

OVER  
**40**  
YEARS  
OF ACADEMIC  
WISDOM



# PRESIDENCY UNIVERSITY

## CSE3078 – Cryptography and Network Security



## School of Computer Science and Engineering

---

# **Module 1**

## **Introduction to Cryptography and types of Ciphers**



# Introduction to Cryptography

---

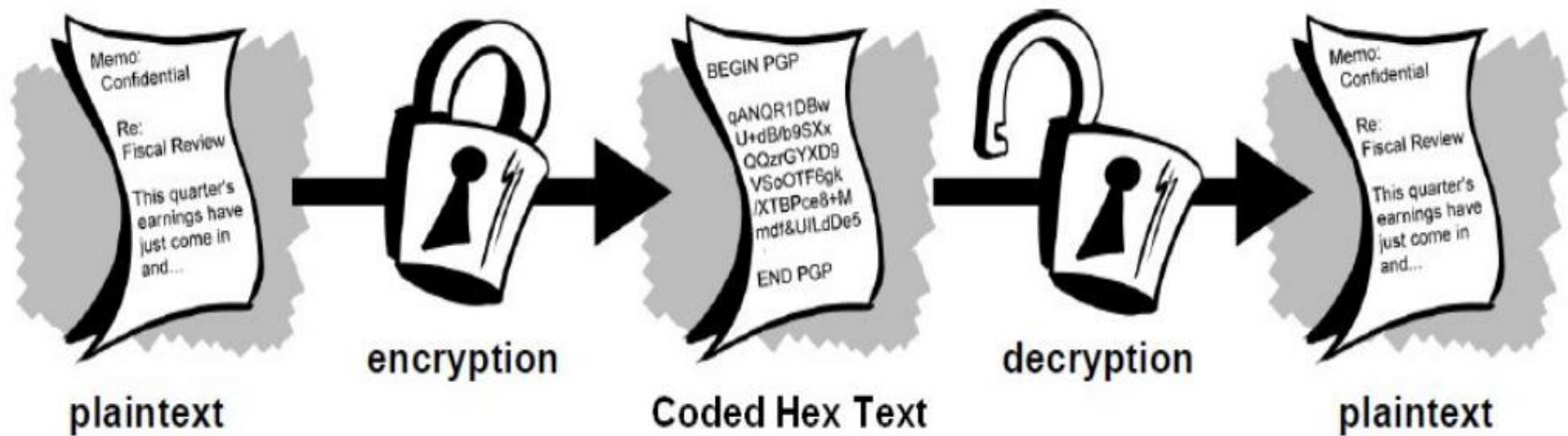
## Definition

Cryptography is the science of using mathematics to encrypt and decrypt data - **Phil Zimmermann**

Cryptography is the art and science of keeping messages secure - **Bruce Schneier**



# Terminologies



- 
- ✓ A message is plaintext (sometimes called cleartext).
  - ✓ The process of disguising a message in such a way as to hide its substance is encryption.
  - ✓ An encrypted message is ciphertext.
  - ✓ The process of turning ciphertext back into plaintext is decryption.





- 
- ✓ A cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure



# Cryptosystem

---

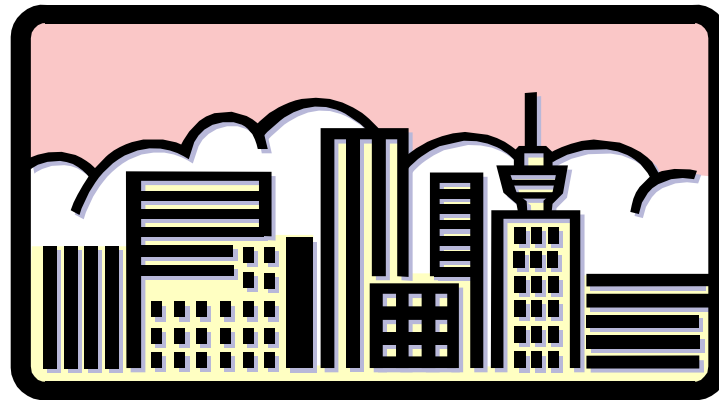
- A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services.
- A cryptosystem is also referred to as a cipher system.
- The various components of a basic cryptosystem are as follows –
  - Plaintext
  - Encryption Algorithm
  - Ciphertext
  - Decryption Algorithm
  - Encryption Key
  - Decryption Key



# OSI Security Architecture

---

- “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts.





# Aspects of Security

---

- consider 3 aspects of information security:
  - security attack
  - security mechanism
  - security service



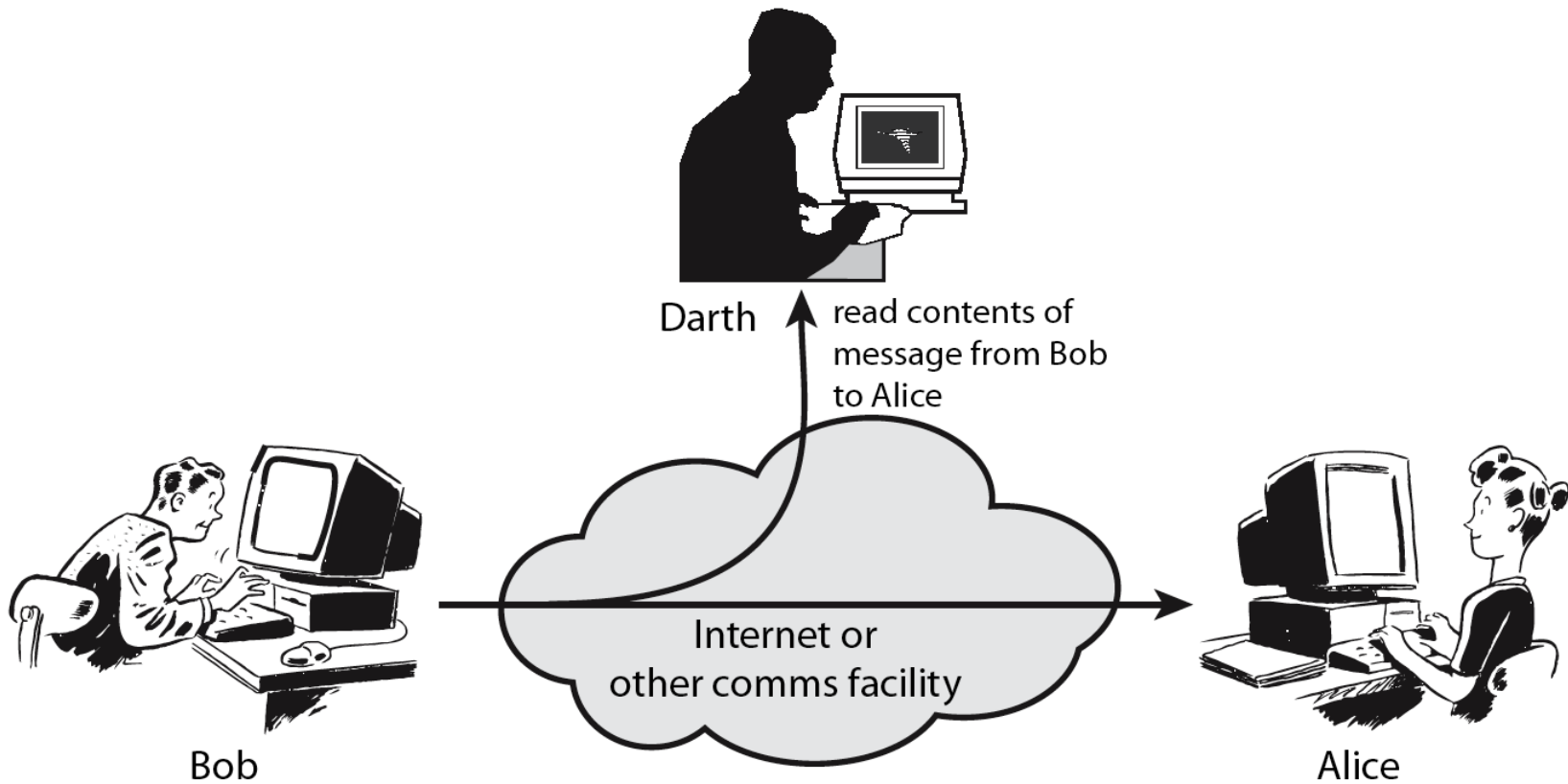
# Security Attack

---

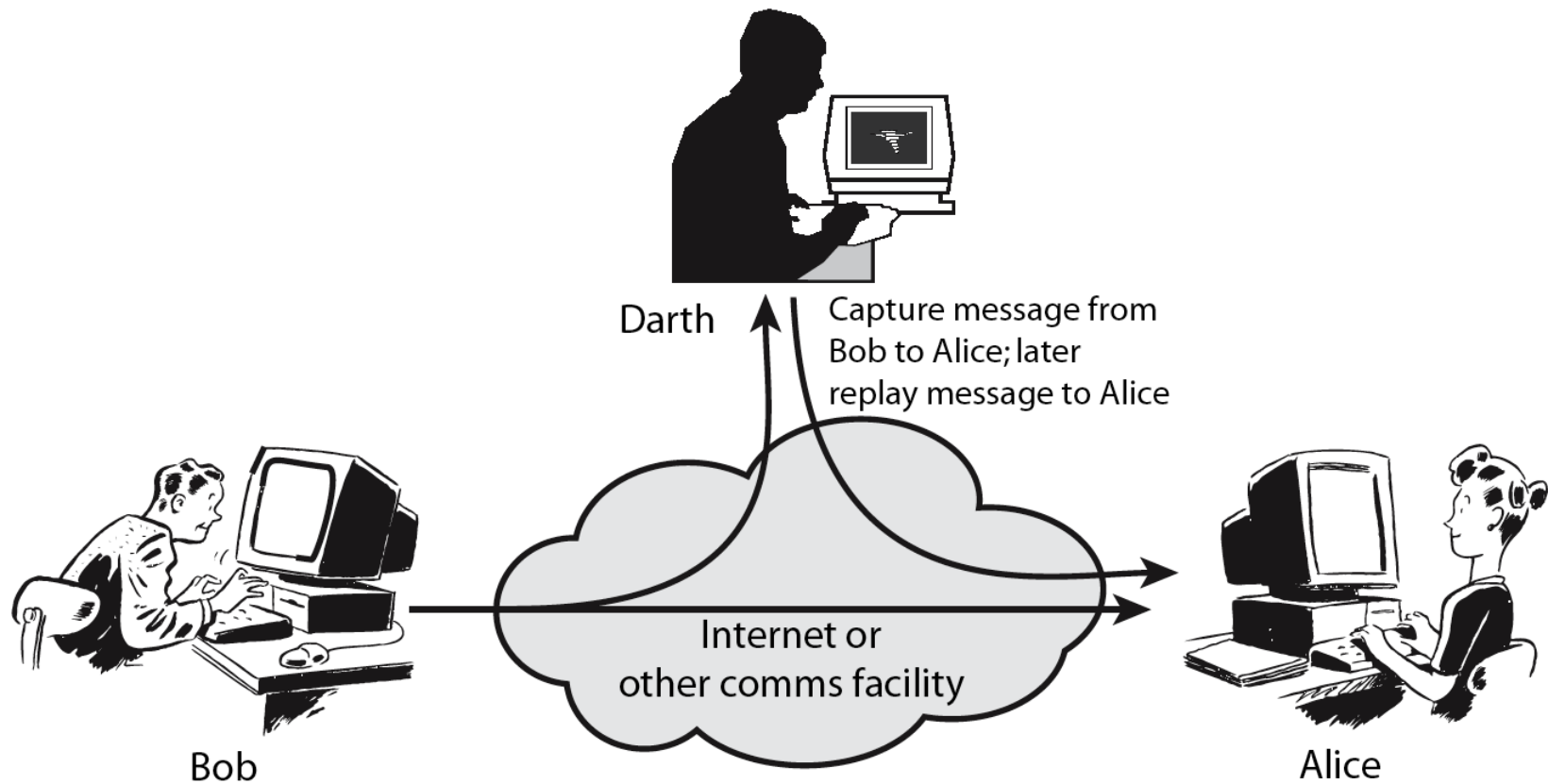
- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active



# Passive Attacks



# Active Attacks



# Security Service

---

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed



# Security Services

---

- X.800:

“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”
- RFC 2828:

“a processing or communication service provided by a system to give a specific kind of protection to system resources”





# Security Services (X.800)

---

- **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 is 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
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic



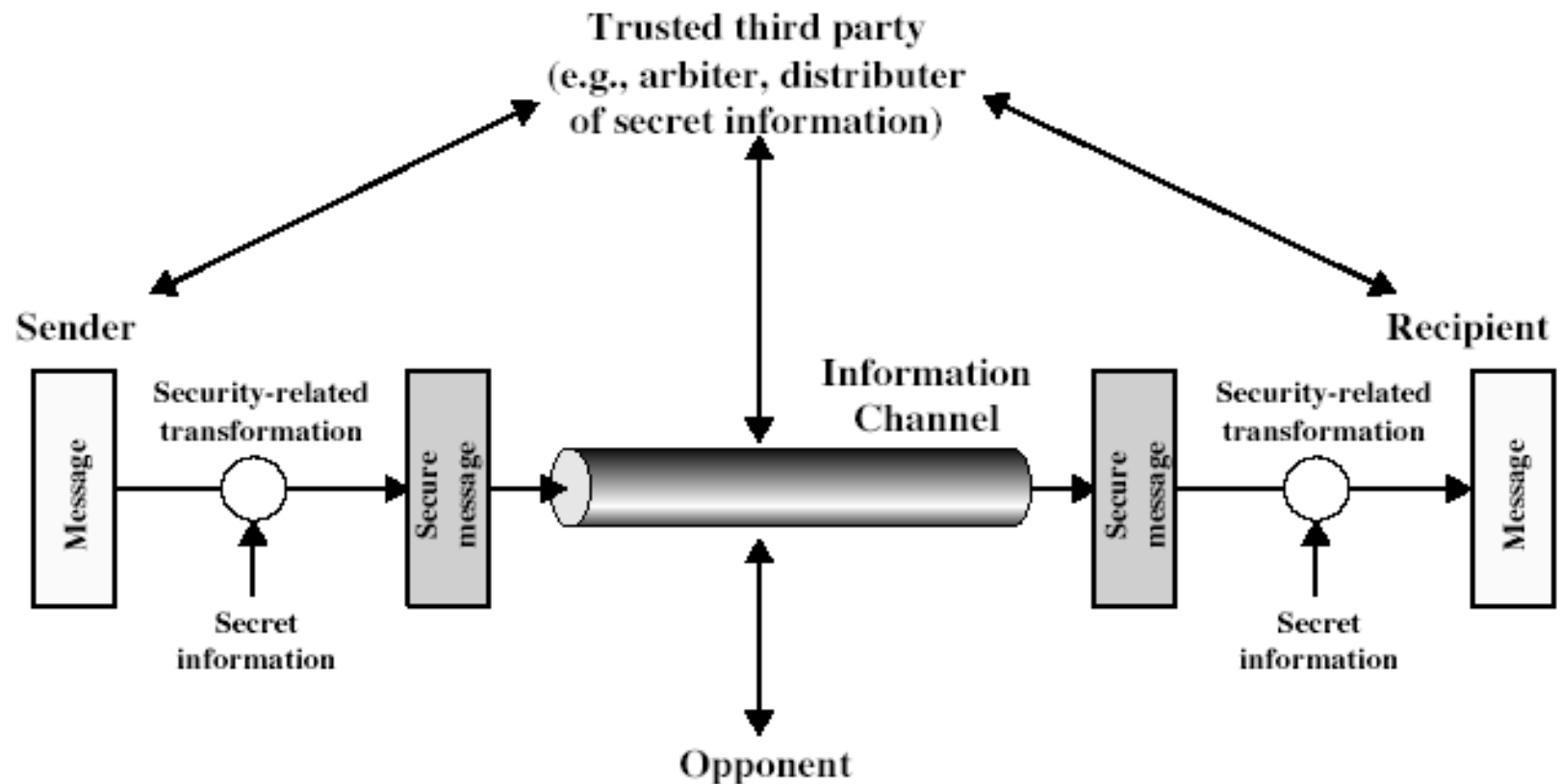
# Security Mechanisms (X.800)

---

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery



# Model for Network Security



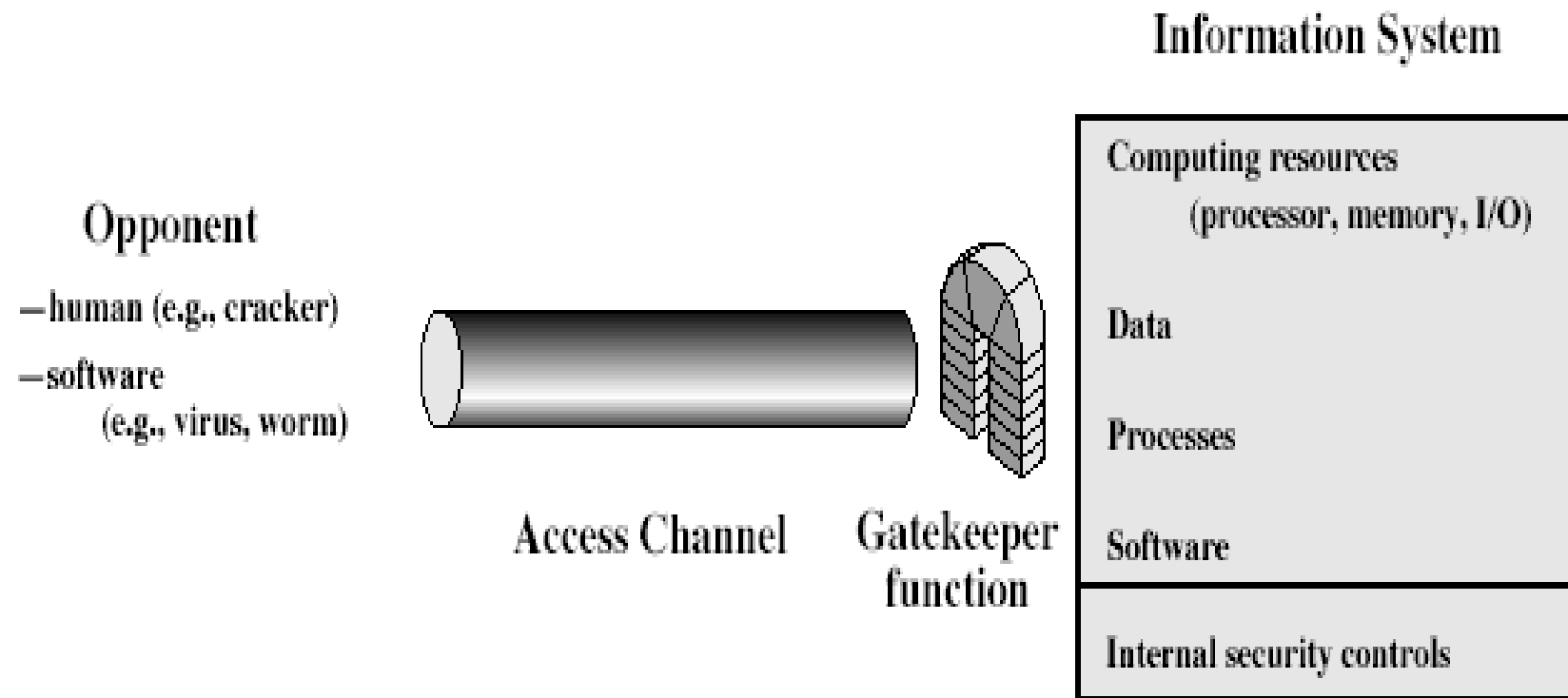
# Model for Network Security

---

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service



# Model for Network Access Security





# Model for Network Access Security

---

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems may be useful to help implement this model

# Classical Substitution Ciphers

---

- where letters of plaintext are replaced by other letters or by numbers or symbols
- or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns



# Caesar Cipher

---

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:

meet me after the toga party

PHHW PH DIWHU WKH WRJD SDUWB



# Caesar Cipher

- can define transformation as:

abcdefghijklmnopqrstuvwxyz  
DEFGHIJKLMNOPQRSTUVWXYZABC

- mathematically give each letter a number

abcdefghijklmnopqrstuvwxyz  
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:

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

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



# 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 "GCUA VQ DTGCM"



# Monoalphabetic Cipher

---

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA



# Monoalphabetic Cipher Security

---

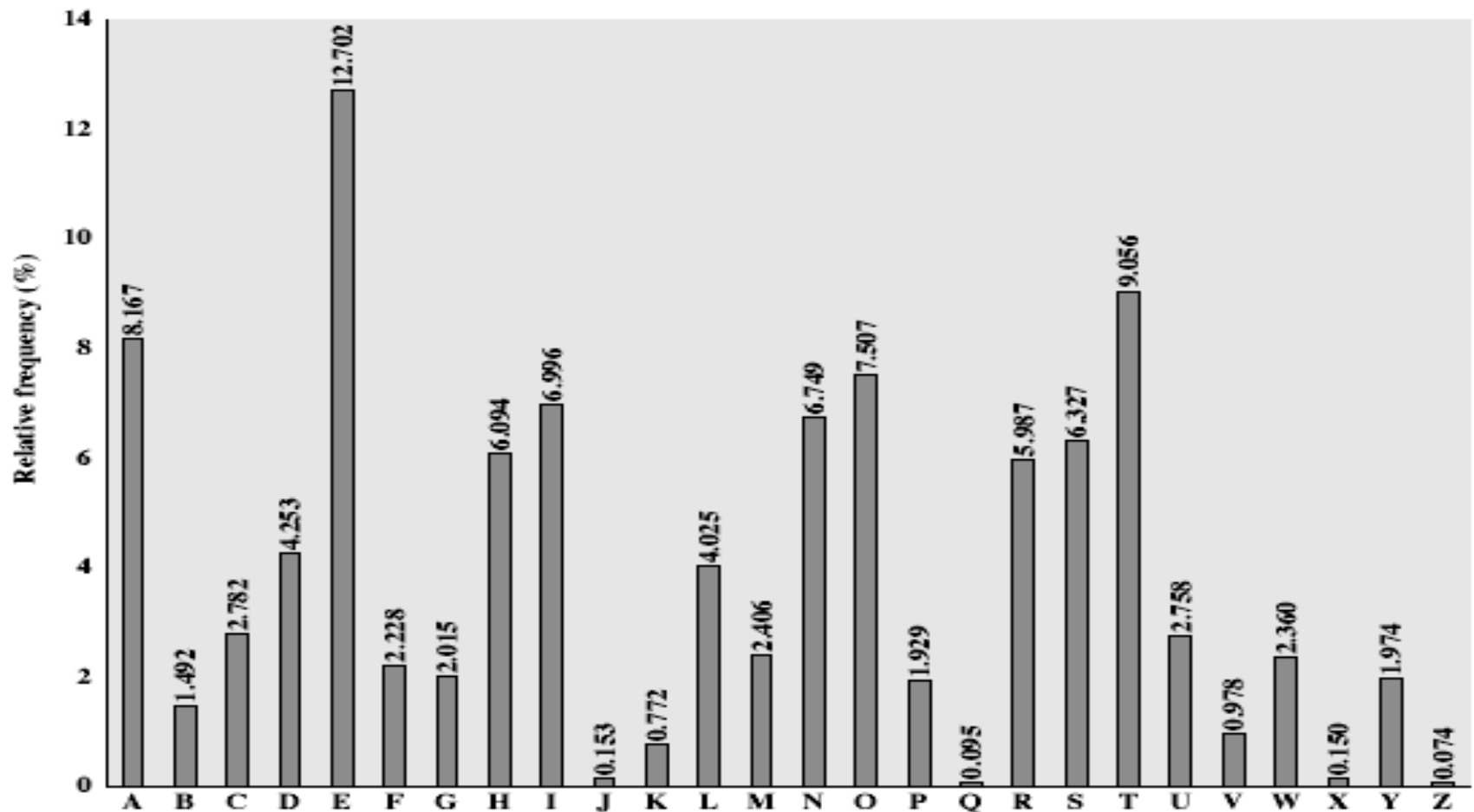
- now have a total of  $26! = 4 \times 10^{26}$  keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics



# Language Redundancy and Cryptanalysis

- human languages are **redundant**
- eg "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

# English Letter Frequencies



# Use in Cryptanalysis

---

- key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Arabian scientists in 9<sup>th</sup> century
- calculate letter frequencies for ciphertext
- compare counts/plots against known values
- if caesar cipher look for common peaks/troughs
  - peaks at: A-E-I triple, NO pair, RST triple
  - troughs at: JK, X-Z
- for monoalphabetic must identify each letter
  - tables of common double/triple letters help



# Example Cryptanalysis

- given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAI Z  
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX  
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- count relative letter frequencies (see text)
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:  
it was disclosed yesterday that several informal but  
direct contacts have been made with political  
representatives of the viet cong in moscow



# Hill cipher

---

- Hill cipher is a polygraphic substitution cipher based on linear algebra.
- Each letter is represented by a number modulo 26. Often the simple scheme  $A = 0, B = 1, \dots, Z = 25$  is used, but this is not an essential feature of the cipher.
- To encrypt a message, each block of  $n$  letters (considered as an  $n$ -component vector) is multiplied by an invertible  $n \times n$  matrix, against modulus 26.





- 
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
  - The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible  $n \times n$  matrices (modulo 26).

## Examples

**Input : Plaintext: ACT**

**Key: GYBNQKURP**

**Output : Ciphertext: POH**

# Encryption

- We have to encrypt the message 'ACT' (n=3).
- The key is 'GYBNQKURP' which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

- The message 'ACT' is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

- The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

- which corresponds to ciphertext of 'POH'

# Decryption

- To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters)

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \stackrel{-1}{\equiv} \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

- For the previous Ciphertext ‘POH’:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

- which gives us back ‘ACT’.

# 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
- the **Playfair Cipher** is an example
- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair



# Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- eg. 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



# Encrypting and Decrypting

- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X'
  2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
  4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair



# Security of Playfair Cipher

- security much improved over monoalphabetic
- since have  $26 \times 26 = 676$  digrams
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- and correspondingly more ciphertext
- was widely used for many years
  - eg. by US & British military in WW1
- it **can** be broken, given a few hundred letters
- since still has much of plaintext structure



# Polyalphabetic Ciphers

---

- **polyalphabetic substitution ciphers**
- improve security using multiple cipher alphabets
- make 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



# Vigenère Cipher

---

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long  $K = k_1 k_2 \dots k_d$
- $i^{\text{th}}$  letter specifies  $i^{\text{th}}$  alphabet to use
- use each alphabet in turn
- repeat from start after  $d$  letters in message
- decryption simply works in reverse



# Example of Vigenère Cipher

---

- write the plaintext out
- write the keyword repeated above it
- use each key letter as a caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

key:       deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

# One-Time Pad

---

- if a truly random key as long as the message is used, the cipher will be secure
- called a One-Time pad
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- can only use the key **once** though
- problems in generation & safe distribution of key



# Modern Block Ciphers

---

- now look at modern block ciphers
- one of the most widely used types of cryptographic algorithms
- provide secrecy /authentication services
- focus on DES (Data Encryption Standard)
- to illustrate block cipher design principles



# Block vs Stream Ciphers

---

- block ciphers process messages in blocks, each of which is then en/decrypted
- like a substitution on very big characters
  - 64-bits or more
- stream ciphers process messages a bit or byte at a time when en/decrypting
- many current ciphers are block ciphers
- broader range of applications



# Block Cipher Principles

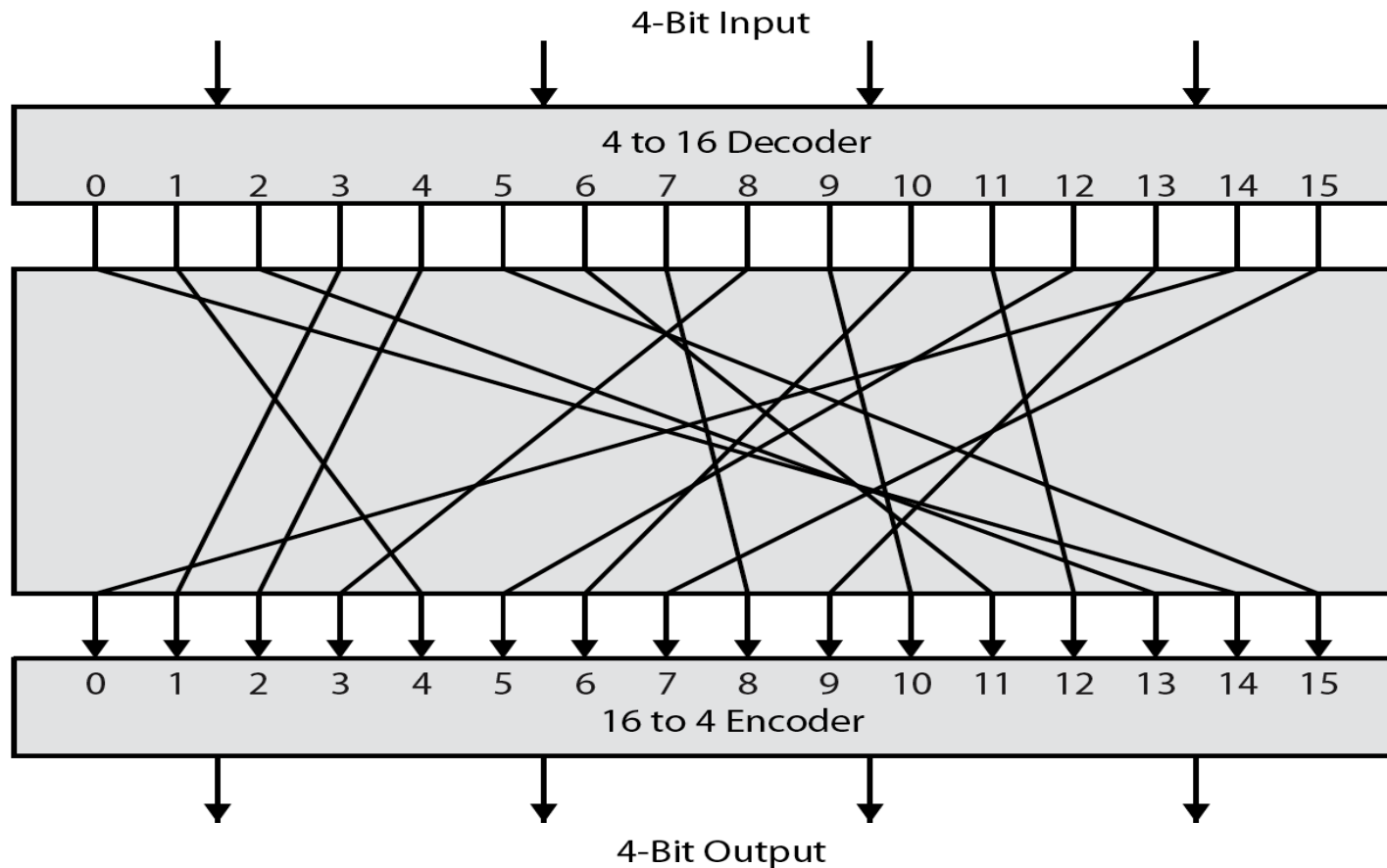
---

- most symmetric block ciphers are based on a **Feistel Cipher Structure**
- needed since must be able to **decrypt** ciphertext to recover messages efficiently
- block ciphers look like an extremely large substitution
- would need table of  $2^{64}$  entries for a 64-bit block
- instead create from smaller building blocks
- using idea of a product cipher





# Ideal Block Cipher



# Claude Shannon and Substitution-Permutation Ciphers

---

- Claude Shannon introduced idea of substitution-permutation (S-P) networks in 1949 paper
- form basis of modern block ciphers
- S-P nets are based on the two primitive cryptographic operations seen before:
  - *substitution* (S-box)
  - *permutation* (P-box)
- provide *confusion* & *diffusion* of message & key



# Confusion and Diffusion

---

- cipher needs to completely obscure statistical properties of original message
- a one-time pad does this
- more practically Shannon suggested combining S & P elements to obtain:
- **diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
- **confusion** – makes relationship between ciphertext and key as complex as possible

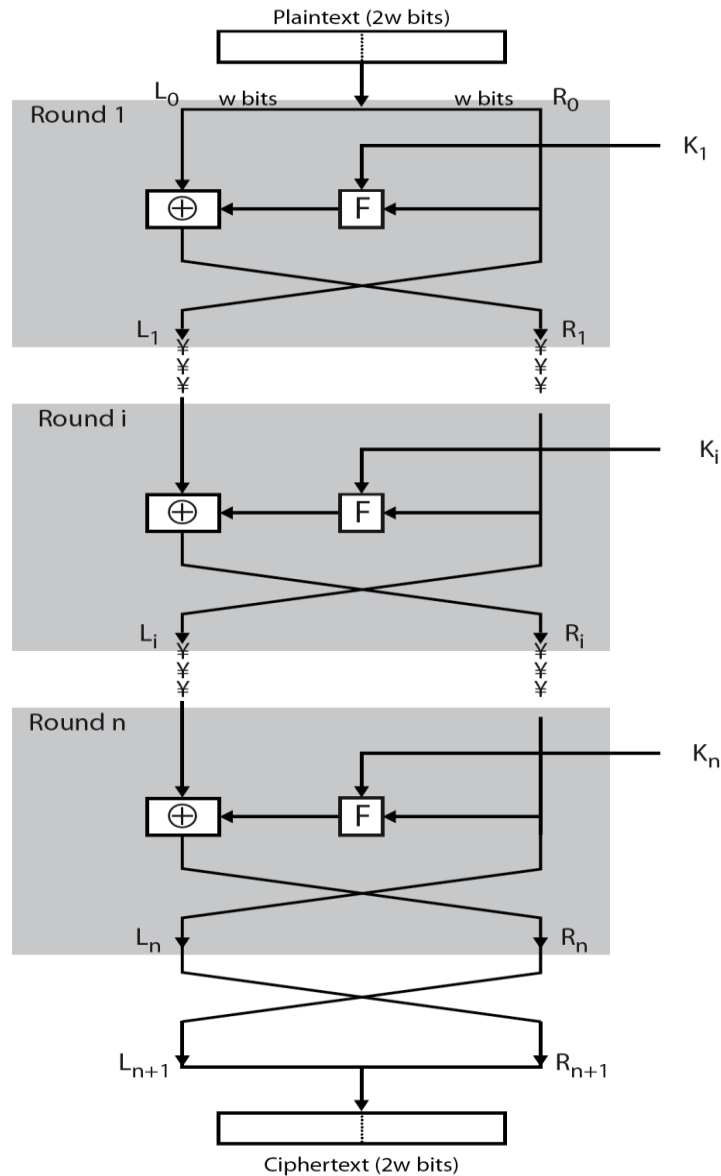
# Feistel Cipher Structure

---

- Horst Feistel devised the **feistel cipher**
  - based on concept of invertible product cipher
- partitions input block into two halves
  - process through multiple rounds which
  - perform a substitution on left data half
  - based on round function of right half & subkey
  - then have permutation swapping halves
- implements Shannon's S-P net concept



# Feistel Cipher Structure



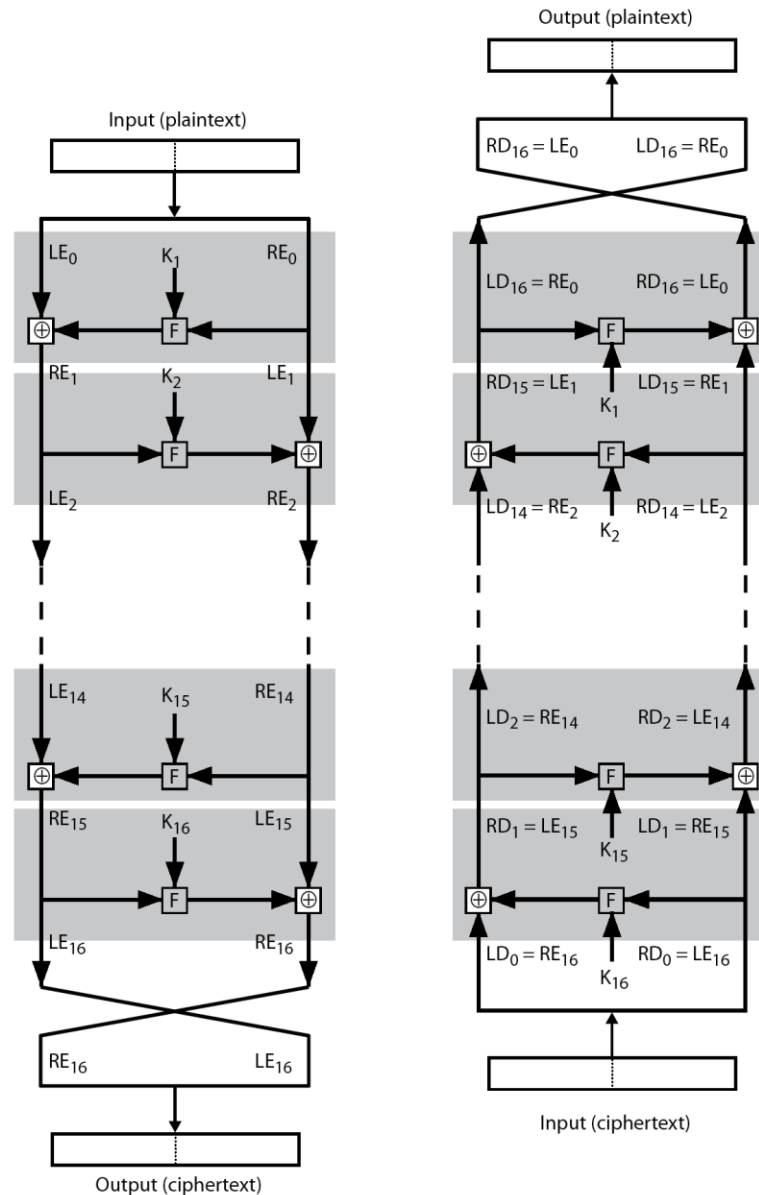
# Feistel Cipher Design Elements

---

- block size
- key size
- number of rounds
- subkey generation algorithm
- round function
- fast software en/decryption
- ease of analysis



# Feistel Cipher Decryption





# THANK YOU



**PRESIDENCY  
UNIVERSITY**

Private University Estd. in Karnataka State by Act No. 41 of 2013

