a time

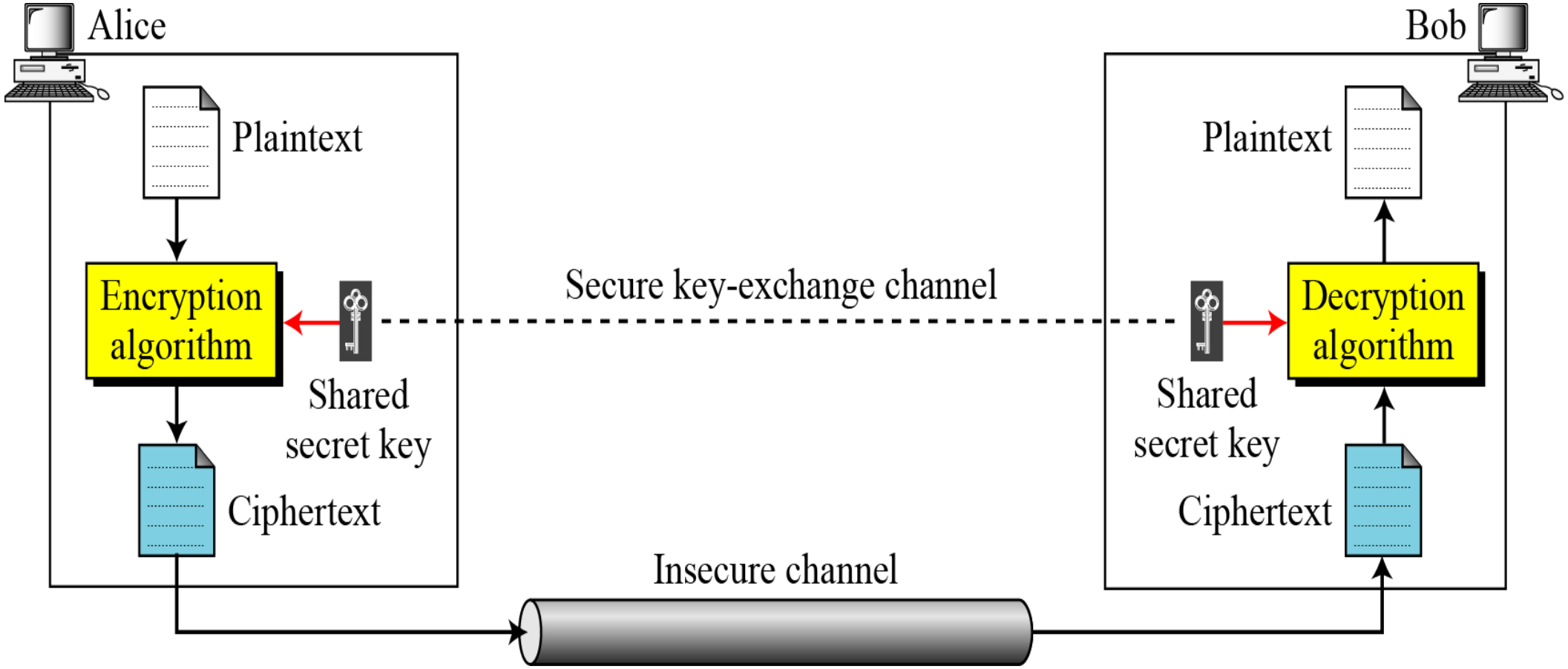
- Asymmetric cipher: different keys used for encryption and decryption

Symmetric Cipher Model

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm

- Security depends on the secrecy of the key, not the secrecy of the algorithm

Symmetric Key Cipher Model



Symmetric Encryption

- Mathematically:
  - $Y = E_K(X)$ or $Y = E(K, X)$
  - $X = D_K(Y)$ or $X = D(K, Y)$
- X = plaintext
- Y = ciphertext
- K = secret key
- E = encryption algorithm
- D = decryption algorithm
- Both E and D are known to public

Symmetric Encryption

- type of encryption operations used
  - Substitution
  - Transposition
  - Product
- way in which plaintext is processed
  - Block
  - Stream

Classical Ciphers

- Plaintext is viewed as a sequence of elements (e.g., bits or characters)
- Substitution cipher:
  - replacing each element of the plaintext with another element.
- Transposition (or permutation) cipher:
  - rearranging the order of the elements of the plaintext.
- Product cipher: using multiple stages of substitutions and transpositions

Substitution Ciphers

- A substitution cipher replaces one symbol with another.
- Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.
- In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Substitution Ciphers

- The following shows a plaintext and its corresponding ciphertext.
- The cipher is probably monoalphabetic because both l's are encrypted as O's.

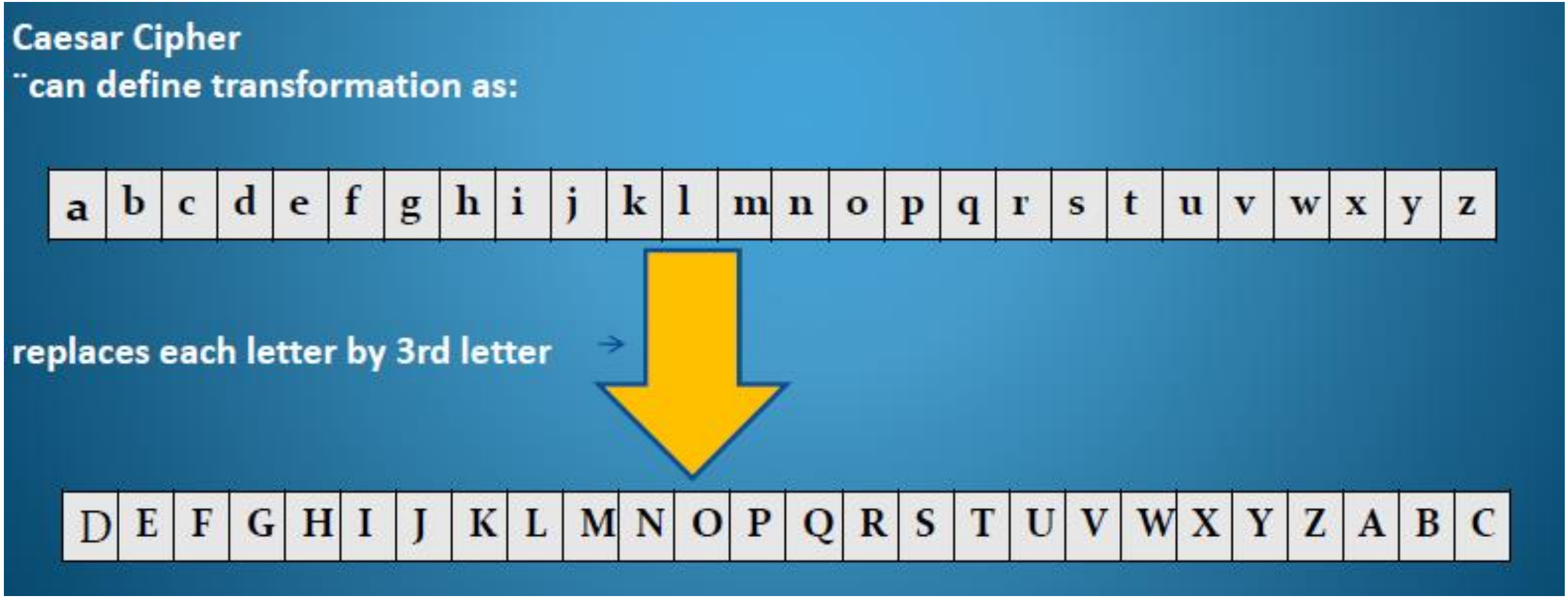
Plaintext: hello **Ciphertext:** KHOOR

Caesar Cipher

- The simplest monoalphabetic cipher is the additive cipher.
- This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature.

Caesar Cipher / Shift Cipher

- earliest known substitution cipher
- by Julius Caesar
- first use in military affairs
- replaces each letter by 3rd letter after



- Example:

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

Caesar Cipher / Shift Cipher

- **Caesar Cipher can define Mathematical transformation as:**
- **First we convert the letters of the alphabet to number so that we can operate on them mathematically.**
- **We convert ‘a’ to 0, ‘b’ to 1, ‘c’ to 3.right through to ‘z’ 25 as shown below.**

Caesar Cipher / Shift Cipher

- mathematically give each letter a number

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

- then have Caesar cipher as:

$c = E_k(p) = (p + k) \bmod (26)$

$p = D_k(c) = (c - k) \bmod (26)$

Caesar Cipher transformation Example:

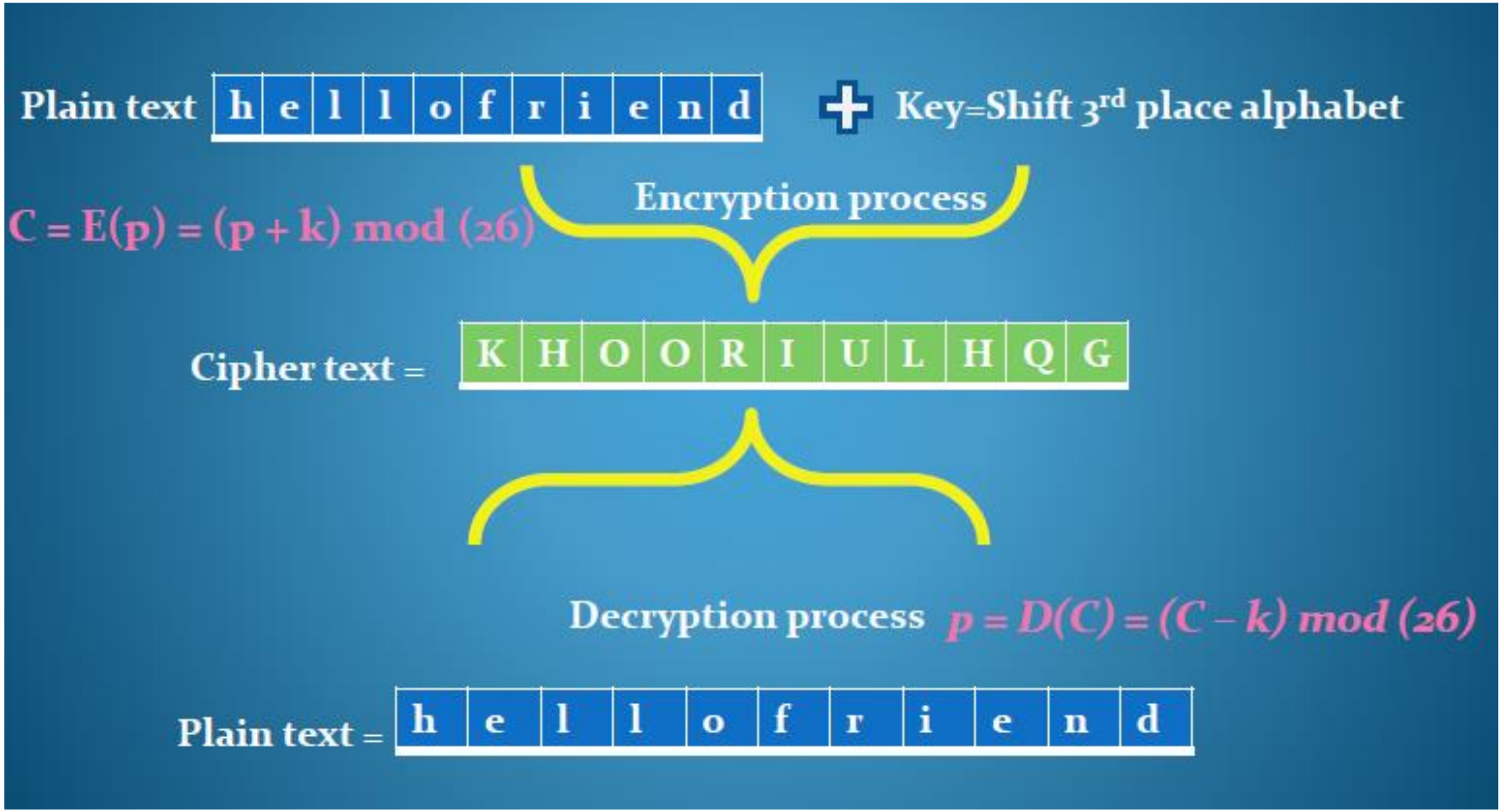
1. Steps- Encryption and decryption process using Caesar cipher
2. Choose Plain text (original message).

Hello friend → Plain text

3. Applying Caesar cipher replaces each letter by 3rd letter algorithm

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	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

4. Use key for Encryption
   Key= Number of shift alphabet called key


Plain text h e l l o f r i e n d
Key=Shift 3rd place alphabet
C = E(p) = (p + k) mod (26)
Encryption process
Cipher text = K H O O R I U L H Q G
Decryption process p = D(C) = (C – k) mod (26)
Plain text = h e l l o f r i e n d

Example

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

- Encrypt: **Covid**
- **Key: 6**
- **(P+K) mod 26**
- **Ciphertext = ?**

Example

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

- Encrypt: **Covid**
- **Key: 6**
- **Ciphertext: iuboj**
- **Decryption: (C-K) mod 26**

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
- do need to recognize when have plaintext
- eg. break ciphertext "jfxd yt gwjfp"

Brute Force Search

- always possible to simply try every key
- most basic attack, exponential in key length
- assume either know / recognise plaintext

Brute Force Search

- Ciphertext = “GRR MGAR OY JOBOJKJ OT ZNXKK VGXZY”
- Perform decryption with each possible key:
  - Decrypted plaintext with key 1

    FQQ LFZQ NX INANIJI NS YMWJJ UFWYX
  - Decrypted plaintext with key 2

    EPP KEYP MW HMZMHIH MR XLVII TEVXW
  - Decrypted plaintext with key 3

    DOO JDXO LV GLYLGHG LQ WKUHH SDUWV

Brute Force Search

- Decryption with each possible key (continued)
  - Decrypted plaintext with key 4

    CNN ICWN KU FKXKFGF KP VJTGG RCTVU
  - Decrypted plaintext with key 5

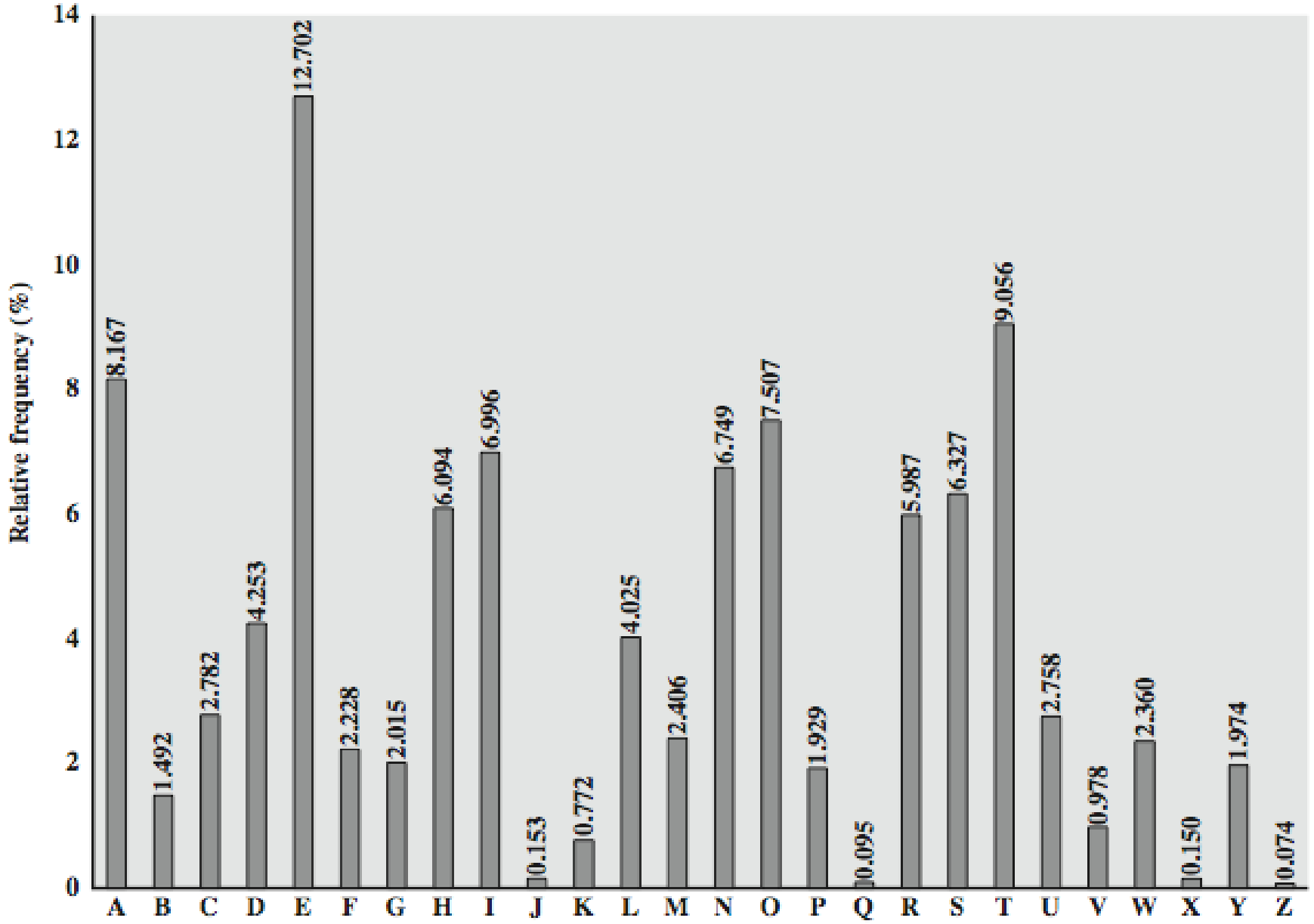
    BMM HBVM JT EJWJEFE JO UISFF QBSUT
  - Decrypted plaintext with key 6

    ALL GAUL IS DIVIDED IN THREE PARTS
  - And so on….
- Only one of the Decrypted plaintexts makes sense

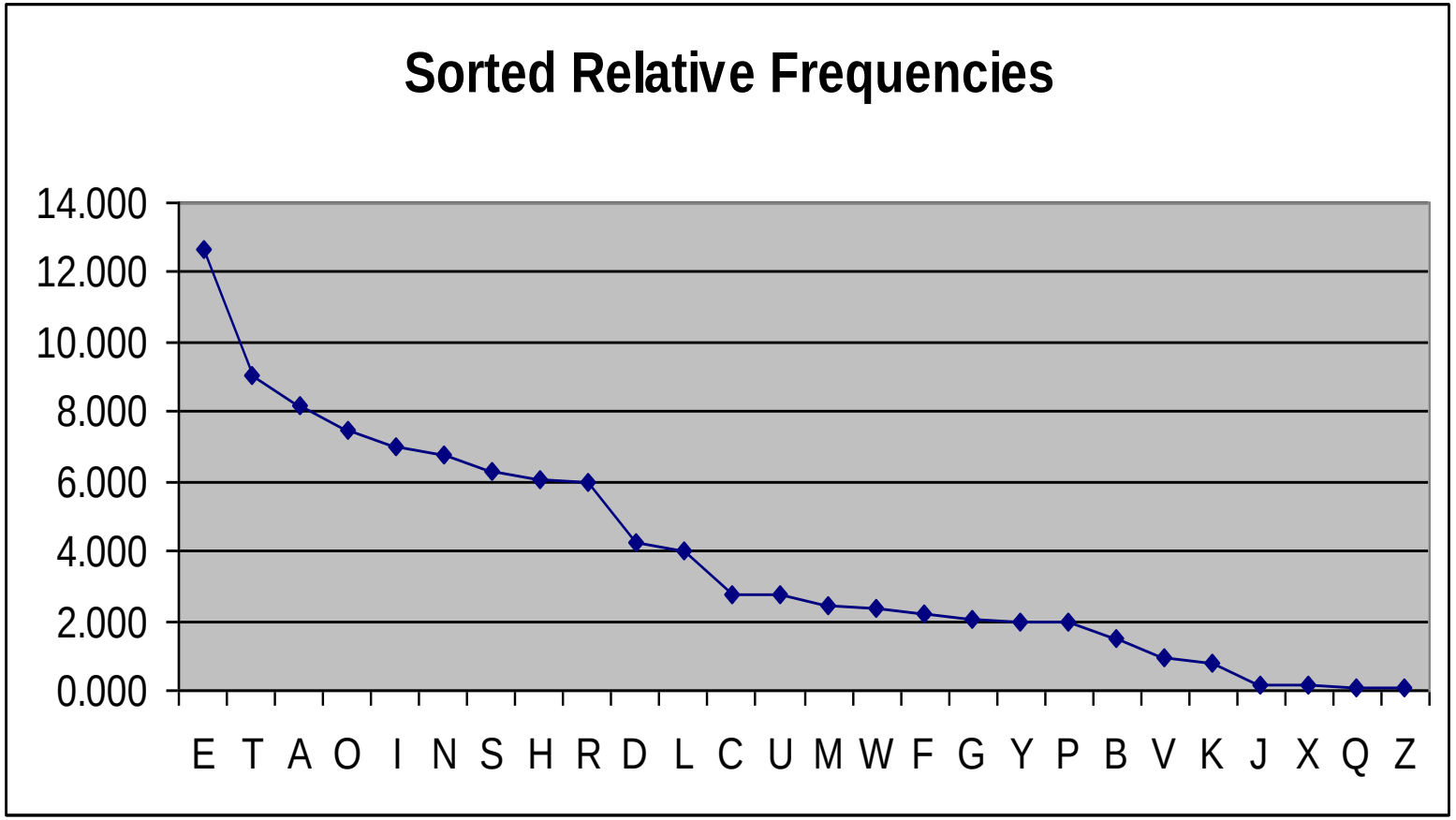
Language Redundancy and Cryptanalysis

- human languages are redundant
- e.g., "th lrd s m shphrd shll nt wnt"
- letters are not equally commonly used
- in English E is by far the most common letter
  - followed by T,R,N,I,O,A,S
- other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter frequencies for various languages

Frequency Analysis



Frequency analysis



Example

- Cipher Text:
  - wkh sdvvzrug lv vhyhq grqw whoo dqbrqh

Example Cryptanalysis

- given ciphertext:
  - UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  - VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  - EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- count relative letter frequencies

Example Cryptanalysis

- given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- guess P & Z are e and t
- guess ZW is th and hence ZWP is “the”

Cryptanalysis

- You can have tables of single, double & triple letter frequencies for various languages

- **Common pairs :** TH, EA, OF, TO, IN, IT, IS, BE, AS, AT, SO, WE, HE, BY, OR, ON, DO, IF, ME, MY, UP
- **Common repeated letters:** SS, EE, TT, FF, LL, MM and OO
- **Common triplets:** THE, EST, FOR, AND, HIS, ENT or THA

Towards the Polyalphabetic Substitution Ciphers

- Main weaknesses of monoalphabetic substitution ciphers
  - In ciphertext, different letters have different frequency
    - each letter in the ciphertext corresponds to only one letter in the plaintext letter

- Developed into a practical cipher by Vigenère (published in 1586)

Polyalphabetic Ciphers

- In polyalphabetic substitution, each occurrence of a character may have a different substitute.

- The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

Polyalphabetic Substitution Ciphers

- makes cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached

Substitution Cipher

- **Monoalphabetic Cipher :**
  - A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key.
- **Polyalphabetic Cipher :**
  - A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

R.NO	Monoalphabetic Cipher	Polyalphabetic Cipher
1	Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
2	The relationship between a character in the plain text and the characters in the cipher text is one-to-one.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
3	Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.	Each alphabetic character of plain text can be mapped onto ‘m’ alphabetic characters of a cipher text.
4	A stream cipher is a monoalphabetic cipher if the value of key does not depend on the position of the plain text character in the plain text stream.	A stream cipher is a polyalphabetic cipher if the value of key does depend on the position of the plain text character in the plain text stream.
5	It includes additive, multiplicative, affine and monoalphabetic substitution cipher.	It includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.
6	It is a simple substitution cipher.	It is multiple substitutions cipher.
7	Monoalphabetic Cipher is described as a substitution cipher in which the same fixed mappings from plain text to cipher letters across the entire text are used.	Polyalphabetic Cipher is described as substitution cipher in which plain text letters in different positions are enciphered using different cryptoalphabets.
8	Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.	Polyalphabetic ciphers are much stronger.

Other Cipher

- Railfence Cipher
- Playfair Cipher