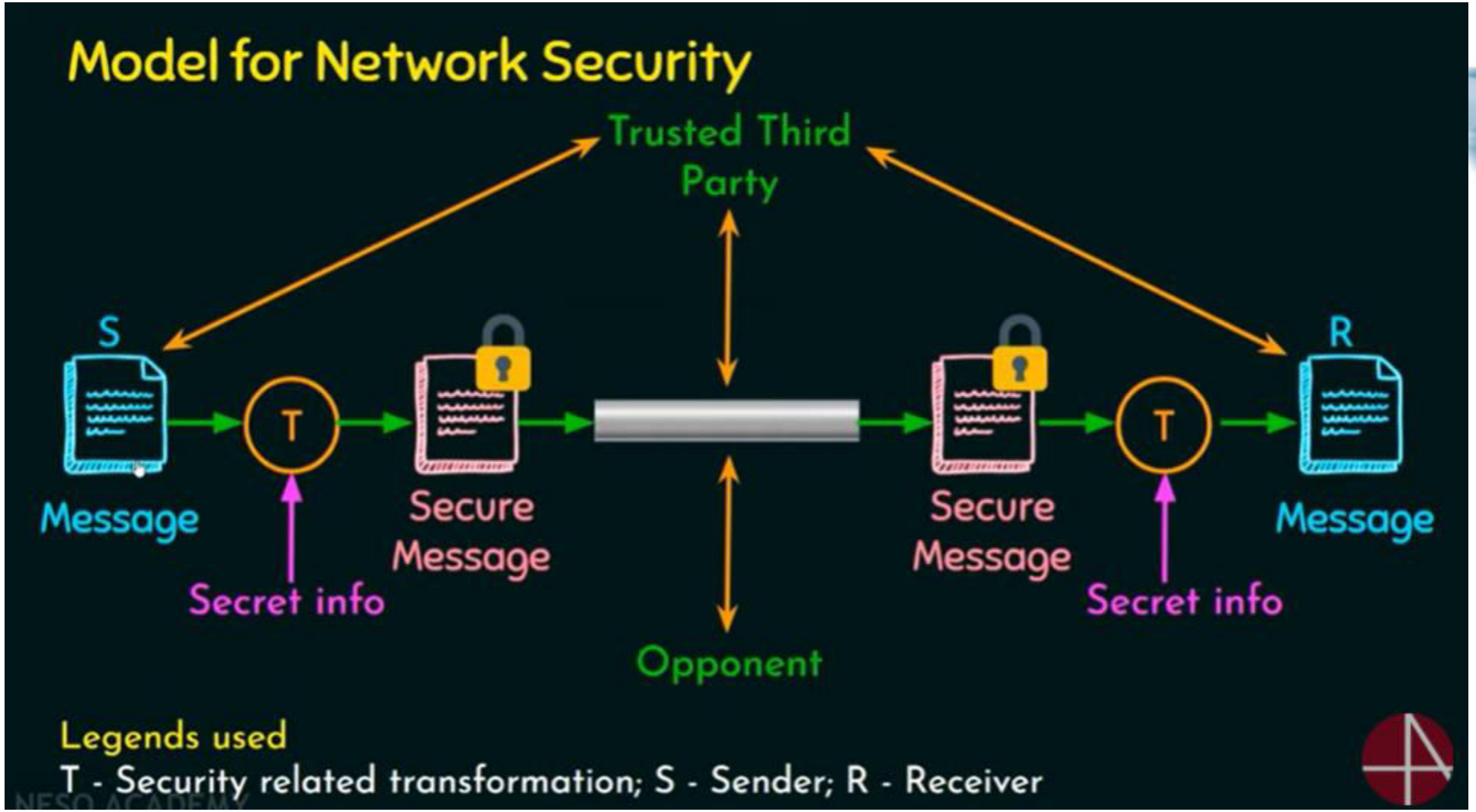
CSE 4215

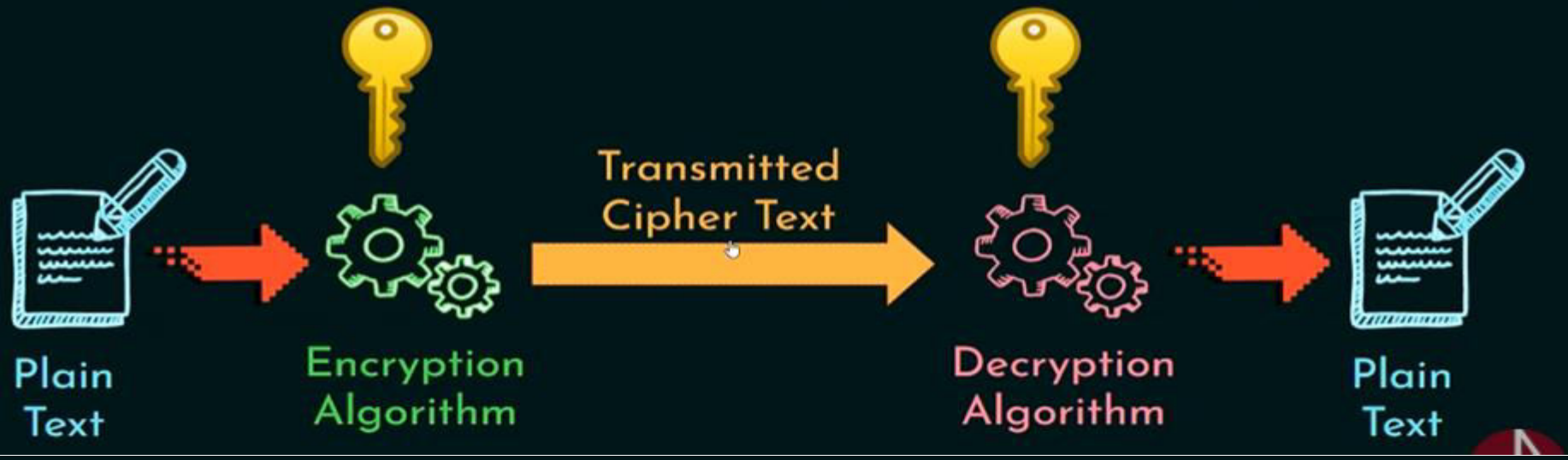
Chapter 3

Network Security Model


Model for Network Security
Trusted Third Party
S
R
T
T
Message
Secret info
Secure Message
Secure Message
Secret info
Message
Opponent
Legends used
T - Security related transformation; S - Sender; R - Receiver

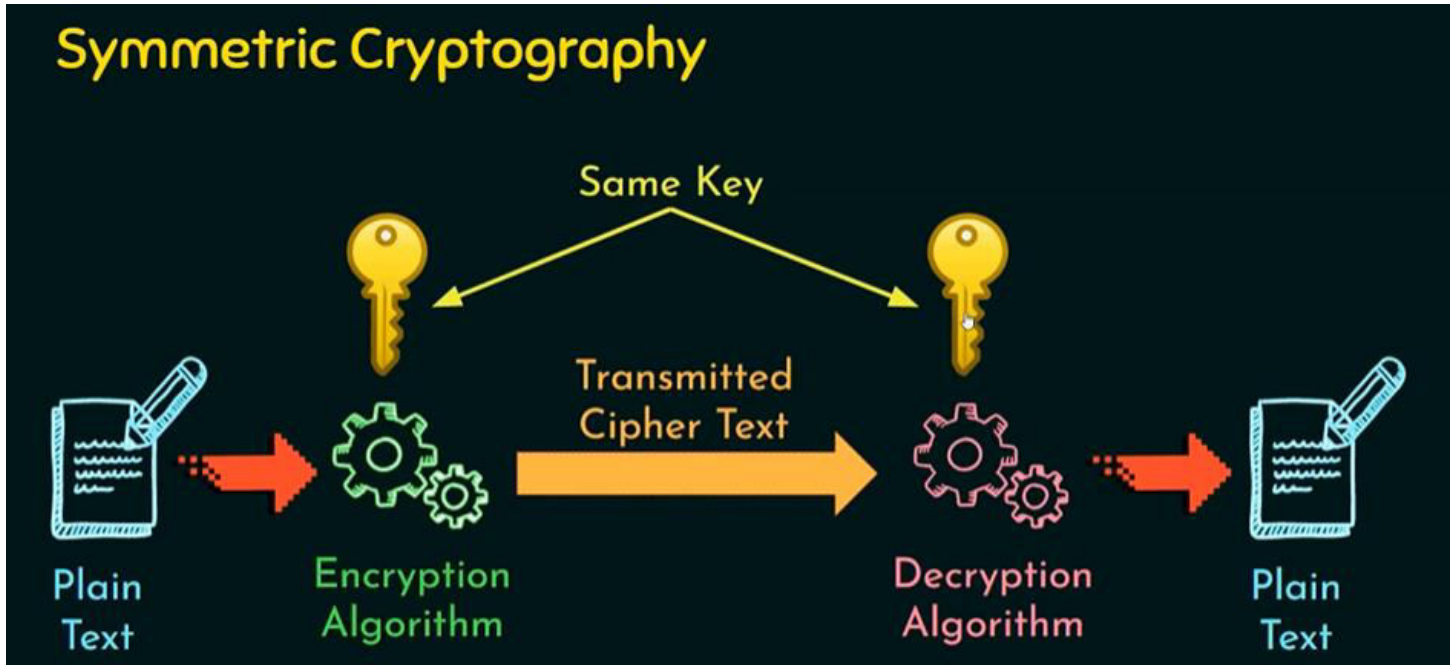
Cryptography

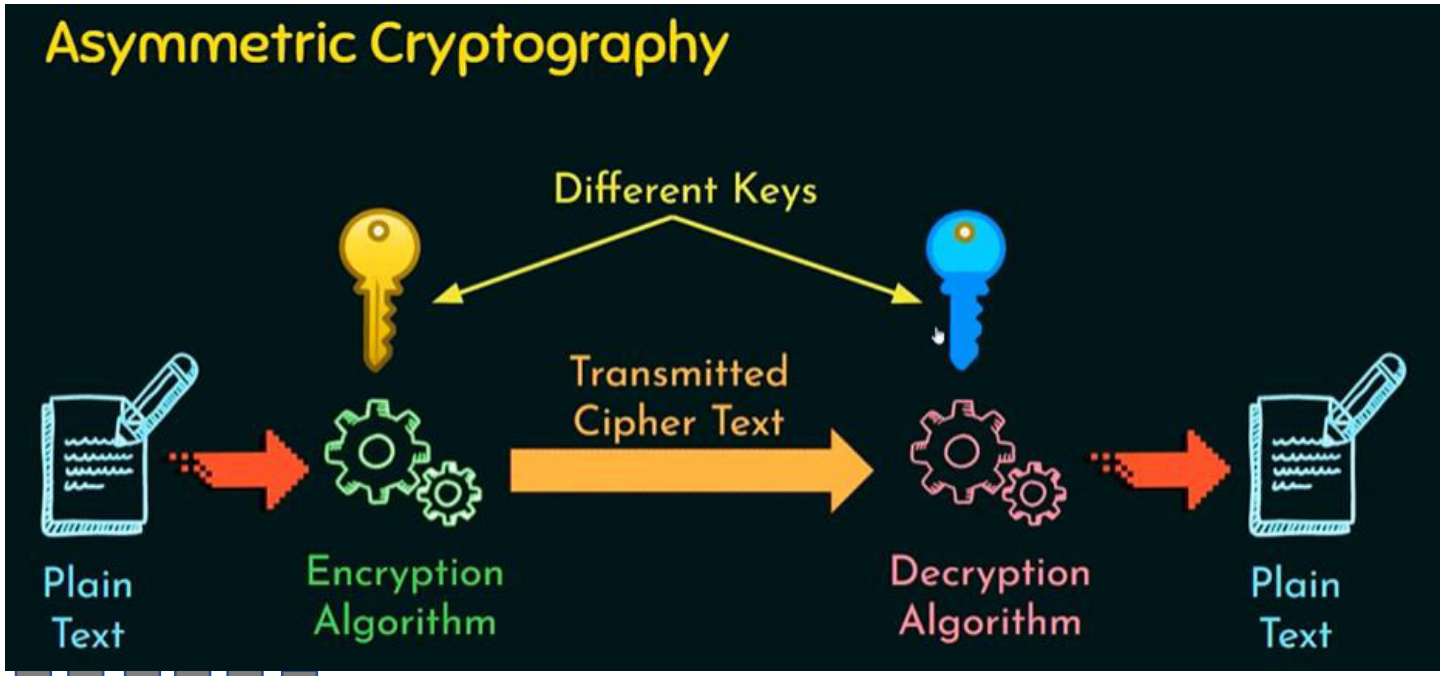
"The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form."



Types of Cryptography

- ★ Symmetric Cryptography (Private Key Cryptography)
- ★ Asymmetric Cryptography (Public Key Cryptography)


Symmetric Cryptography
Same Key
Transmitted
Cipher Text
Plain
Text
Encryption
Algorithm
Decryption
Algorithm
Plain
Text


Asymmetric Cryptography
Different Keys
Transmitted
Cipher Text
Plain
Text
Encryption
Algorithm
Decryption
Algorithm
Plain
Text

Some 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; independent of the plaintext
- **Encipher** (encrypt) - converting plaintext to ciphertext
- **Decipher** (decrypt) - recovering ciphertext from plaintext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis** (code breaking) - study of principles/ methods of deciphering ciphertext without knowing key
- **Cryptology** - field of both cryptography and cryptanalysis

Guess the Plaintext

Ciphertext – Plaintext

Ciphertext

2D570755676DFF11E71B6C8511EFE7A7D3B02A3CEE63165050AB5
F4C4D19A4AAB07656A636654C6F39A4AC0FEA2035CCDD7181C0
EBB482A6EBDAEF2AEB35CB5C325CBF0738AEC27D77BEC3938C
590CE77F62CBDCC3EA3D03E06A386BD70BC99A843DD6B7B975
3635C919FA17FC40A3C3DCBD13633D2D56A1A073EA0E73E60C60

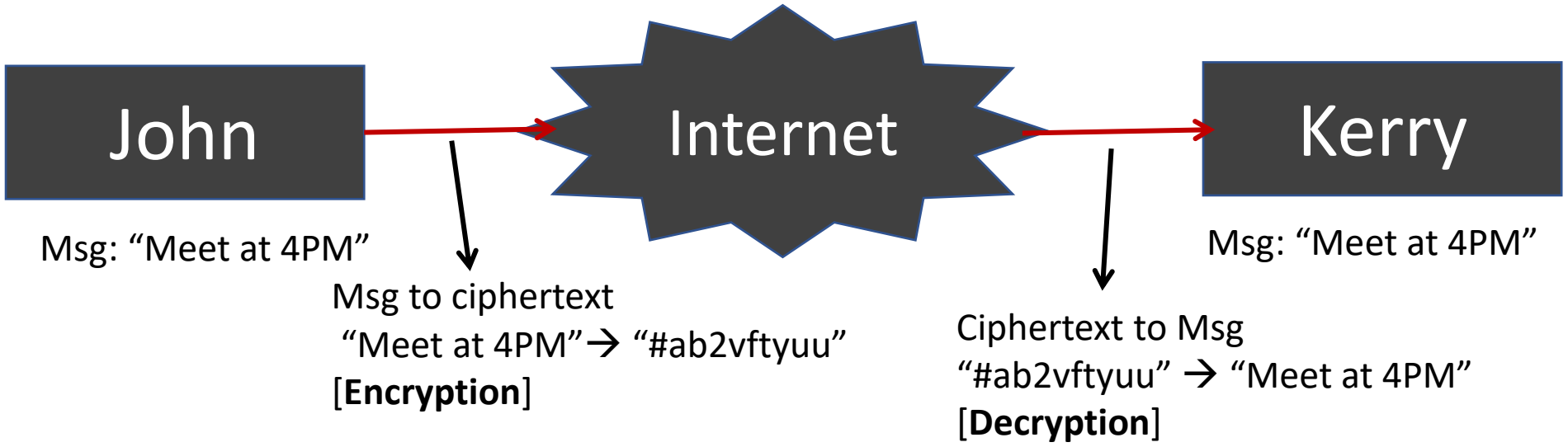
Plaintext

Hello World

Algorithm

RSA Algorithm

Network Security-Example



What is Cryptography?

Cryptography is **the study of secure communications techniques** that allow only the sender and intended recipient of a message to view its contents

Encryption: a process to convert readable to unreadable format
Decryption: a process to convert unreadable to readable format
Key: string of bits used by the cryptographic algorithm to convert plaintext→ciphertext and vice versa

Private key: known only to the particular person
Public key: known to everyone

Types of Cryptography?

i) Symmetric Cryptography: ii) **Asymmetric Cryptography** and iii) **Hash Function**

1. Symmetric Cryptography: It is simplest type of encryption technique when one key (private k1)used to encrypt and decrypt. It is less complex, faster and used for bulk data transfer. But it is not safe as the same key is used at both ends. The most popular symmetric encryption technique is DES (Data Encryption System).

2. Asymmetric Cryptography : It is the type of encryption technique when two keys (one private k1 and one public k2) used to encrypt and decrypt. A message encrypted using public key must be decrypted by private key while a message encrypted using private key must be decrypted by public key. The popular asymmetric algorithms are RSA, DSA, Elliptic curve etc.

3. Hash Function: No usage of key concept. When a variable length message passed to a Hash function then a fixed value is found known as Hash value/code. Many OS uses it to encrypt passwords.

Attacks on Conventional Encryption Scheme

General approaches

1. Cryptanalysis
2. Brute-force attack

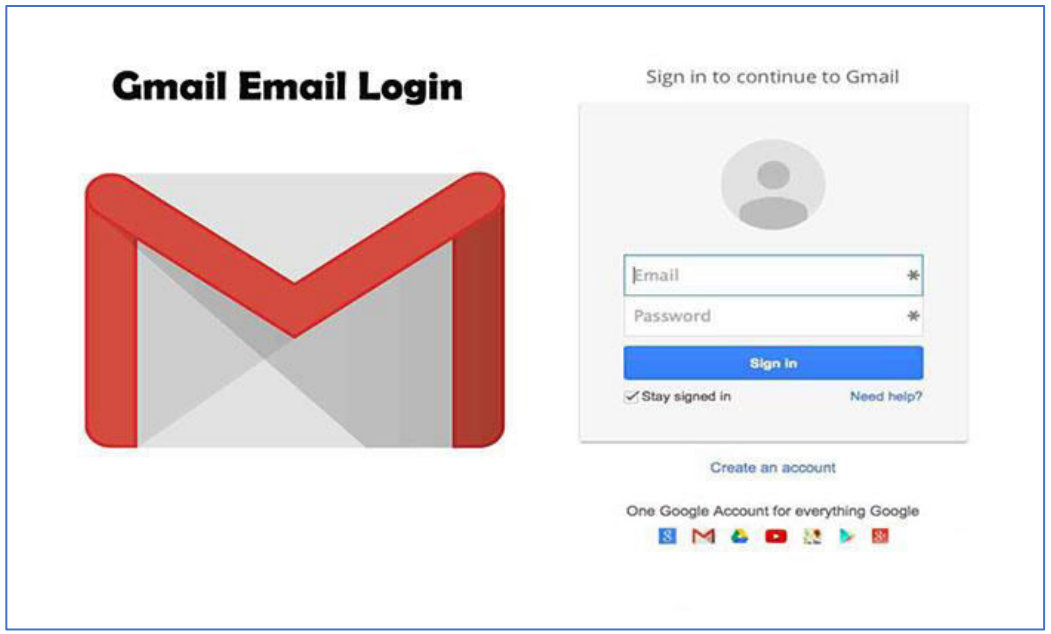
Cryptanlysis Type	Known to cryptanalyst
Ciphertext Only	★ Encryption Algorithm ★ Ciphertext
Known Plaintext	★ Encryption Algorithm ★ Ciphertext ★ One or more PT-CT pairs formed with secret key
Chosen Plaintext	★ Encryption Algorithm ★ Ciphertext ★ PT message chosen by cryptanalyst, together with its CT generated with the secret key
Chosen Ciphertext	★ Encryption Algorithm ★ Ciphertext ★ CT chosen by cryptanalyst, together with its corresponding decrypted PT generated with the secret key
Chosen Text	★ Chosen Plaintext and Chosen Ciphertext

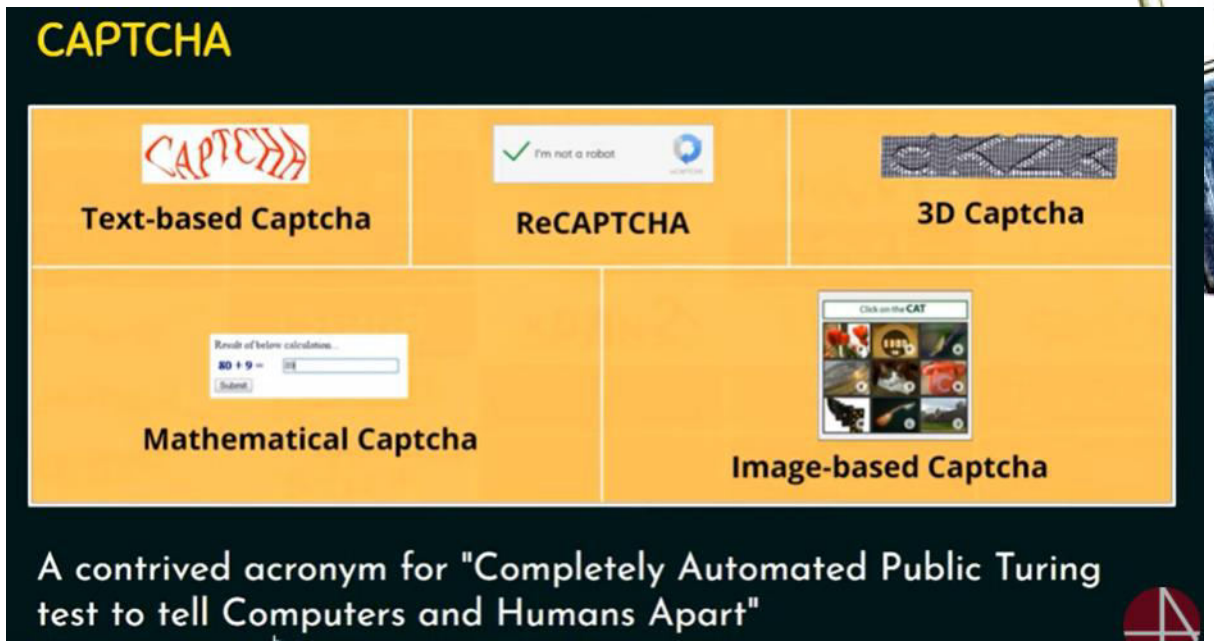
Brute-force attack

- ★ Trying every possible key.
- ★ Until an intelligible translation of the ciphertext into plaintext is obtained.
- ★ Guessing.
- ★ Exhaustive key search.
- ★ Software Tools that can perform brute-force attack.

Aircrack-ng	DaveGrohl	John the ripper
Cain and Abel	Hashcat	Rainbowcrack
Crack	Hydra	Ophcrack

Brute-force Attacks





When several false attempts are made from the same account Google provides Captha test

Classical Encryption Techniques

Symmetric encryption also referred to as conventional encryption is of 2 types as we can say it has 2 techniques

1) Substitution Technique/cipher: It is the one in which the letters of the plain text are replaced by other letter or number or symbol. Ex. Name→IWPX
2) Transposition Technique/cipher: Performing some sort of permutation on the plaintext letters ie it reorder the symbols. Ex. NAME→EAMN or AEMN or MENA etc. (total 4!=24 permutations)

Substitution Technique

★ Letters are replaced by other letters or symbols.

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

a → M

b → X

x → Z

g → A

Plaintext : bag

Ciphertext : XMA

Classical Encryption Technique

Substitution	Transposition
❖ Caesar Cipher	❖ Rail Fence
❖ Monoalphabetic Cipher	❖ Row Column Transposition
❖ Playfair Cipher	
❖ Hill Cipher	
❖ Polyalphabetic Cipher	
❖ One-Time Pad	

Transposition Technique

★ Applying some sort of permutation on the plaintext letters.

★ Plaintext: NESO

★ Ciphertext: ESON, SONE, ONES, ENOS . . . .

Substitution cipher

Caesar Cipher

- ★ Letters are replaced by other letters or symbols.
- ★ The earlier known and simplest method used be Julius Caesar.
- ★ Replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Algorithm:

For each plaintext letter 'p', substitute the ciphertext letter 'C':

$C = E(p, k) \bmod 26 = (p + k) \bmod 26$

$p = D(C, k) \bmod 26 = (C - k) \bmod 26$

If (C-k) is –ve, add 26

Example (encrypt "Stamford University") in Caesar cipher k=3

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
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

S	t	a	m	f	o	r	d		U	n	i	v	e	r	s	i	t	y
V	W	D	P	I	R	U	G		X	Q	L	Y	H	U	V	L	W	B

Plaintext

Cipher text

Substitution cipher

Shift Cipher

Shift Cipher with key=3 is called Caesar Cipher

Example:

Plaintext: Game

Key : 4

Ciphertext: KEQI

Caesar Cipher – Pros and Cons

Pros

1. Simple
2. Easy to implement.

Cons

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try. (Vulnerable to Brute-force attack)
3. The language of the plaintext is known and easily recognizable.

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
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

Substitution cipher

Brute force attack

Ciphertext: SQDYMZK

Shifts	Back	Result	Shifts	Back	Result
0	[26]	SQDYMZK	13	[13]	FDQLZMX
1	[25]	TREZNAL	14	[12]	GERMANY
2	[24]	USFAOBM	15	[11]	HFSNBOZ
3	[23]	VTGBPCN	16	[10]	IGTOCPA
4	[22]	WUHCQDO	17	[9]	JHUPDQB
5	[21]	XVIDREP	18	[8]	KIVQERC
6	[20]	YWJESFQ	19	[7]	LJWRFSD
7	[19]	ZXKFTGR	20	[6]	MKXSGTE
8	[18]	AYLGUHS	21	[5]	NLYTHUF
9	[17]	BZMHVIT	22	[4]	OMZUIVG
10	[16]	CANIWJU	23	[3]	PNAVJWH
11	[15]	DBOJXKV	24	[2]	QOBWKXI
12	[14]	ECPKYLW	25	[1]	RPCXLYJ
13	[13]	FDQLZMX			

Caesar Cipher – Pros and Cons

Pros

1. Simple
2. Easy to implement.

Cons

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try. (Vulnerable to Brute-force attack)
3. The language of the plaintext is known and easily recognizable.

Only 25 keys are possible, very easy to decrypt by attacker

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
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

Substitution cipher

Monoalphabetic Cipher

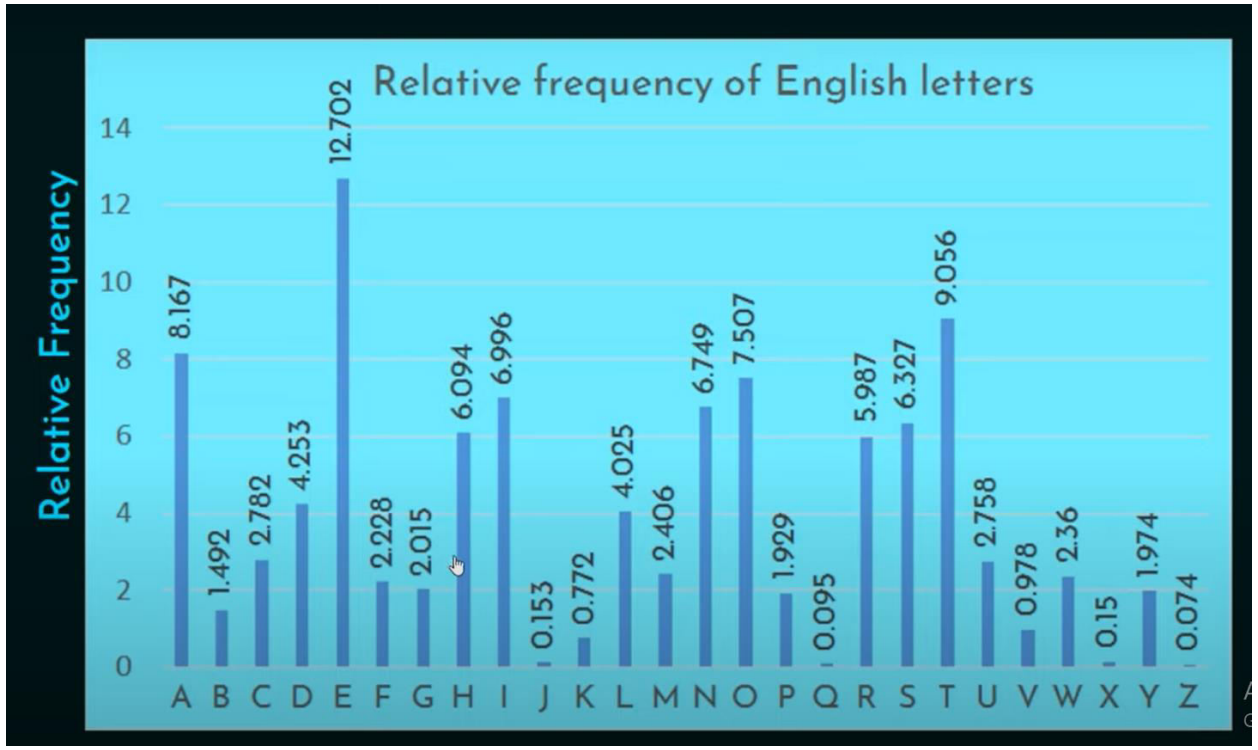
- ★ The "cipher" line can be any permutation of the 26 alphabetic characters.
- ★ This would seem to eliminate brute-force techniques for cryptanalysis.
- ★ A single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.
- ★ English language - Nature of plain text is known.

Plaintext: Game
Ciphertext: FITU

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

Drawbacks of Monoalphabetic Cipher

As English like language is used to encrypt a message, the key in Monoalphabetic cipher can be broken

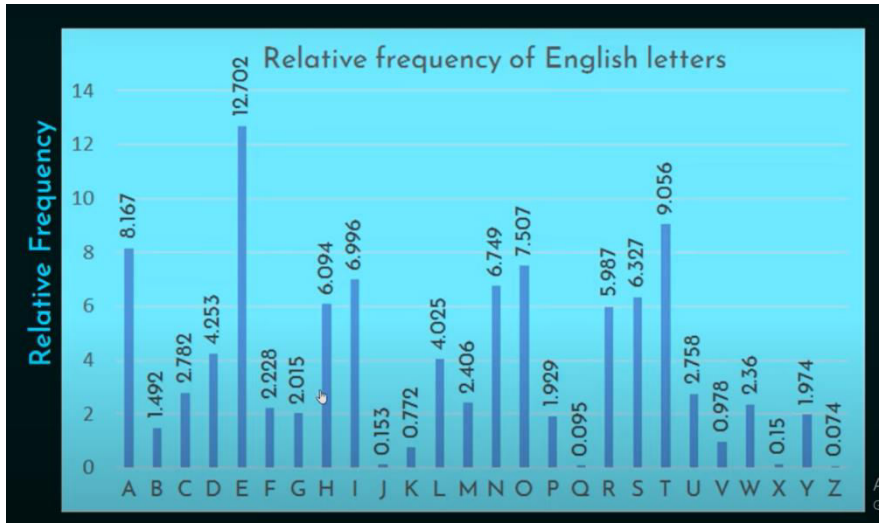


Monoalphabetic Cipher – Example

GZGEWVGRNCP

CT	G	Z	G	E	W	V	G	R	N	C	P
PT	E		E				E				
PT	E		E			T	E				
PT	E		E			T	E			A	
PT	E		E			T	E		L	A	N
PT	E		E			T	E	P	L	A	N
PT	E	X	E	C	U	T	E	P	L	A	N

Drawbacks of Monoalphabetic Cipher



Monoalphabetic Cipher – Example

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

Monoalphabetic Cipher – Example

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
t a e e te a th a t 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

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

Monoalphabetic Cipher

Recover the plaintext using monoalphabetic cipher

“krrg bg gpnrr bk”

Homework!

Encrypt the plaintext “Attack postponed to tomorrow and do not use our secret paper until further info” using Monoalphabetic cipher technique.

Secret Key: The quick brown fox jumps over the lazy dog.

Note: Ignore the second and latter occurrence of alphabets in the key.

Now It’s Quiz Time

Q1: Recovering Ciphertext from plaintext is called _____ ?

A Enchipher

B Dechipher

C Encryption

D Cryptanalysis

30

Q2: Deciphering ciphertext without knowing key _____ ?

A Enchipher

B Dechipher

C Encryption

D Cryptanalysis

30

Q3: Asymmetric Cryptography is based on_____ ?

A. Two private keys

B. Two public keys

C. One public key

D. One private and one public key

30

Q4: Find Plain Text if CT="HTANI" and key=5?

A TBA

B TBA

C TBA

D COVID

30

Q5: Brute-Force Attack seem to be eliminated when_____ ?

A small key space is used

B Caeser Cipher is used

C Shift Cipher is used

D Monoalphabetic Cipher is used

30

Q6: Identify the device?

A HDD

B SDD

C SSD

D RAM

HDD	SSD
✗ More Physical Damage	✓ Less Physical Damage
✗ Noisy, Vibrate, Hot	✓ No Noise/Vibration or Heat
✗ Consumes More Power	✓ Consumes Less Power
✗ Bootup 30-40 Sec	✓ Bootup 10-13 Sec
✗ Write = 50-120MBps	✓ Write = 200-500MBps
✗ File Opens 30% Slower	✓ 30% Faster than HDD
✓ 1TB HDD = 5-7k BDT	✗ 1TB SSD = 30-32k BDT

30