CS577: Introduction to Blockchain and Cryptocurrency

Introduction to Cryptography

Dr. Raju Halder

Introduction

What is Cryptology

- **cryptography**: The act or art of writing in secret characters.
- **cryptanalysis**: The analysis and deciphering of secret writings.
- **cryptology**: (Webster's) the scientific study of cryptography and cryptanalysis.

In our context **cryptology** is the scientific study of protection of information.

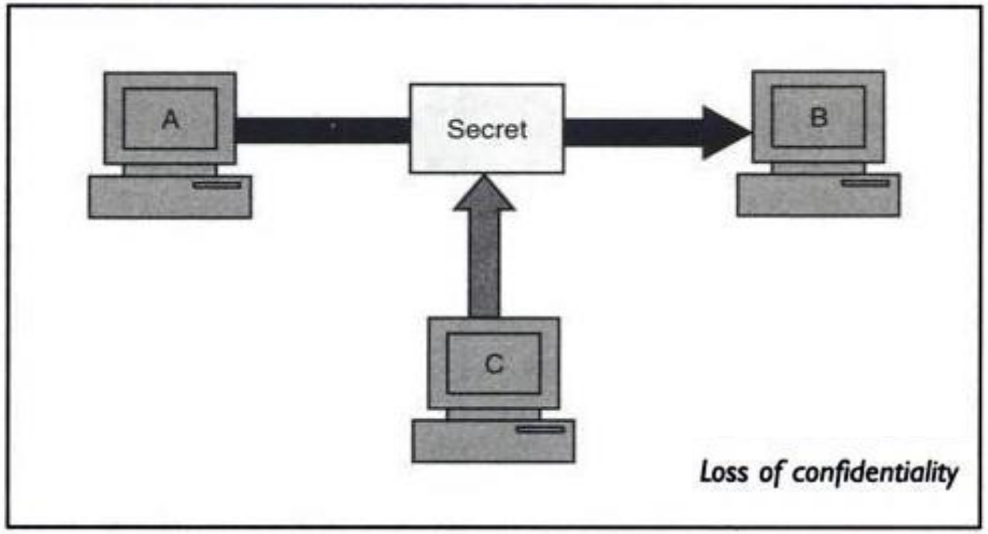
Applications

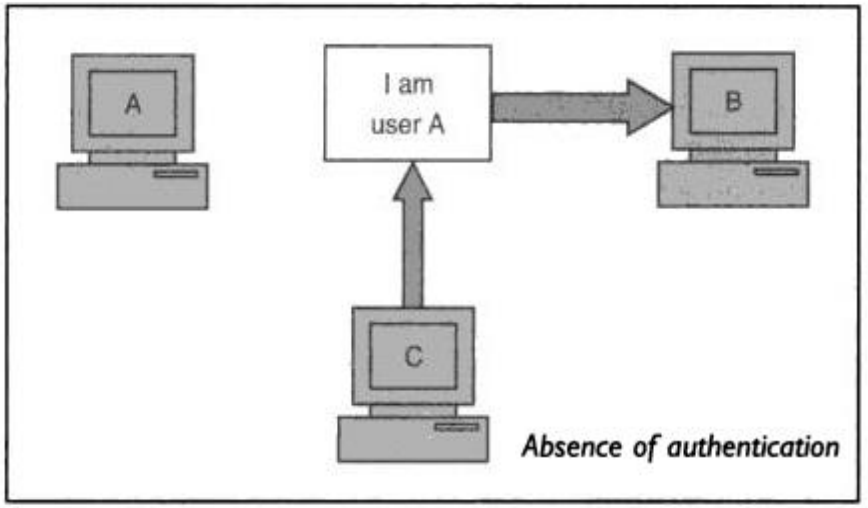
- Secure Communications (war-time)
- File and data base security
- Electronic funds transfer
- Electronic commerce
- Digital cash
- Contract signing
- Electronic mail
- Electronic voting
- Authentication: Passwords, PINs
- Secure identification, Access control
- Secure protocols

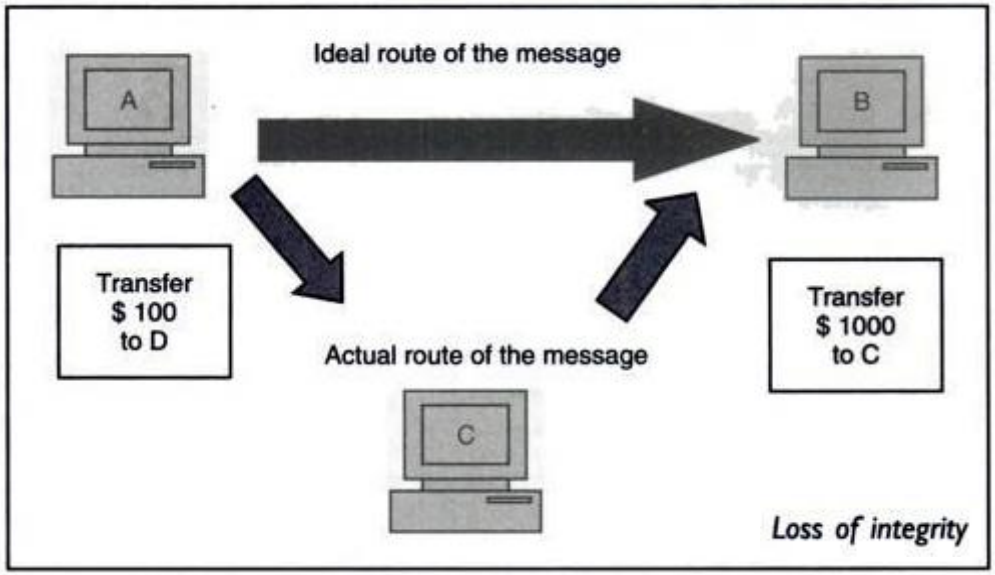
Principles of Security

- **Secrecy/Confidentiality**
  - Only intended receiver understands the message
- **Authentication**
  - Sender and receiver need to confirm each others identity
- **Message Integrity**
  - Ensure that their communication has not been altered, either maliciously or by accident during transmission
- **Nonrepudiation**
  - Sender should not be able to falsely deny that a message was sent
- **Availability (System)**
  - Ensure that the information concerned is readily accessible to the authorized viewer at all times

Principles of Security

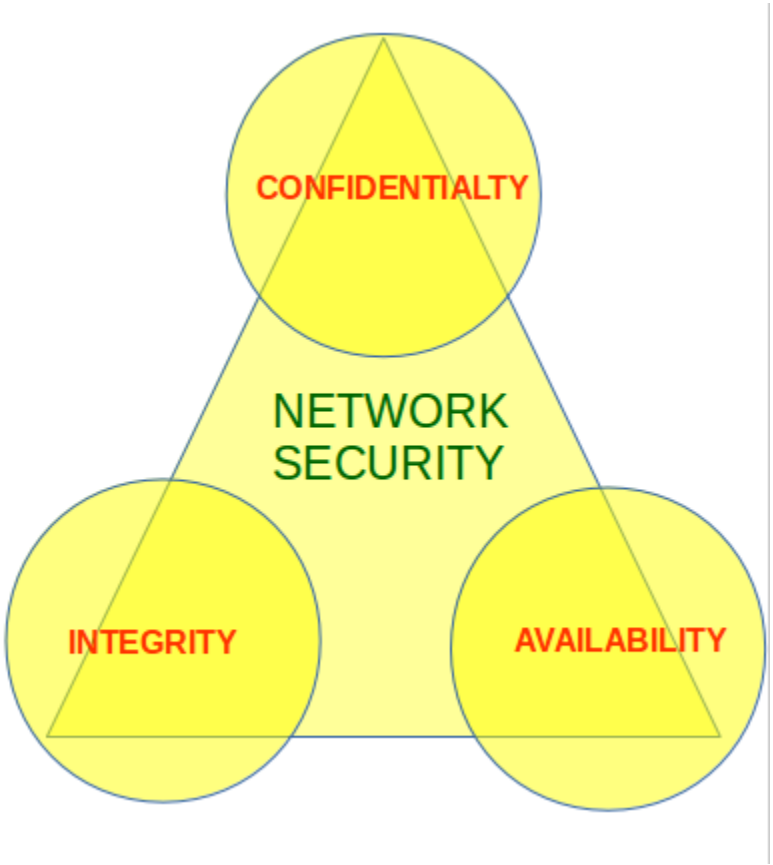






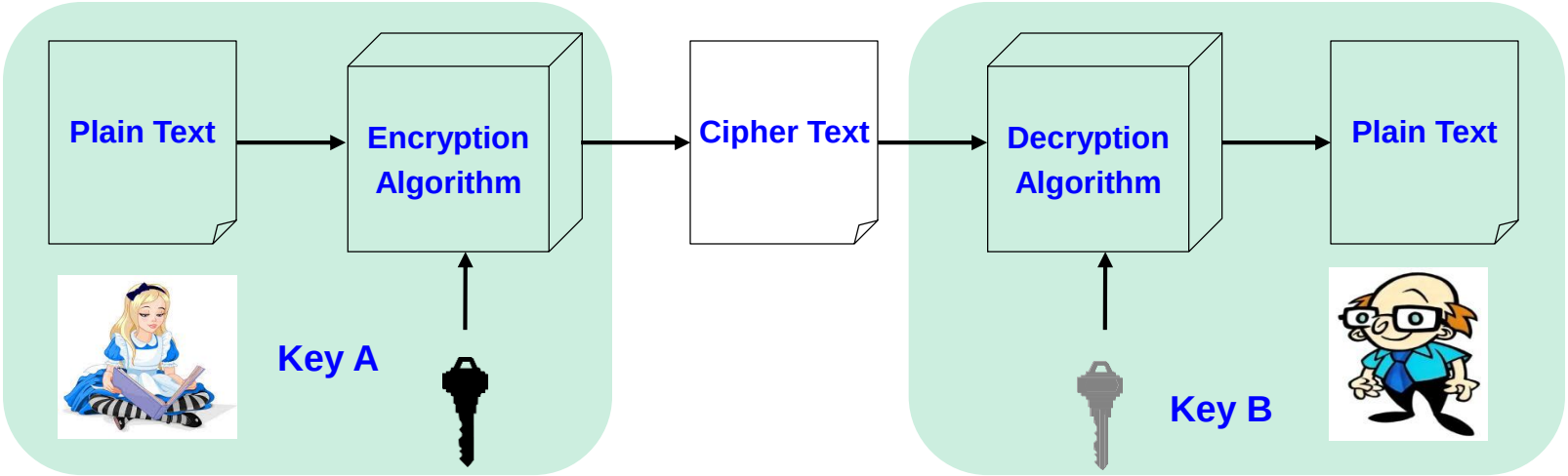
The CIA triad in Cryptography

- Three Fundamental Principles



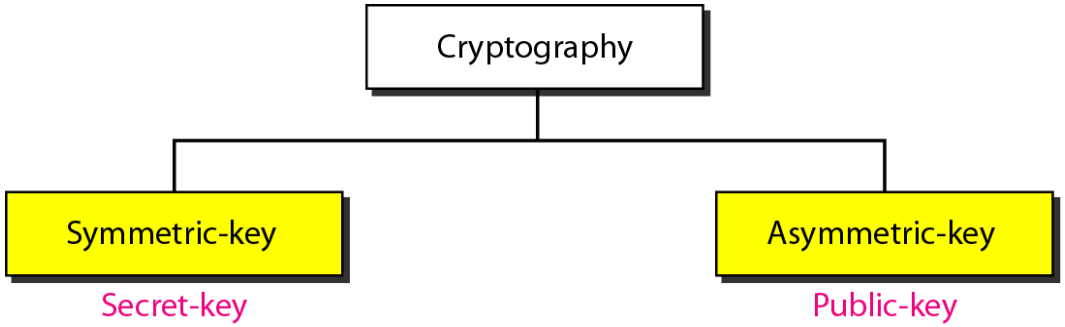
Cryptography components: Cipher

- Cipher is a method for encrypting messages



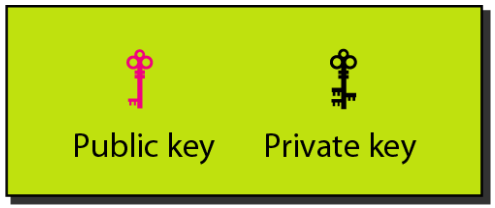
- Encryption algorithms are standardized & published
- The key which is an input to the algorithm is secret
  - Key is a string of numbers or characters
  - If same key is used for encryption & decryption the algorithm is called symmetric
  - If different keys are used for encryption & decryption the algorithm is called asymmetric

Categories of cryptography



Keys used in cryptography

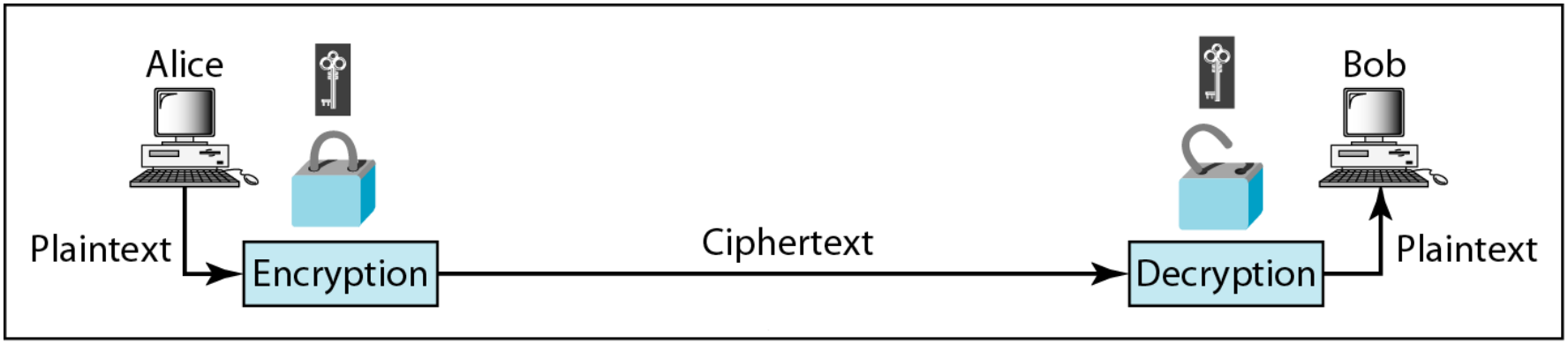
Symmetric-key cryptography



Asymmetric-key cryptography

Symmetric-key cryptography

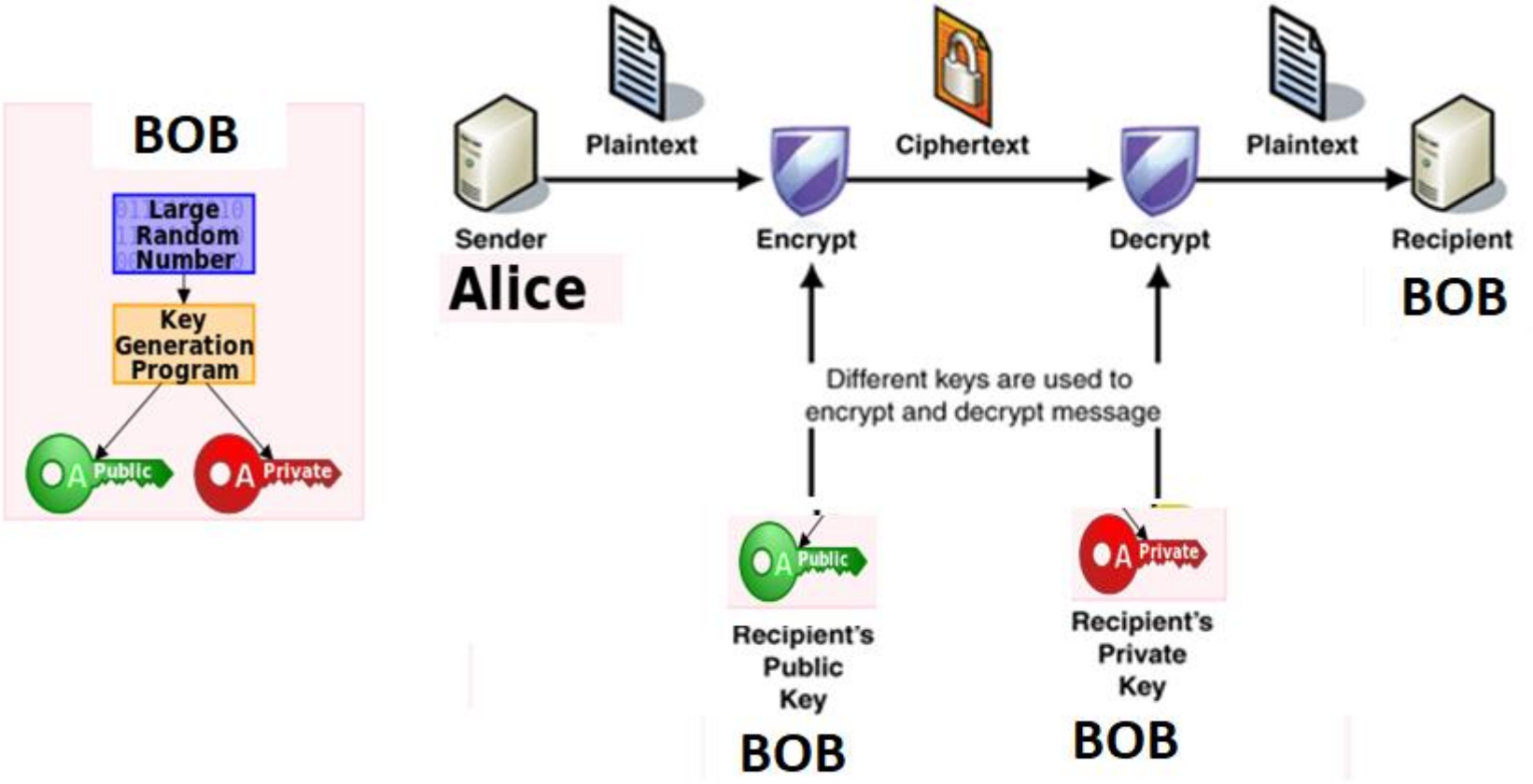
Symmetric-key cryptography



a. Symmetric-key cryptography

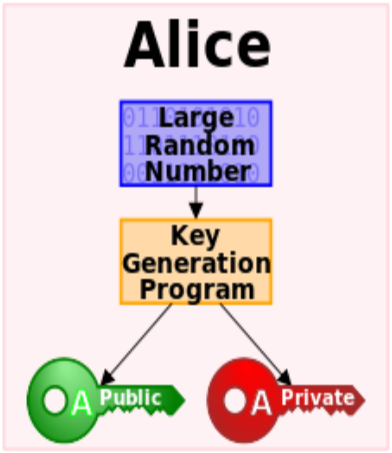
Digital Signatures

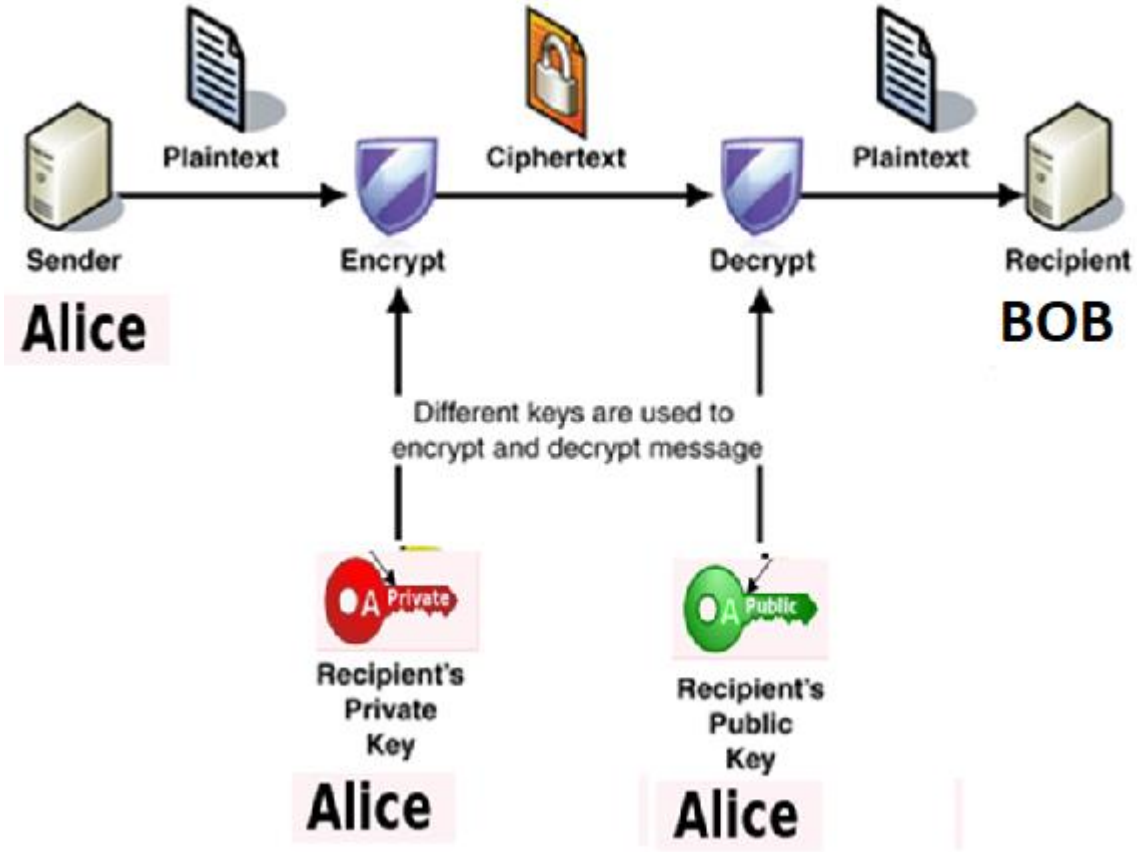
Asymmetric Key Cryptography



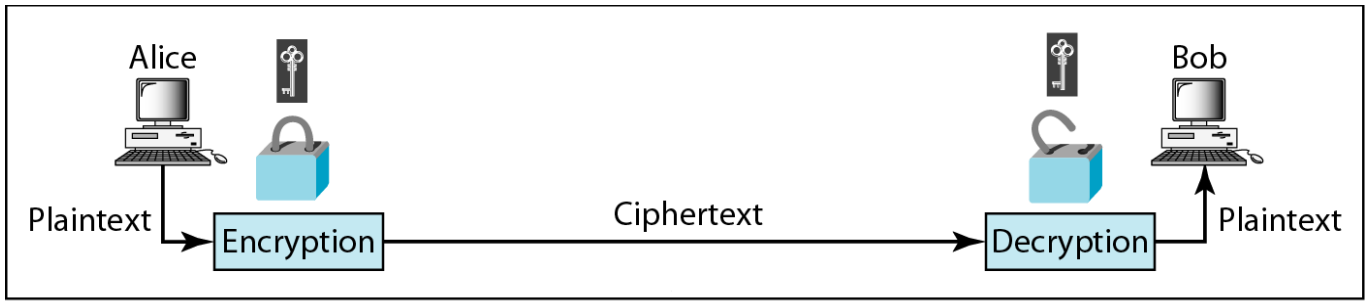
Digital Signatures

Asymmetric Key Cryptography

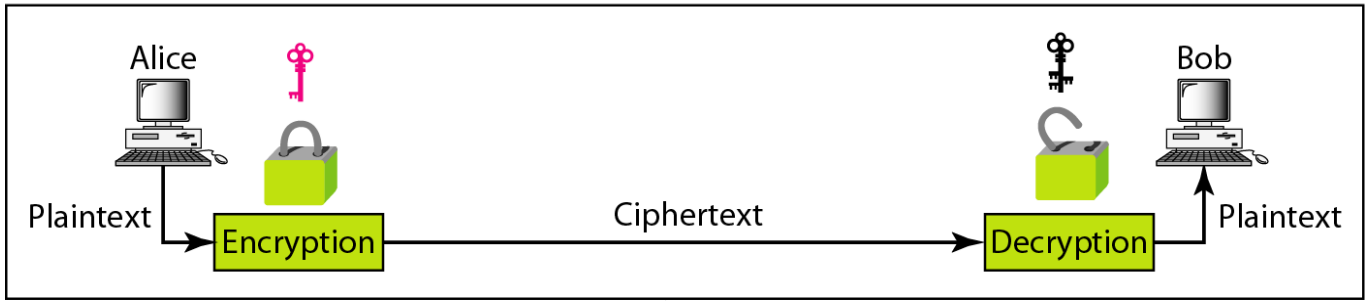




Comparison between two categories of cryptography



a. Symmetric-key cryptography



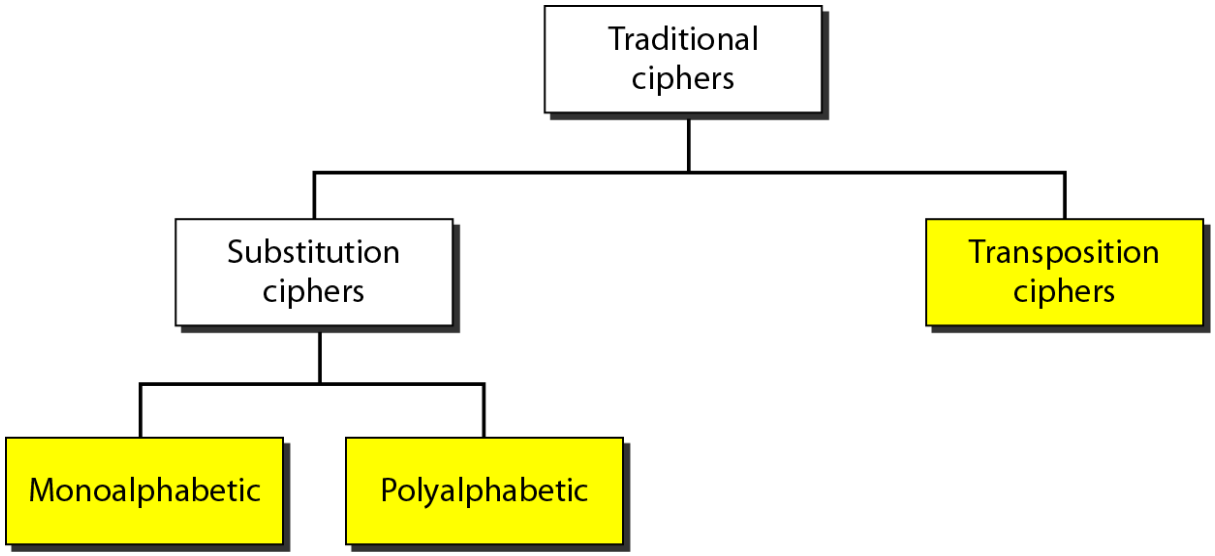
b. Asymmetric-key cryptography

SYMMETRIC-KEY CRYPTOGRAPHY

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.

Traditional Ciphers
Simple Modern Ciphers
Modern Round Ciphers
Mode of Operation

Traditional ciphers



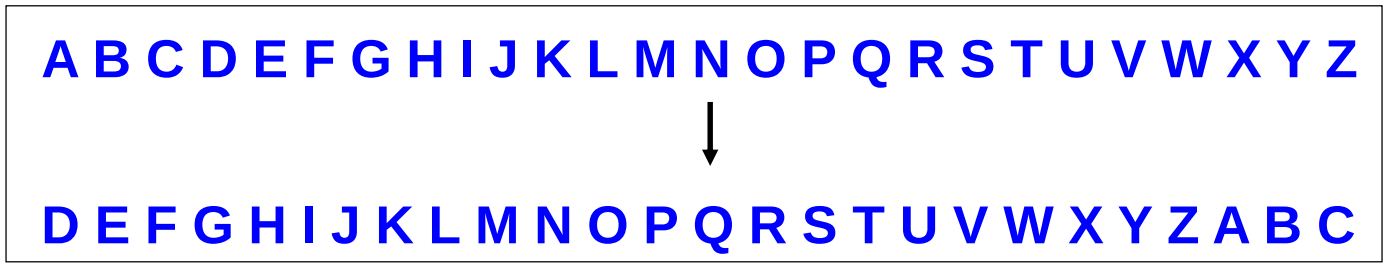
Note

A substitution cipher replaces one symbol with another.

Substitution Ciphers

Caesar Cipher

- Caesar Cipher is a method in which each letter in the alphabet is rotated by three letters as shown

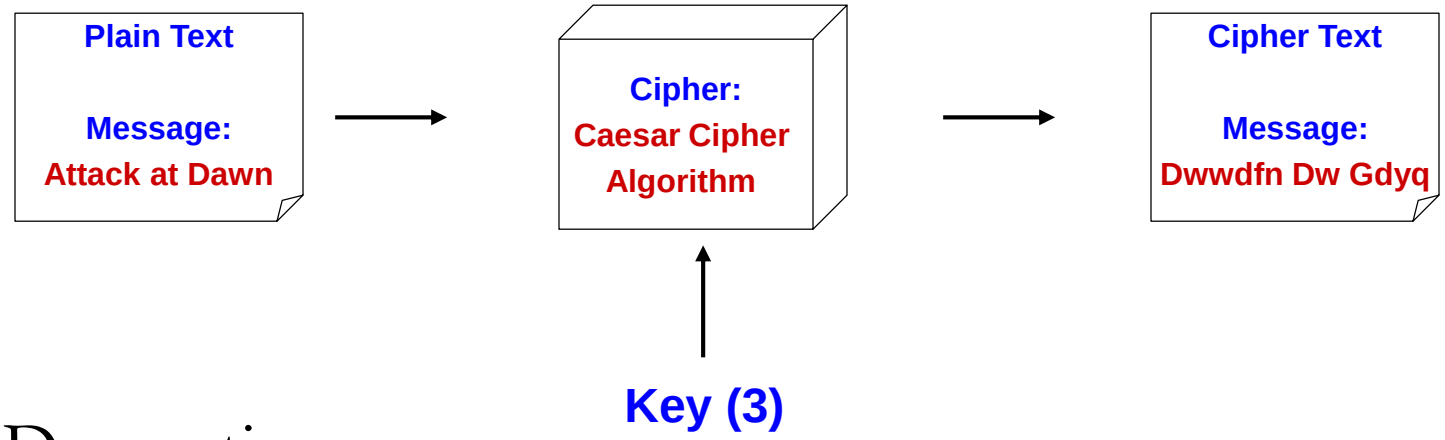


- Let us try to encrypt the message
  - "Attack at Dawn"

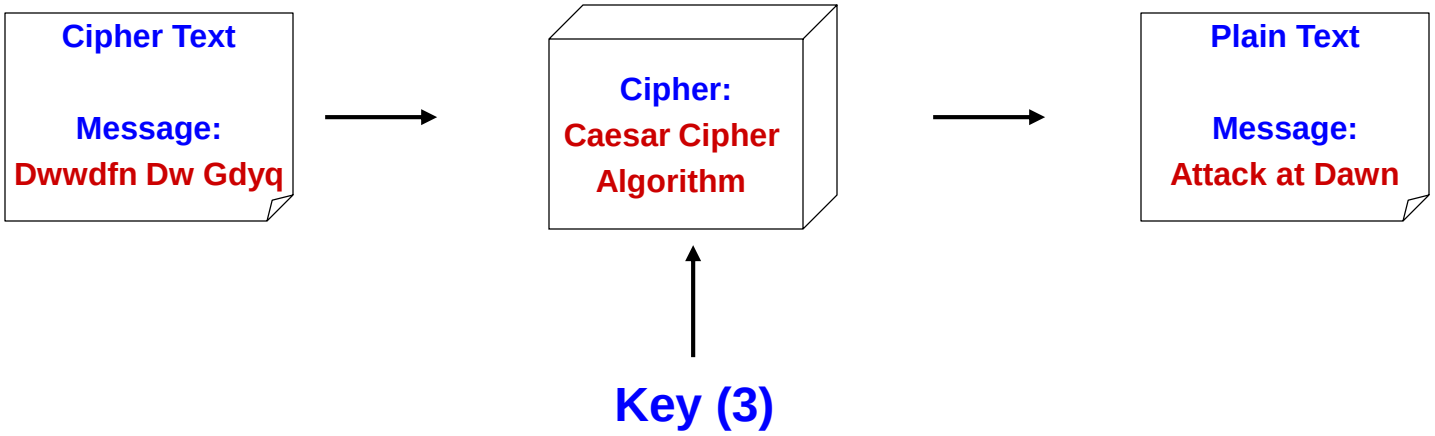
Substitution Ciphers

Caesar Cipher

Encryption



Decryption



How many different keys are possible?

Cæsar cipher

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	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

Cæsar cipher

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
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

shift alphabet by n (6)

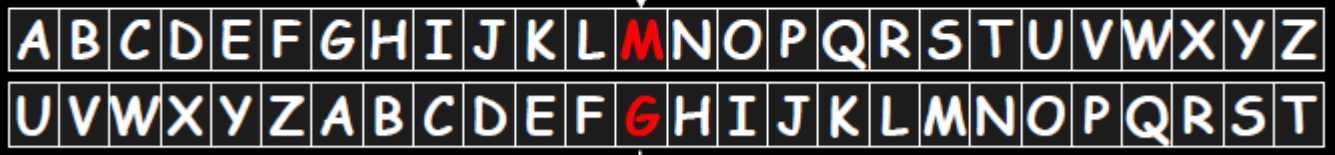
Cæsar cipher

MY CAT HAS FLEAS

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
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

Cæsar cipher

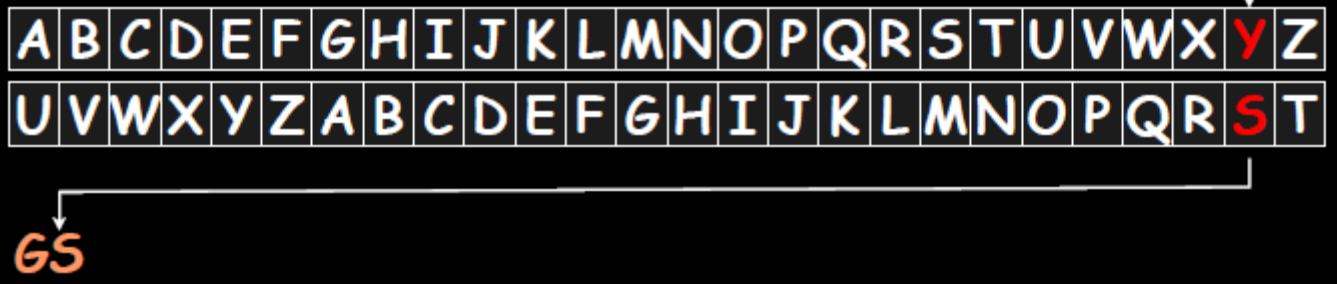
MY CAT HAS FLEAS



G

Cæsar cipher

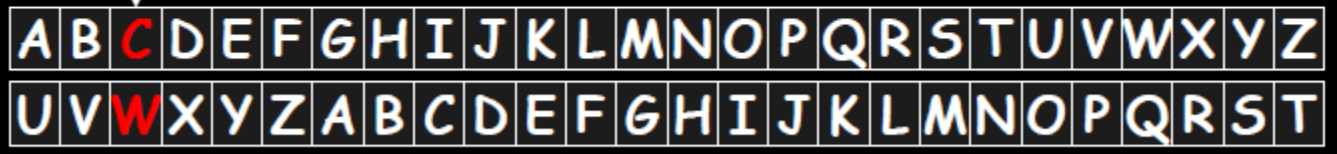
MY CAT HAS FLEAS



GS

Cæsar cipher

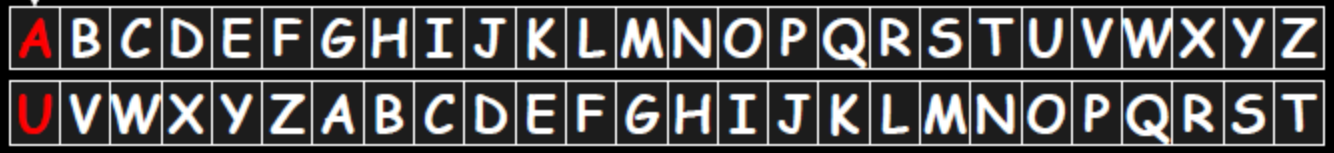
MY CAT HAS FLEAS



GSW

Cæsar cipher

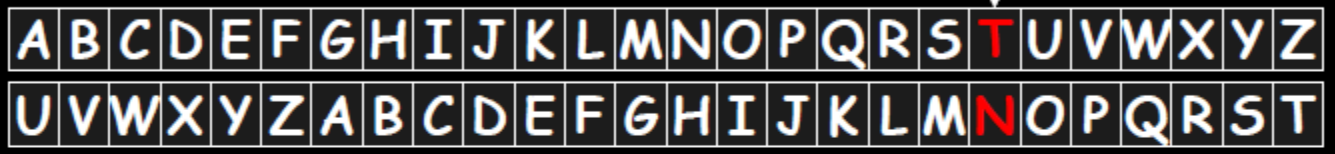
MY CAT HAS FLEAS



GSWU

Cæsar cipher

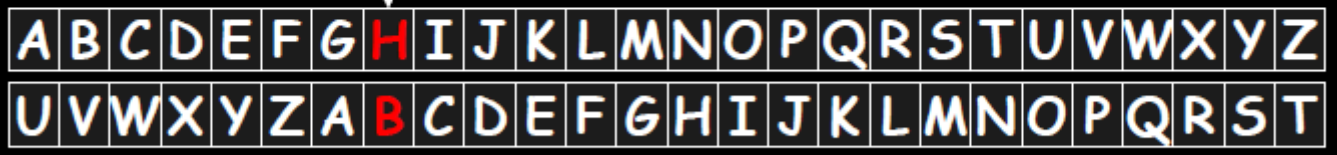
MY CAT HAS FLEAS



GSWUN

Cæsar cipher

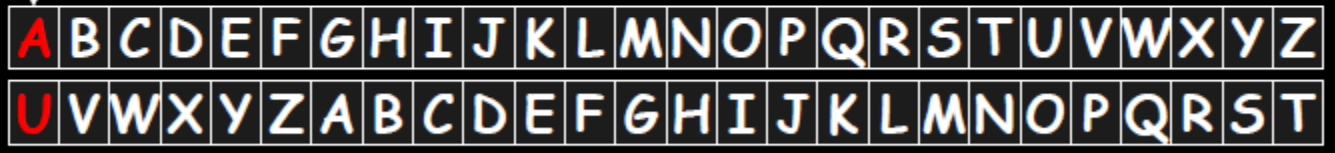
MY CAT HAS FLEAS



GSWUNB

Cæsar cipher

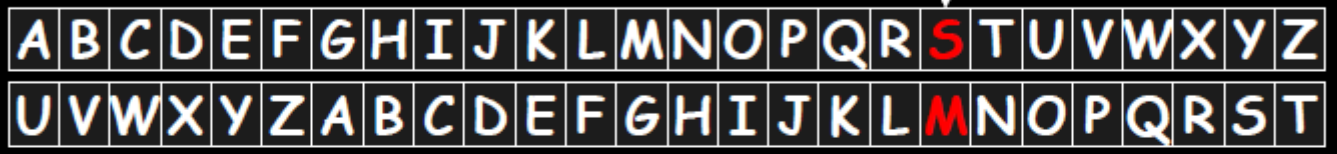
MY CAT HAS FLEAS



GSWUNBU

Cæsar cipher

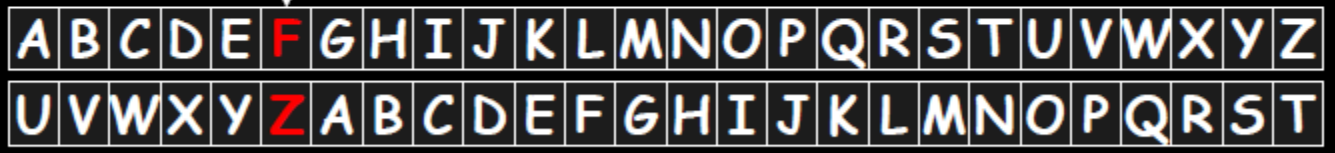
MY CAT HAS FLEAS



GSWUNBUM

Cæsar cipher

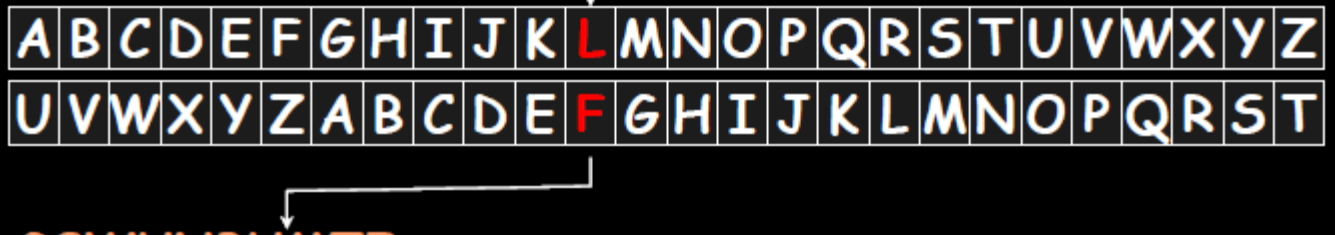
MY CAT HAS FLEAS



GSWUNBUMZ

Cæsar cipher

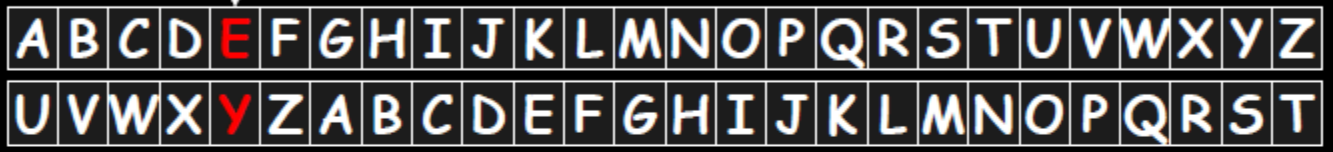
MY CAT HAS FLEAS



GSWUNBUMZF

Cæsar cipher

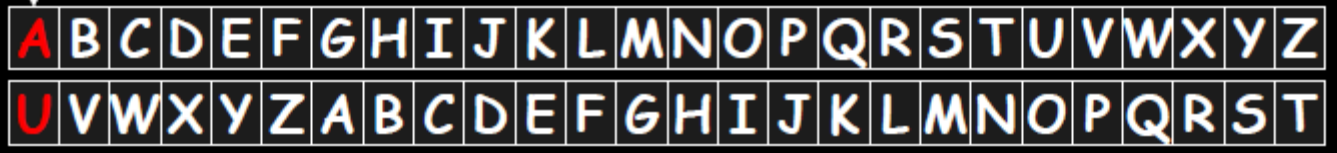
MY CAT HAS FLEAS



GSWUNBUMZFY

Cæsar cipher

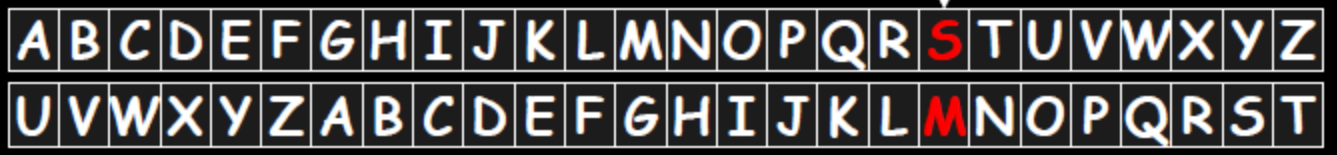
MY CAT HAS FLEAS



GSWUNBUMZFYU

Cæsar cipher

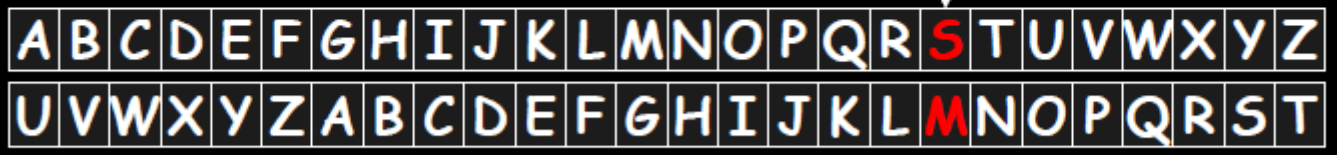
MY CAT HAS FLEAS



GSWUNBMUFZYUM

Cæsar cipher

MY CAT HAS FLEAS



GSWUNBMUFZYUM

- Convey one piece of information for decryption: *shift value*
- trivially easy to crack (26 possibilities for a 26 character alphabet)

Substitution Cipher

Monoalphabetic Cipher

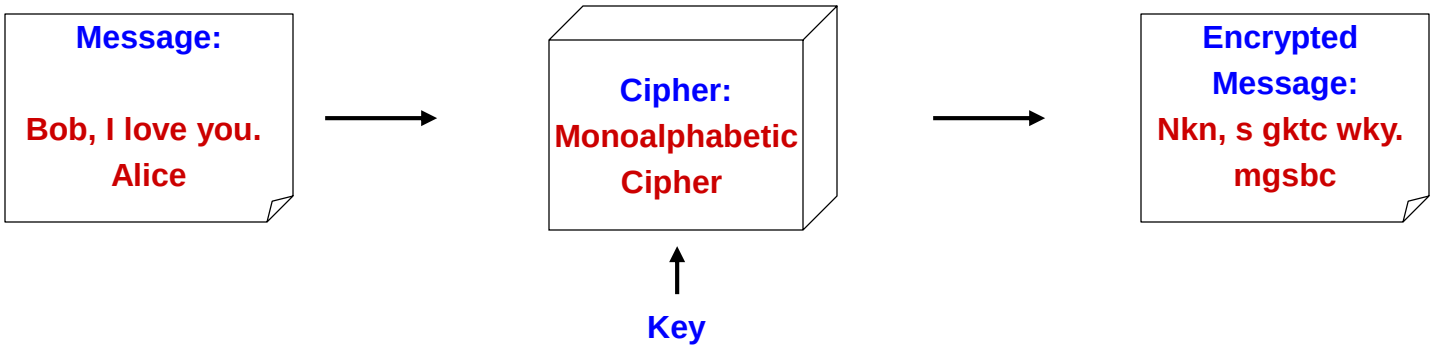
- Any letter can be substituted for any other letter
  - Each letter has to have a unique substitute

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

↓

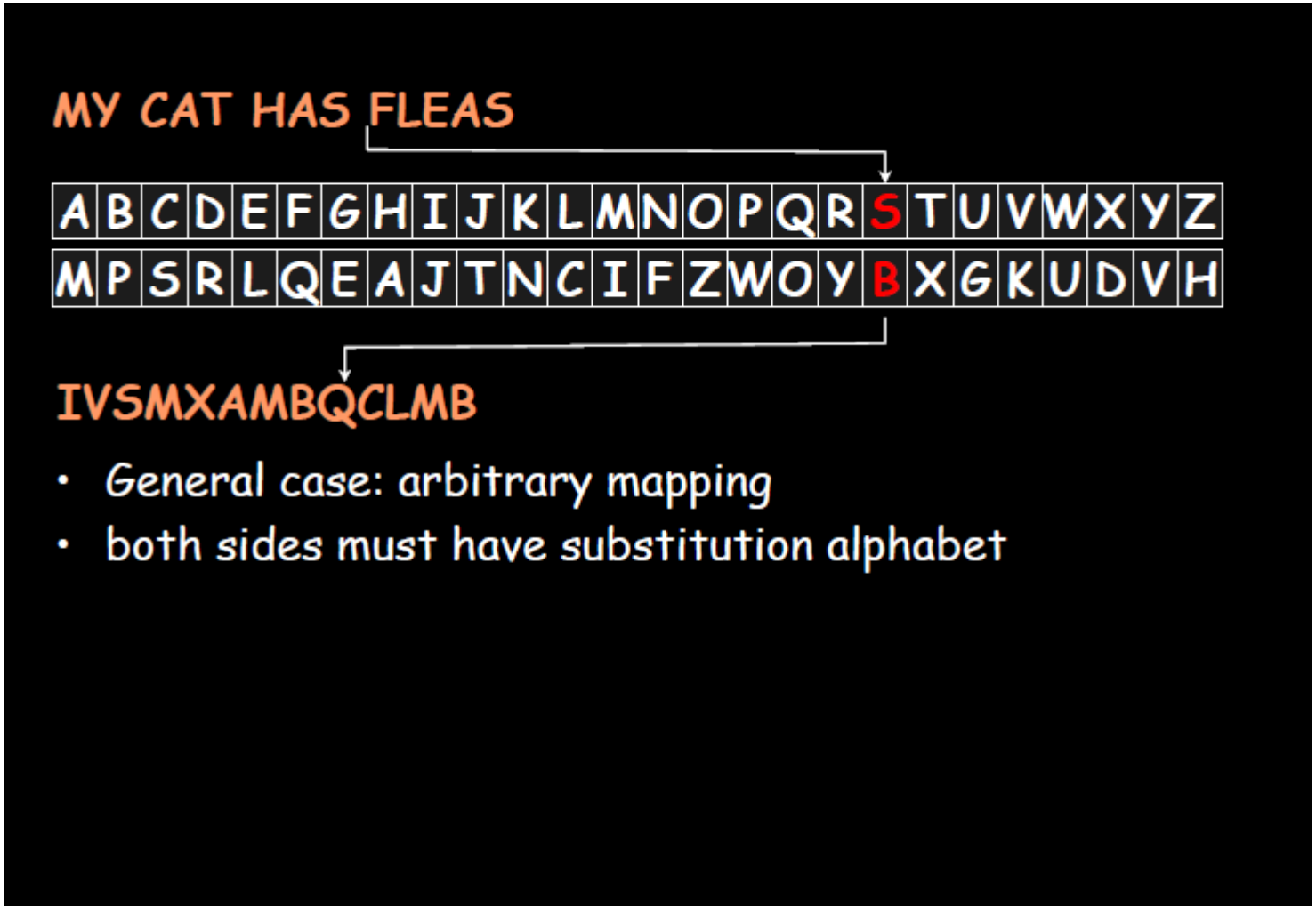
M N B V C X Z A S D F G H J K L P O I U Y T R E W Q

- There are 26! pairing of letters ($\sim 10^{26}$)
- Brute Force approach would be too time consuming
  - Statistical Analysis would make it feasible to crack the key



Substitution Cipher

Monoalphabetic Cipher



Substitution Cipher

Monoalphabetic Cipher

Statistical Analysis

Letter frequencies

- E: 12%
- A, H, I, N, O, R, S, T: 6 – 9%
- D, L: 4%
- B, C, F, G, M, P, U, W, Y: 1.5 – 2.8%
- J, K, Q, V, X, Z: < 1%

Common digrams:

- TH, HE, IN, ER, AN, RE, …

Common trigrams

- THE, ING, AND, HER, ERE, …

Substitution Cipher

Polyalphabetic Caesar Cipher

- Developed by Blaise de Vigenere
  - Also called Vigenere cipher
- Use table and key word to encipher a message
  - repeat keyword over text: (e.g. key=FACE)

    FA CEF ACE FACEF ....

    MY CAT HAS FLEAS
- encrypt: find intersection:
  - row = keyword letter
  - column = plaintext letter
- decrypt: column = keyword letter, search for intersection = ciphertext letter
- message is encrypted with as many substitution ciphers as there are letters in the keyword

Vigenère polyalphabetic cipher

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

R

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY 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
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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EE

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY H

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY HC

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY HCW

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY HCW K

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY HCW KL

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY HCW KLG

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY HCW KLGE

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

FA CEF ACE FACEF

~~MY CAT HAS FLEAS~~

RY EEY HCW KLGEX

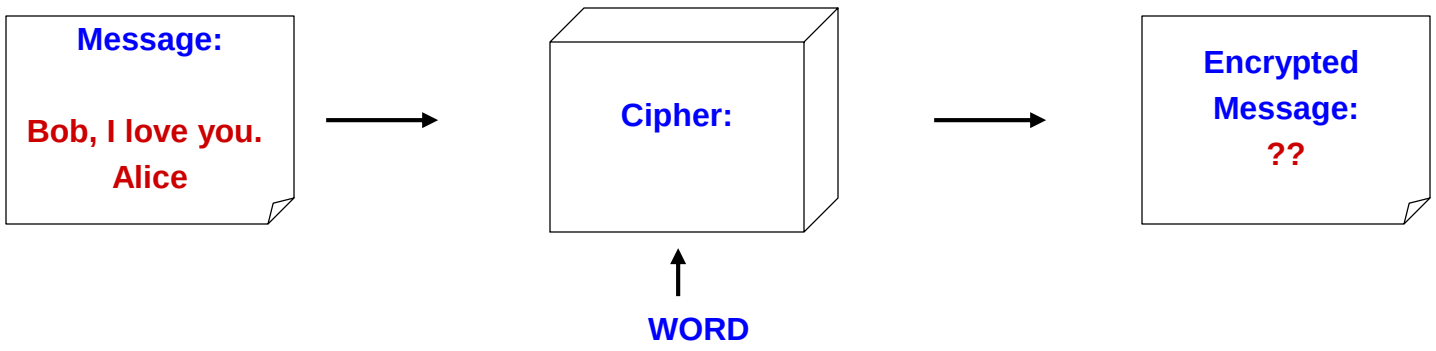
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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

Substitution Cipher

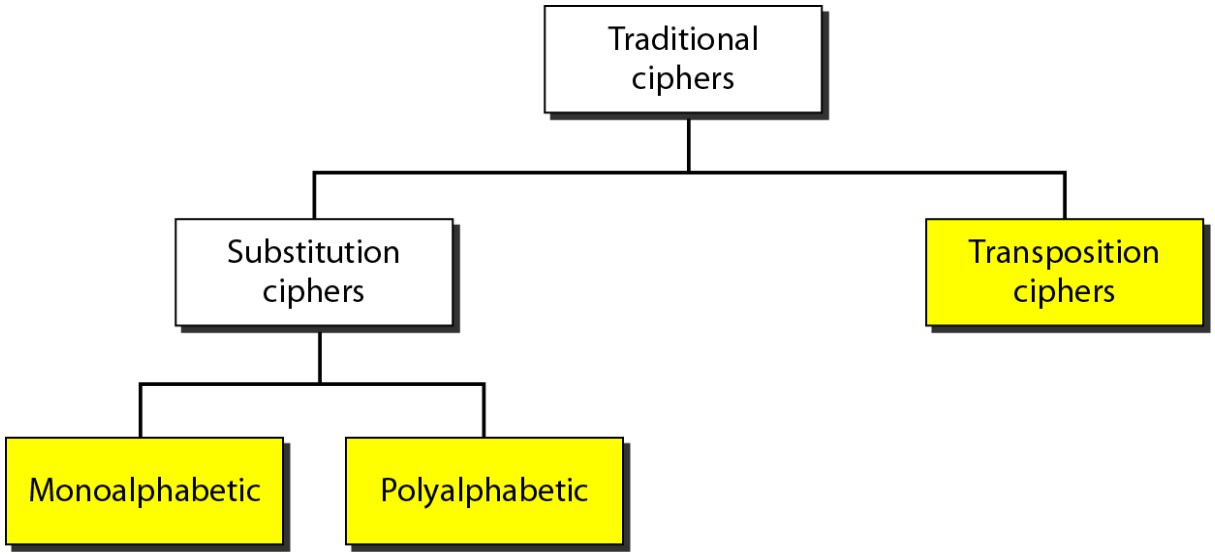
Using a key to shift alphabet

- Obtain a key to for the algorithm and then shift the alphabets
  - For instance if the key is 'word' we will shift all the letters by four and remove the letters w, o, r, & d from the encryption
- We have to ensure that the mapping is one-to-one
  - no single letter in plain text can map to two different letters in cipher text
  - no single letter in cipher text can map to two different letters in plain text

Plain Text	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
	↓
C1(k=6)	W O R D A B C E F G H I J K L M N P Q S T U V X Y Z



Traditional ciphers



Transposition Cipher

Columnar Transposition

- This involves rearrangement of characters on the plain text into columns
- The following example shows how letters are transformed
  - If the letters are not exact multiples of the transposition size there may be a few short letters in the last column which can be padded with an infrequent letter such as x or z

Plain Text	Cipher Text
T H I S I	T S S O H
S A M E S	O A N I W
S A G E T	H A A S O
O S H O W	L R S T O
H O W A C	I M G H W
O L U M N	U T P I R
A R T R A	S E E O A
N S P O S	M R O O K
I T I O N	I S T W C
W O R K S	N A S N S

Ciphers

Shannon's Characteristics of "Good" Ciphers

- The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
- The set of keys and the enciphering algorithm should be free from complexity.
- The implementation of the process should be as simple as possible.
- Errors in ciphering should not propagate and cause corruption of further information in the message.
- The size of the enciphered text should be no larger than the text of the original message.

Encryption Systems

Properties of Trustworthy Systems

- It is based on sound mathematics.
  - Good cryptographic algorithms are are derived from solid principles.
- It has been analyzed by competent experts and found to be sound.
  - Since it is hard for the writer to envisage all possible attacks on the algorithm
- It has stood the "test of time."
  - Over time people continue to review both mathematical foundations of an algorithm and the way it builds upon those foundations.
  - The flaws in most algorithms are discovered soon after their release.

Cryptanalysis

Techniques

- Cryptanalysis is the process of breaking an encryption code
  - Tedious and difficult process
- Several techniques can be used to deduce the algorithm
  - Attempt to recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straightforward decryption algorithm
  - Attempt to infer some meaning without even breaking the encryption, such as noticing an unusual frequency of communication or determining something by whether the communication was short or long
  - Attempt to deduce the key, in order to break subsequent messages easily
  - Attempt to find weaknesses in the implementation or environment of use of encryption
  - Attempt to find general weaknesses in an encryption algorithm, without necessarily having intercepted any messages

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