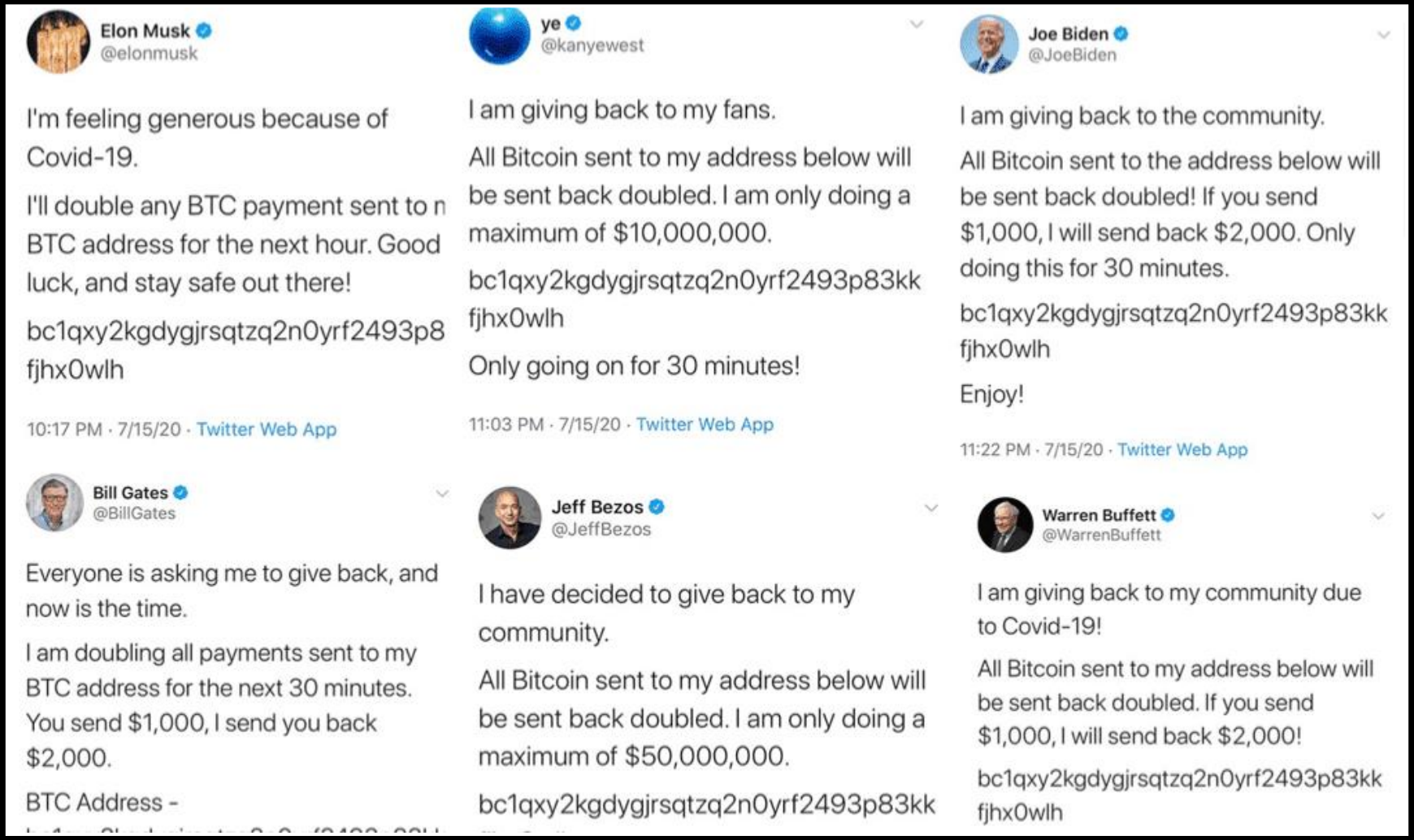
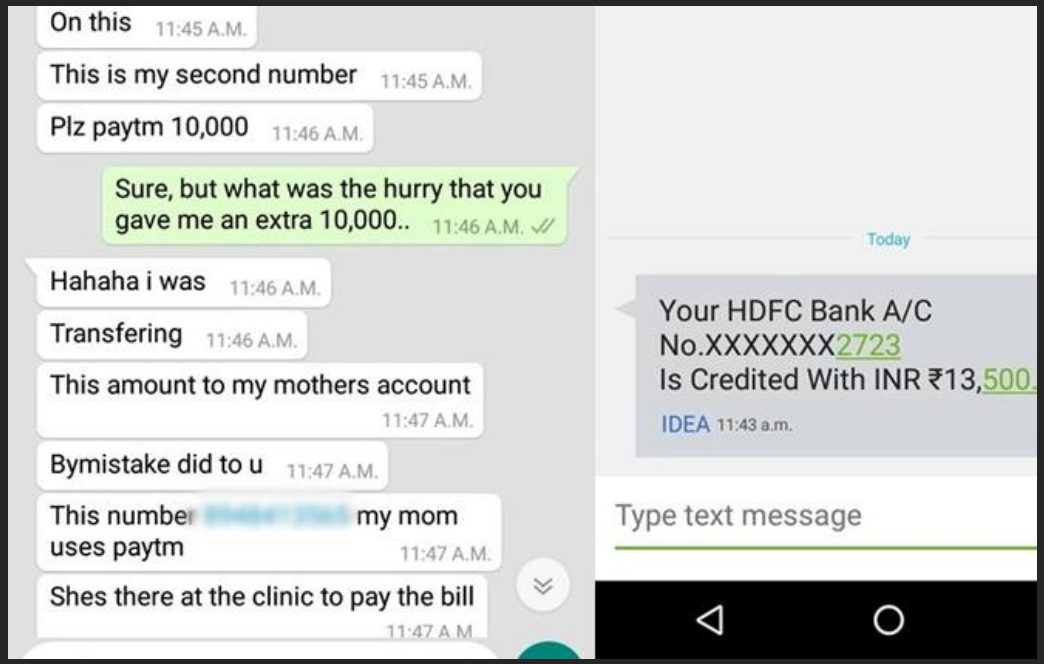
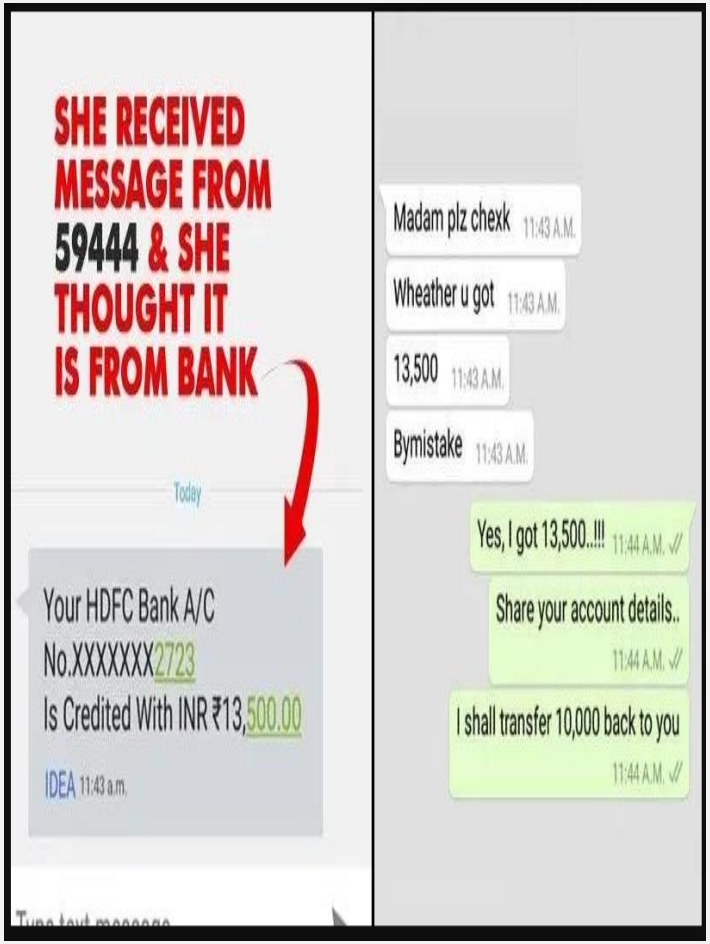


TWITTER SCAM

OLX FRAUD


On this 11:45 A.M.
This is my second number 11:45 A.M.
Plz paytm 10,000 11:46 A.M.
Sure, but what was the hurry that you gave me an extra 10,000.. 11:46 A.M.
Hahaha i was 11:46 A.M.
Transfering 11:46 A.M.
This amount to my mothers account 11:47 A.M.
Bymistake did to u 11:47 A.M.
This numbe my mom uses paytm 11:47 A.M.
Shes there at the clinic to pay the bill 11:47 A.M.
Today
Your HDFC Bank A/C No.XXXXXXX2723 Is Credited With INR ₹13,500.
IDEA 11:43 a.m.
Type text message


Vishal- OLX
Madam plz chexk 11:43 A.M.
Wheather u got 11:43 A.M.
13,500 11:43 A.M.
Bymistake 11:43 A.M.
Yes, I got 13,500..!!! 11:44 A.M.
Share your account details.. 11:44 A.M.
I shall transfer 10,000 back to you 11:44 A.M.
Image posted on Facebook by Velpuri Pavithra S


SHE RECEIVED MESSAGE FROM 59444 & SHE THOUGHT IT IS FROM BANK
Today
Your HDFC Bank A/C No.XXXXXXX2723 Is Credited With INR ₹13,500.00
IDEA 11:43 a.m.
Madam plz chexk 11:43 A.M.
Wheather u got 11:43 A.M.
13,500 11:43 A.M.
Bymistake 11:43 A.M.
Yes, I got 13,500..!!! 11:44 A.M.
Share your account details.. 11:44 A.M.
I shall transfer 10,000 back to you 11:44 A.M.

JAMTARA CHEATS

amtara cheats
city a bank fraud h

Many From Hyd Fall Prey Every Day

Mahesh.Buddi
@timesgroup.com

yderabad: Fraudsters from amtara are duping over a do- en victims from the city every ay and siphoning off lakhs om their bank accounts. Ho- ever, despite the high crime ate police have not been able to o to Jamtara since the begin- ing of the lockdown due to va- ious constraints.

In the past ten days, cyber- rime units in all three com- issionerates have received ver 600 petitions and registe- ed 130 cases. Of them 58 cases ertain to OTP fraud, e-SIM raud, KYC fraud where the ictims have lost over ₹1 crore.

According to Cyberabad in- pector K Srinivas, in the past w months over 40% of comp- ints received by cybercrime nits every day fall under such ategories of fraud. "Most of- ces are committed by gangs ting from Jamtara and ding areas," the in- d. "They know poli- ng up too many interstate cases due to the pan- demic," said an investigator.

Rachakonda cybercrime inspector Laxmikanth Reddy said they are currently taking up interstate investigations on- ly when they can travel by road. "Since the lockdown, we have made a few arrests from AP. The offenders from Jamtara area are targeting people by making them install remote ac- cess applications on the phone posing as customer ca tives," the inspector s

Apart from KYC week alone police ved seven compla e-SIM fraud an said that in alm dence point gangs. Cy ner VC phon ac

KEEP YOUR E-SPACE SAFE

<10% Arrest rate in cases pertaining to Jamtara frauds

<5% Pro reco rate in such fra

JAMTARA GANG PLAYS

Vishing calls | Calls made posing as bank officials to obtain card details of victim

Customer care fraud | Fraudsters make victims upload details through fake cell phone details uploaded on websites as customer care numbers

KYC fraud | Posing executives of PayT or other companies, fraudsters make victims install remot access software, ste information remotel

SIM swaps | Offenders pose as telecom execu tives, make victim send a code to service pro- vider to deactivate service and activate their (fraudster) SIM with the victim's number

Google View forms | Through a link sent bulk SMS seeking personal details to en account does not get blocked, fraudsters bank account, personal details

INS COURSE OBJECTIVES

Describe the basics of Information Security

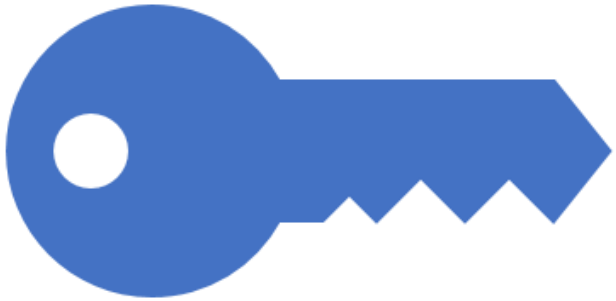
Illustrate different cryptographic algorithms for security.

Describe various access control policies and models.

Understand Security issues related to Software, Web and Networks

TEXT BOOKS

- Cryptography and Network Security, Behrouz A. Forouzan, McGraw – Hill, 2nd edition 2008
- Information Security :Principles and Practice, Mark Stamp, Wiley, 2nd Edition 2011
- Cryptography and Network Security, Atul Kahate, McGraw – Hill, 4th Edition 2019
- Cryptography and Network Security, William Stallings, Pearson Education, 4th Edition 2014



Prepared By

-Anooja Joy

Cryptography

Introduction

Cryptography: study of encryption principles/methods which generate codes to secure transmission of information

Cryptanalysis (codebreaking): process of obtaining original message from encrypted message without knowing algorithms. the study of principles/ methods of deciphering ciphertext *without* knowing key.

Cryptology: science of encryption; combines cryptography and cryptanalysis for making and breaking “secret codes”.

Cryptology --> Cryptography + Cryptanalysis

Cryptography Basic Principles

- **Encryption:** The process of encoding a message so that its meaning is not obvious. The encryption function E takes as input a key k and a message m, to produce a ciphertext c. That is, c = E(k,m)
- **Decryption:** The process of decoding and retrieving original message back. The decryption function D takes as input a key k and a ciphertext c, to produce a message m.m = D(k,c)
- **Non-Repudiation:** The ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- **Integrity:** Cryptography should ensure that the messages that are received by the receiver are not altered anywhere on the communication path. This can be achieved by using the concept of cryptographic hash.
- **Authentication:** authentication ensures that the message was originated from the originator claimed in the message.

Cast of Characters

Alice- Sender(Laptop)

Bob-Reciever(Server)

Trudy/Eve- Intruder(Bad guy-probably human)

Terminologies

- **Plaintext** - the original message
- **Ciphertext** - the coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receive(basically long random numbers)

Eg: 3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

- **Encipher /Encryption** - converting plaintext to ciphertext Y=E(K,X)
- **Decipher /Decryption** - recovering ciphertext from plaintext X=D(K,Y)

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/receive(basically long random numbers).

Eg: 3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

- **Encipher /Encryption** - converting plaintext to ciphertext Y=E(K,X)
- **Decipher /Decryption** - recovering ciphertext from plaintext

X=D(K,Y)

Kerchoff's Principle

1. The system is completely known to the attacker. That is, crypto algorithms are not secret, only the key is secret. **The security of an encryption system must depend only on the secrecy of key, not on the secrecy of the algorithm.** But algorithm should be strong enough.

2. Attacker may be in possession with number of cipher texts together with plain text but should be unable to decrypt cipher text.

This is known as **Kerchoffs' Principle**

Eg: Nearly all proprietary encryption systems have been broken like Enigma, DeCSS, zipcrack.

Secure systems use published algorithms like PGP, OpenSSL, Truecrypt.

Confusion and Diffusion

- **CONFUSION:** Each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two. *confusion* refers to making the relationship between the key and the ciphertext as complex and involved as possible
- The property of confusion hides the relationship between the ciphertext and the key.
- This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected.
- An algorithm providing good confusion will have a complex functional relationship between the plaintext. key pair and the ciphertext

Eg: Substitution

- **DIFFUSION:** Any changes in the plaintext results in multiple changes spread throughout the ciphertext.
- if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable or pseudorandom manner.
- Good diffusion means that the interceptor needs access to much ciphertext to infer the algorithm
- The idea of diffusion is to hide the relationship between the ciphertext and the plain text.

Eg: Permutation Network

Claude Shannon Characteristics of a Good Cipher

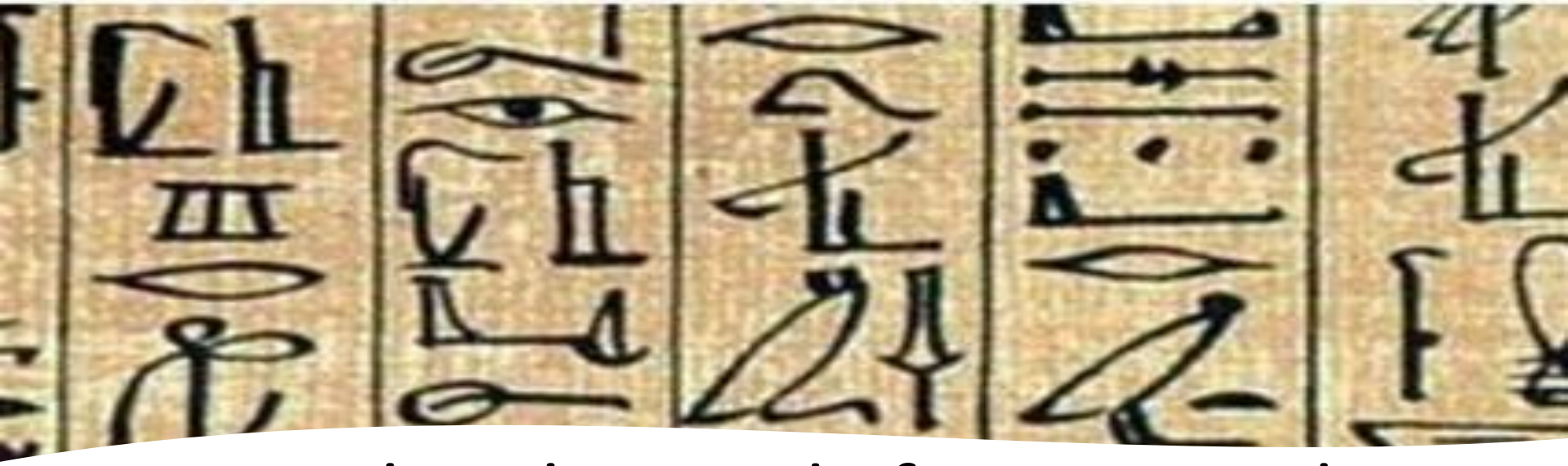
1. The amount of secrecy needed should determine the amount of work needed for the encryption and decryption of the data.
2. The set of keys and the enciphering algorithm should be free from complexity
3. The implementation of the enciphering process should be as simple as possible
4. Any errors in the enciphering should not propagate and cause corruption of further data
5. The size of the ciphertext should be no larger than the text of the original message

Cryptographic Goals

1.**Confidentiality**- Confidential information shouldn't be made available to unauthorized individuals

2.**Integrity**-assures information and programs are changed only in a specific and authorized manner

3.**Availability**-assures timely and reliable use of information



Historical Background of Cryptography

- The word 'cryptography' was coined by combining two Greek words, **'Krypto**' meaning **hidden** and **'graphene**' meaning **writing**.
- The first known evidence of cryptography can be traced to the use of '**hieroglyph'** of Egyptians that has been used 4000 years ago.
- The earlier Roman method of cryptography, popularly known as the **Caesar Shift Cipher**
- Improved coding techniques such as **Vigenere Coding** came into existence in the 15th century
- In the early 20th century, the invention of mechanical and electromechanical machines, such as the **Enigma rotor machine**

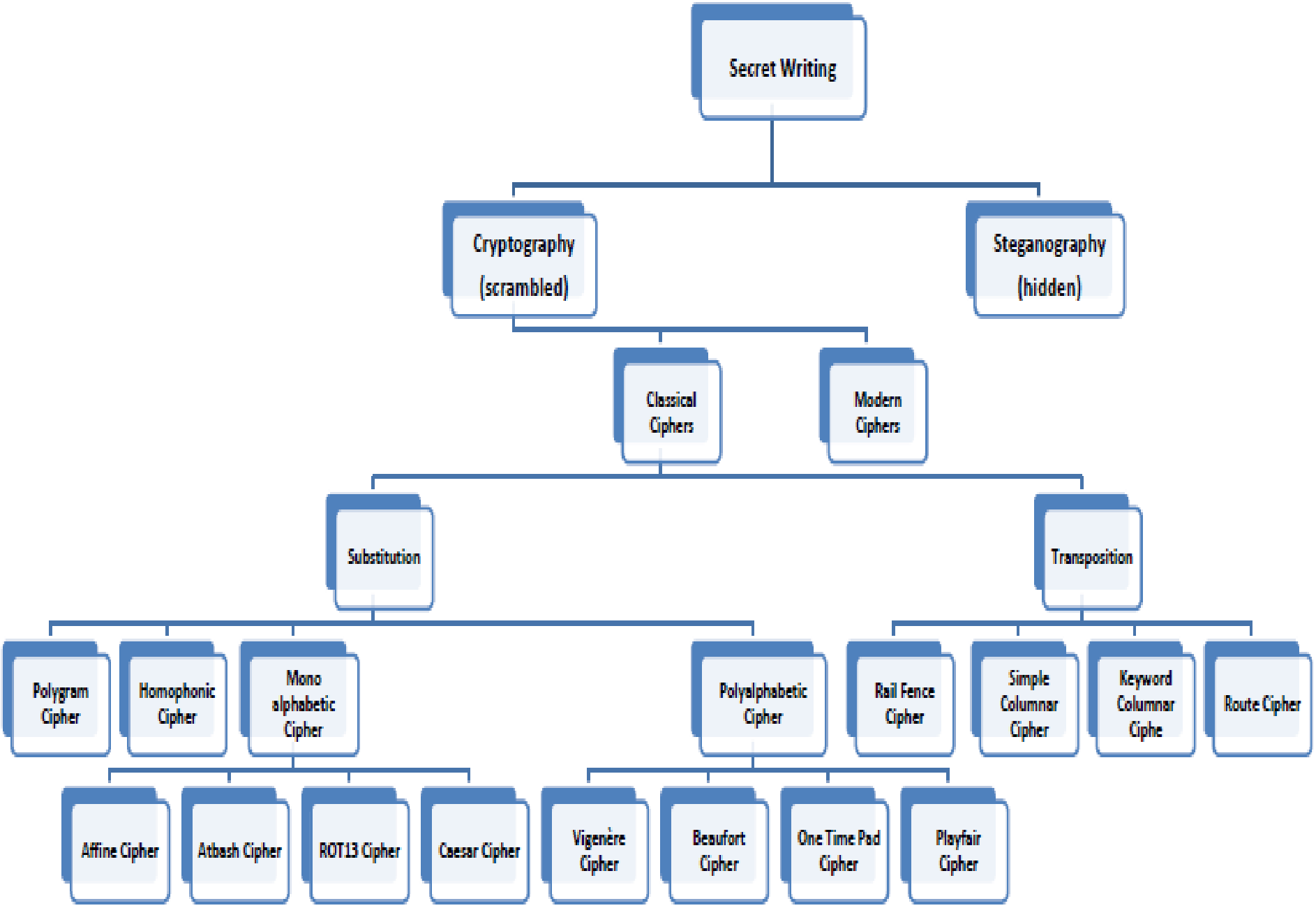
Types of Cryptographic systems

Cryptographic systems are characterized as follows:

1. **No: of keys used:** Symmetric(Private Key) & Asymmetric(Public Key)

2. **Type of operations for transforming plain text to cipher text: Substitution & Transposition**

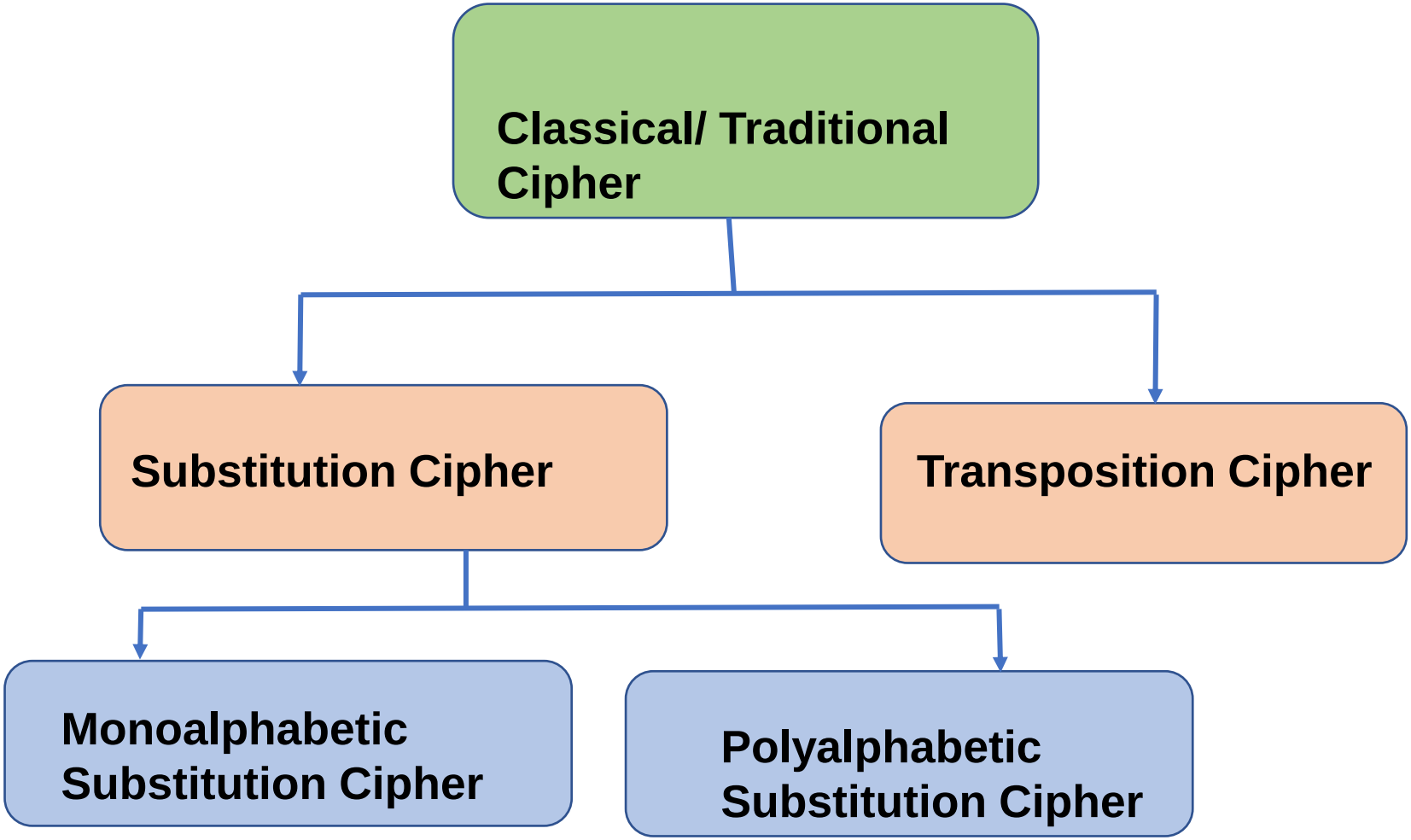
3. **Way in which plain text is processed: Stream & Block**


Secret Writing
Cryptography (scrambled)
Steganography (hidden)
Classical Ciphers
Modern Ciphers
Substitution
Transposition
Polygram Cipher
Homophonic Cipher
Mono alphabetic Cipher
Polyalphabetic Cipher
Rail Fence Cipher
Simple Columnar Cipher
Keyword Columnar Ciphe
Route Cipher
Affine Cipher
Atbash Cipher
ROT13 Cipher
Caesar Cipher
Vigenère Cipher
Beaufort Cipher
One Time Pad Cipher
Playfair Cipher

Classical Cryptography

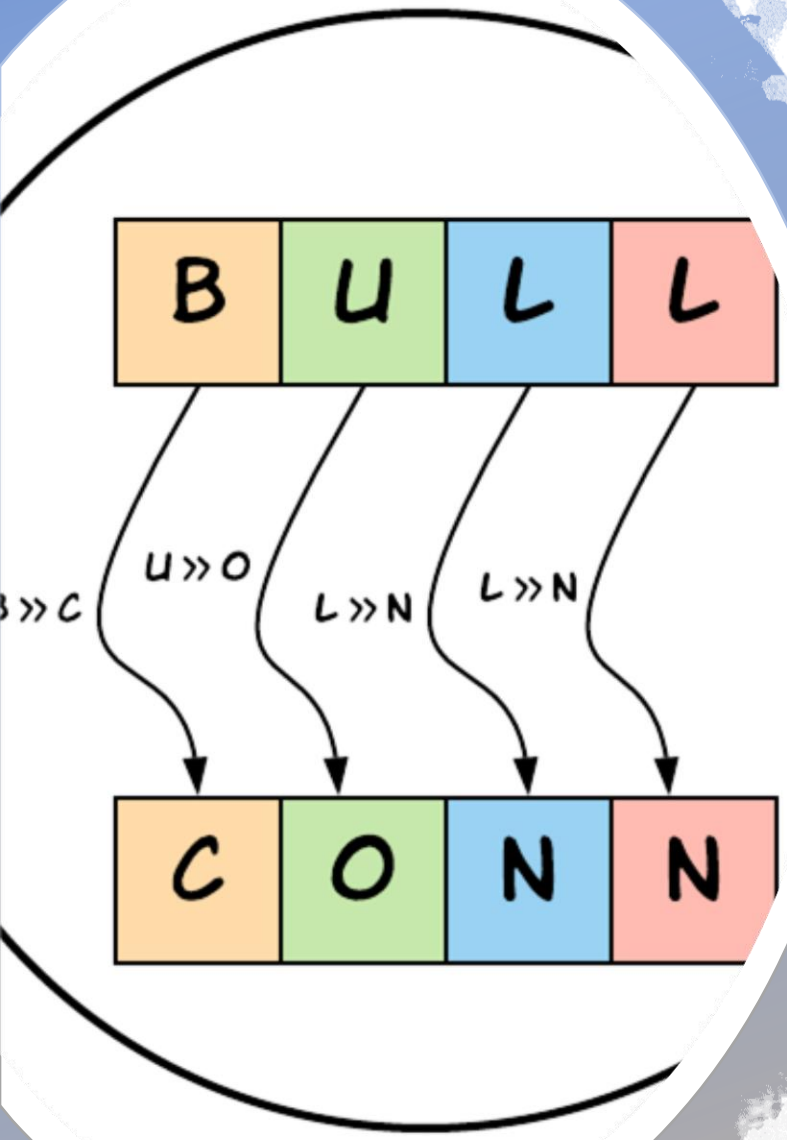
classical encryption techniques
uses symmetric encryption techniques

CLASSICAL CRYPTOGRAPHY



Representation of Characters

Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



SUBSTITUTION CIPHERS

SUBSTITUTION CIPHER

- Use a correspondence table for **substitution**
- Substitute each character by another character or symbol
- It's been classified to **monoalphabetic substitution cipher** and **polyalpha substitution cipher**

A substitution cipher replaces one symbol with another. Letters of plaintext are replaced by other letters or by numbers or symbols

▪**Example:**

➢In the cipher table below, plaintext ' **r** ' is always replaced by cipher text ' **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
X	D	G	S	Z	A	N	Y	O	B	T	M	J	C	E	V	F	H	K	W	P	L	Q	U	R	I

Plain Text:	s e c r e t	w r i t i n g s
Cipher Text:	K Z G H Z W	Q H O W O C N K

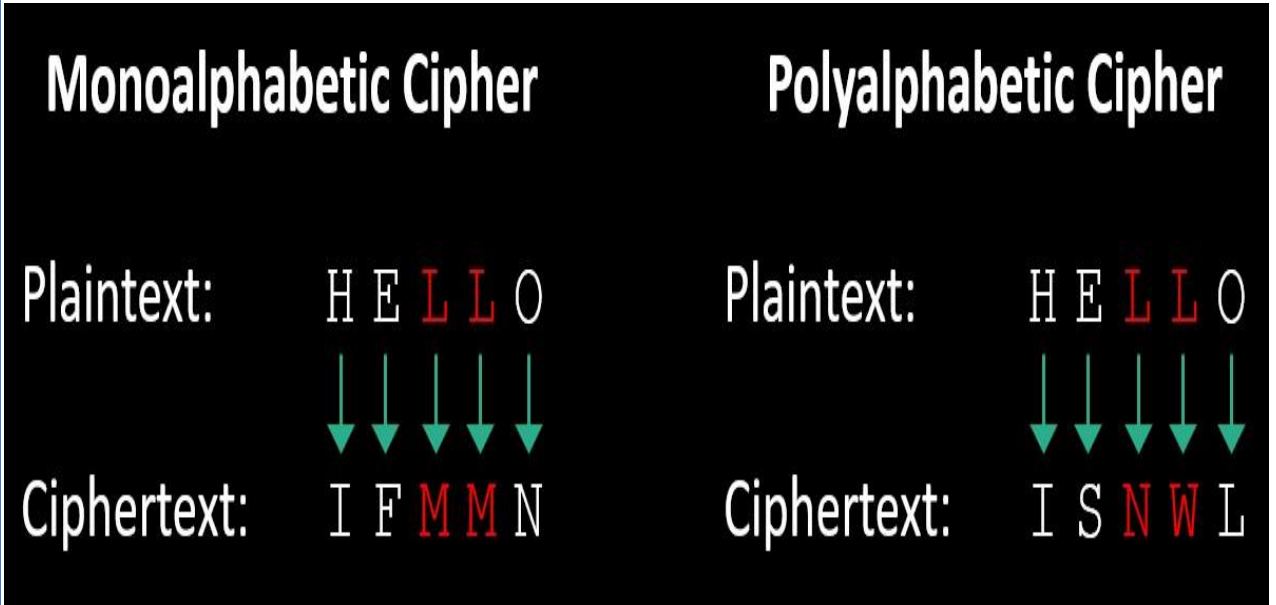
MONOALPHABETIC AND POLY-ALPHABETIC

- **Mono Alphabetic Cipher:** A monoalphabetic cipher is one where each symbol in the input is mapped to a fixed symbol in the output. *Each occurrence of character is encrypted by same character .* If we decide to replace A with D it's not necessary B should be replaced with E *ie random substitution.*

Eg: additive, multiplicative, affine

- **Poly Alphabetic Cipher:** Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

Eg: Playfair Cipher, Roto, One-time pad, Enigma cipher and Vigenere.



SR.NO	MONOALPHABETIC CIPHER	POLYALPHABETIC CIPHER
1	Each symbol in plain text is mapped to a fixed symbol in cipher text.	Uses multiple substitution alphabets.
2	The relationship between a character in the plain text and the characters in the cipher text is one-to-one ie ame fixed mappings from plain text to cipher letters across the entire text.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many ie plain text letters in different positions are enciphered using different cryptoalphabets.
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 ki 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 id does depend on the position of the plain text character in the plain text stream.
5	Eg: additive, multiplicative, affine and monoalphabetic substitution cipher.	Eg: autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.
7	Monoalphabetic ciphers are not that stronger as compared to polyalphabetic cipher.	Polyalphabetic ciphers are much stronger.

Cryptanalysis of Monoalphabetic Substitution Cipher

- Every character can be encoded by every alphabet letter, there are 26! possible pairs of letters in the Latin alphabet (which is 26-letter long).
- But frequency analysis and brute-force attacks are still able to compromise cipher
- Monoalphabetic Cipher can be broken through the use of Frequency Analysis method.
- By comparing frequent cipher text letters with the letters which are frequently used in the language used for encryption. By using this approach, it is assumed that analyzing of encoded messages of size of about 50 letters, is sufficient for discovering the substitutions.

1. Shift Cipher / Additive Cipher

- Shift cipher has a key k can take a range from 0 to 25.

ENCRYPTION

	K	H	A	N	
	10	7	0	13	
+	19	19	19	19	
(	29	26	19	32	) mod 26
	3	0	19	6	
	D	A	T	G	

Shift cipher replace each alphabet by another alphabet which is 'shifted' by some fixed number between 0 and 25. It uses **modulo operator** to encrypt and decrypt messages.

- Shift cipher can be mentioned as as:

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

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

- Decryption is equivalent to find additive inverse

Q : Plaintext: **hello** and Key: *Shift=15*

DECRYPTION

	D	A	T	G	
	3	0	19	6	
-	19	19	19	19	
(	-16	-19	0	-13	) mod 26
	10	7	0	13	
	K	H	A	N	

SHIFT CIPHER EXAMPLE

Use the additive cipher with key = 15 to encrypt the message "hello".

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

CAESAR CIPHER

- Earliest known substitution cipher by Julius Caesar in Gallic wars for military affairs

Caesar cipher is a shift cipher that uses a shift of 3 for translation

- It's a monoalphabetic substitution cipher which replaces each alphabet with 3 alphabets further
  - $C = E(p) = (p + 3) \bmod (26)$
  - $p = D(C) = (C - 3) \bmod (26)$

CAESAR CIPHER EXAMPLE

Plaintext: spongebobsqua repants

Key: *Shift=3*

Ciphertext: VSRQJHEREVT XDUHSDQWV

Q: attack at dawn

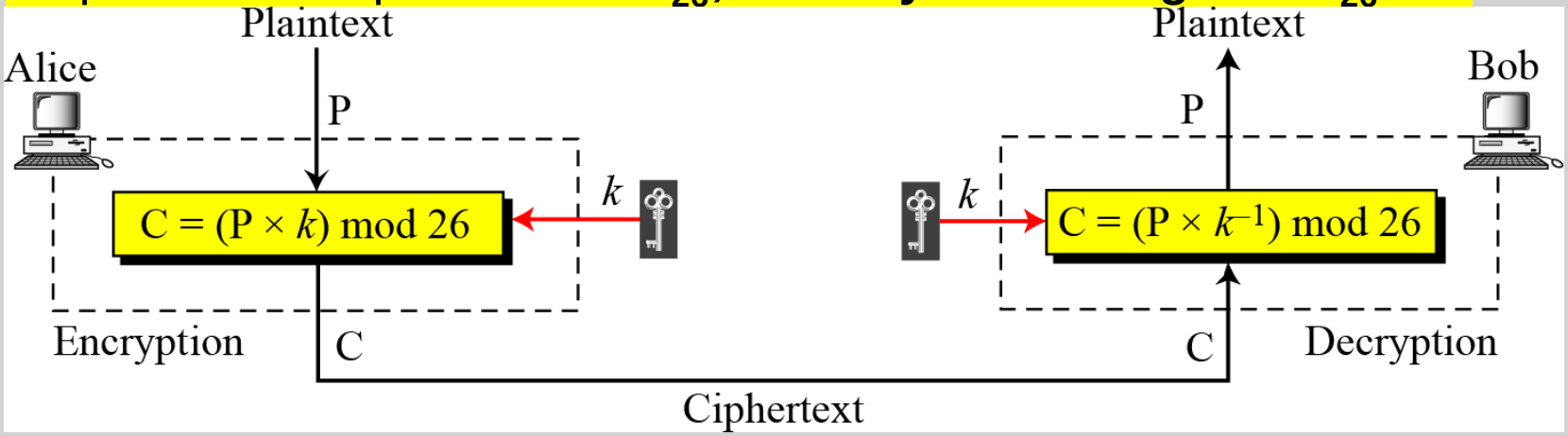
Cryptanalysis of Caesar Cipher

- Caesar cipher can be easily broken using brute force attacks. To discover the plaintext one should just check all the possible 26 (for the Latin alphabet) shifts.
- Like other substitution ciphers, the Caesar cipher can also be attacked using known ciphertext attacks and letter frequency analysis of the ciphertext.

Q. Break ciphertext “ERE L ORYH BRX DOLFH"

MULTIPLICATIVE CIPHER

In a multiplicative cipher, multiplication is used to convert plaintext to cipher text **in Z_{26}; the key is an integer in Z_{26}*.**



How to select key K?

- **In order to create unique cipher characters, key should be a multiplier which is co-prime (the values do not share any factors when dividing) in relation to the size of the alphabet (26). Also for decryption, key should be having multiplicative inverse.**
- **The key needs to be in Z_{26}* in order that its mul. Inverse exists. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25**

Multiplicative Cipher

- **For Decryption multiplicative inverse of key is multiplied with cipher text.**

Multiplicative Inverse:

- **In modular arithmetic, a & b are multiplicative inverses of each other if, (a*b) mod n =1**

Find mul. Inv of 7 in Z26 i.e (7* x) mod 26 = 1. Multiplicative inverse of 7 is 15.

Example:

Use multiplicative cipher to encrypt the message "hello" with key of 7.

Plaintext: h $\rightarrow$ 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow$ U

B	1	(1 * 7) % 26 = 7	H
C	2	(2 * 7) % 26 = 14	O
D	3	(3 * 7) % 26 = 21	V
E	4	(4 * 7) % 26 = 2	C
F	5	(5 * 7) % 26 = 9	J
G	6	(6 * 7) % 26 = 16	Q
H	7	(7 * 7) % 26 = 23	X
I	8	(8 * 7) % 26 = 4	E
J	9	(9 * 7) % 26 = 11	L
K	10	(10 * 7) % 26 = 18	S
L	11	(11 * 7) % 26 = 25	Z
M	12	(12 * 7) % 26 = 6	G
N	13	(13 * 7) % 26 = 13	N
O	14	(14 * 7) % 26 = 20	U
P	15	(15 * 7) % 26 = 1	B
Q	16	(16 * 7) % 26 = 8	I
R	17	(17 * 7) % 26 = 15	P
S	18	(18 * 7) % 26 = 22	W
T	19	(19 * 7) % 26 = 3	D
U	20	(20 * 7) % 26 = 10	K
V	21	(21 * 7) % 26 = 17	R

Multiplicative Modular Operation with 7

How to find multiplicative inverse?

METHOD 1

- To find a multiplicative inverse, we need to find a number *x* such that: **a*x≡1 mod m.** *Here x* is the inverse of *a*, and we call it a^{-1}
- To find the inverse of 5 modulo 26, solve 5*x≡1 mod26. Hence search each of the numbers 1 to 25 ie 1 to m-1, which satisfies it.

METHOD 2

- Else use **extended euclidian algorithm.** Find diferent x and y values that staisfies ax + my ≡ 1 (mod m)
- Take $\mathbf{p_0 = 0}$ and $\mathbf{p_1 = 1.}$ calculate $\mathbf{p_i = p_{i-2} - p_{i-1}\, q_{i-2}\ (mod\ n)}$. Untill **i+1** times, i indictes upto which there is no reminder.

EXAMPLE 1

Find the inverse of 15 mod 26

i		q_i	P_i
0	26 = 15(1) + 11	1	0
1	15 = 11(1)+4	1	1
2	11=4(2)+3	2	0-1*1mod26=25
3	4=3(1)+1	1	1-25*1mod 26=2
4	3=1(3)	3	25-2*2mod 26=21
			2-21*1mod 26=7

So inverse is 7

EXAMPLE 2

Find the inverse of 17 mod 26

i		q_i	P_i
0	26 = 17(1) + 9	1	0
1	17 = 9(1)+8	1	1
2	9=8(1)+1	1	0-1*1mod26=25
3	8=1(8)	8	1-25*1mod 26=2
			25-2*1 mod 26=23

So inverse is 23

EXAMPLE 3

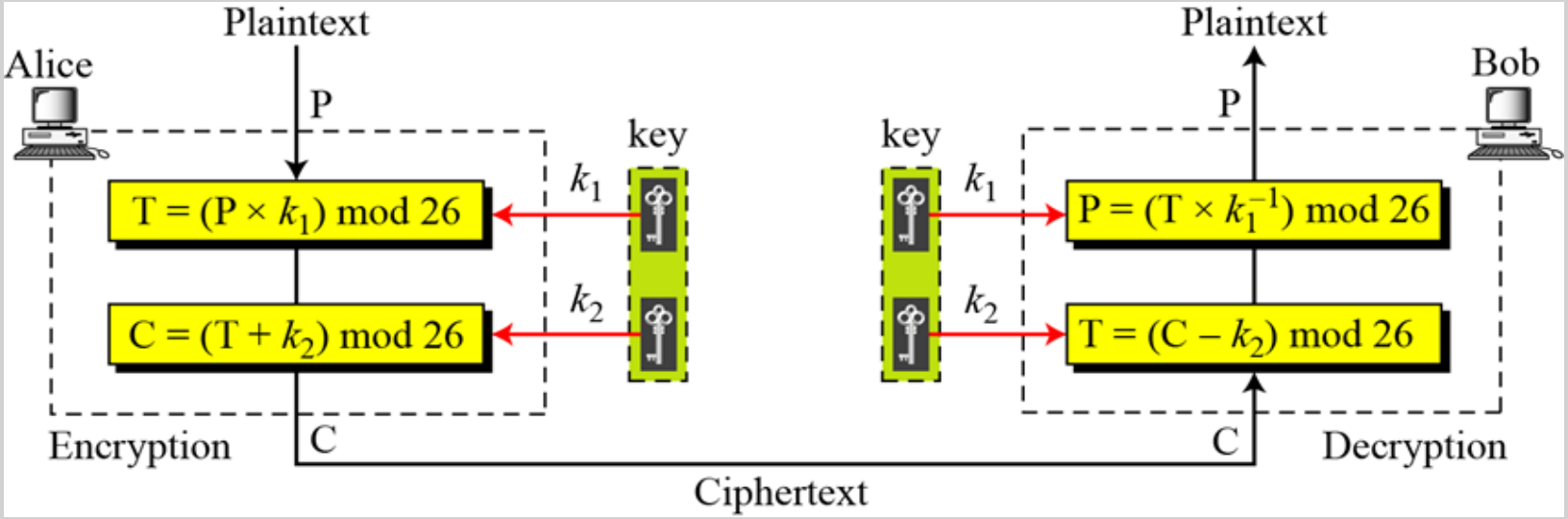
Find the inverse of 5 mod 26

i		q_i	P_i
0	26 = 5(5) + 1	5	0
1	5 = 1(5)	5	1
			0-1*5mod26=21

So inverse is 21

AFFINE CIPHER

- **Affine cipher is a combination of Additive and Multiplicative Ciphers.**



- **Encryption and decryption can be mentioned as**

$$C = (P \times k_1 + k_2) \bmod 26 \qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

AFFINE CIPHER

- **The additive cipher is a special case of an affine cipher in which $k_1 = 1$.The multiplicative cipher is a special case of affine cipher in which $k_2 = 0$**
- **The affine cipher uses a pair of keys in which the first key is from Z_{26}^* and the second is from Z_{26}. The size of the key domain is $26 \times 12 = 312$.**

Example

- **Use an affine cipher to encrypt the message "hello" with the key pair (7, 2).**

P: h → 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 → W

AFFINE CIPHER DECRYPTION EXAMPLE

Q. **Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.**

Solution

C: Z → 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 → h
C: E → 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 → e
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: W → 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 → o

AFFINE CIPHER CHALLENGES

Q1. Let ***a*=5** and ***b*= 7**. Encrypt **"defend the east wall of the castle"**

Q2. Let ***a*=17** and ***b*= 20**. Encrypt **"TWENTY FIFTEEN"**

Q3. Let ***a*=5** and ***b*= 8**. Encrypt **"AFFINE CIPHER"**

Q4. Let ***a*=3** and ***b*= 7**. Encrypt **"SAIL"**

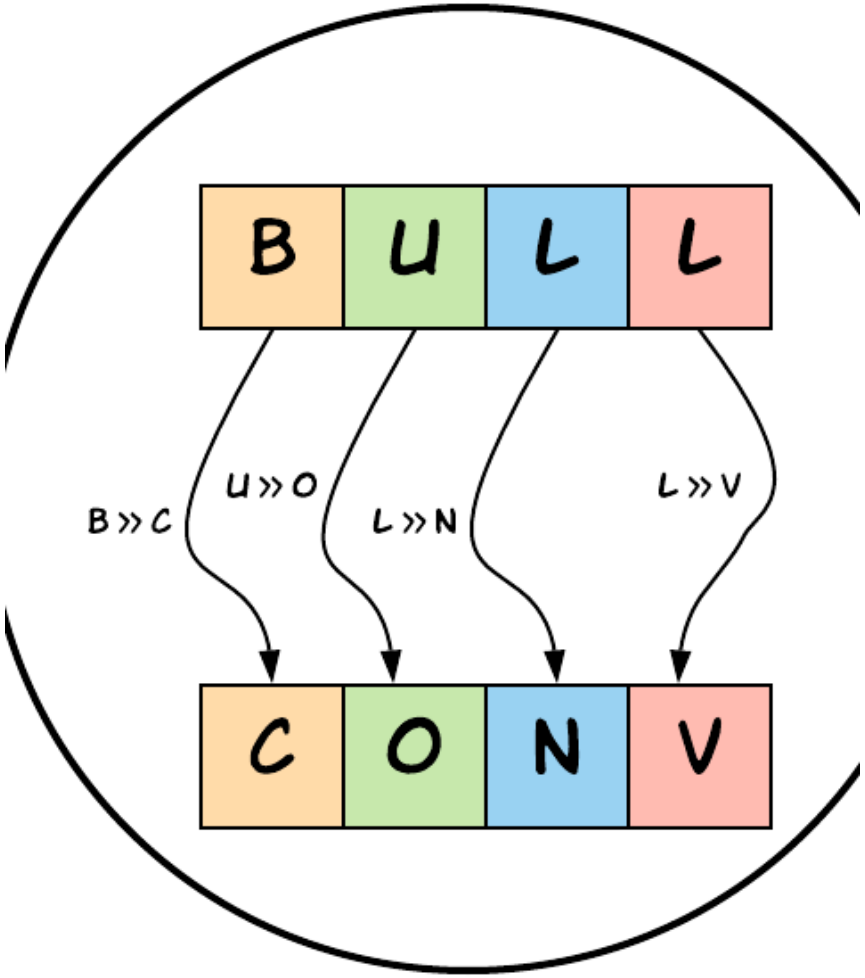
POLYALPHABETIC SUBSTITUTION CIPHER

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.

Plaintext: ATTACK ATDAWN

Ciphertext: LXFOPVEFRNHR

Eg: Vignere Cipher, Alberti Cipher, PlayFair Cipher, hill cipher



Vigenere Cipher

- Vigenère cipher is a simple **polyalphabetic cipher**, in which the ciphertext is obtained by modular addition of a (repeating) key phrase and an open text (both of the same length). The keyword repeated over until the same length of plaintext is called *Keystream*.

$$P = P_1 P_2 P_3 \ldots \qquad C = C_1 C_2 C_3 \ldots \qquad K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$$

$$\text{Encryption: } C_i = P_i + k_i \qquad \text{Decryption: } P_i = C_i - k_i$$

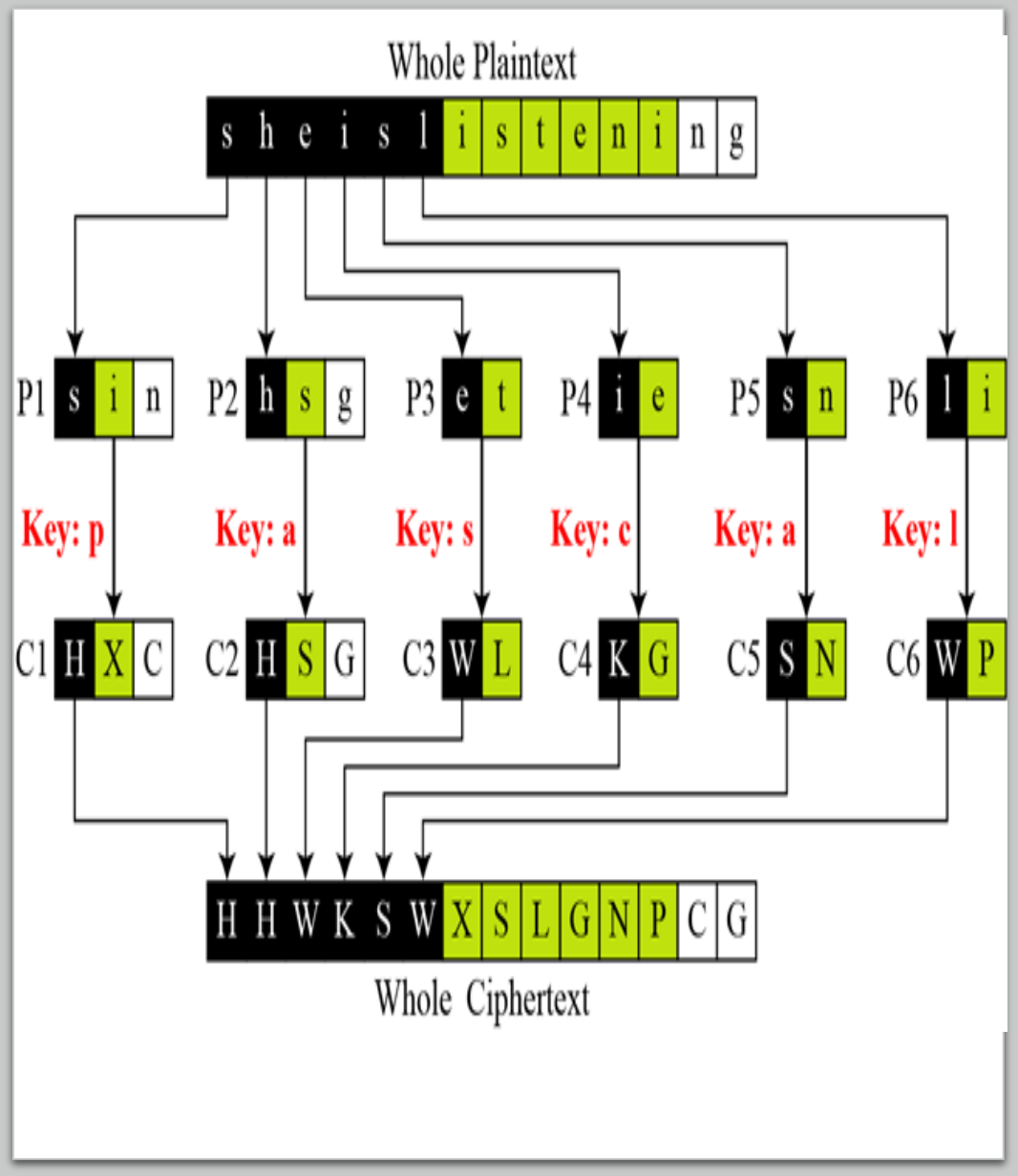
ENCRYPTION EXAMPLE

- **Let us see how we can encrypt the message "She is listening" using the 6-character keyword "PASCAL". The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed)**

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Is vignere cipher a type of additive cipher?

- **Vigenere cipher can be seen as combinations of m additive ciphers.**



	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

Vignere Cipher

ENCRYPTION : $C_i = P_i + K_i \bmod 26$

Decryption: $D_i = C_i - K_i \bmod 26$

In order to simplify the encryption and decryption process, we can use *Vigenère square*

A Vigenere Tableau for encryption and Decryption

Vignere table or Vigenère squarecan be used for encryption and decryption.

To encrypt, use the keyword letter and the plaintext letter as the row index and column ind ex, respectively, and the entry at the row-column intersection is the letter in the ciphertext.

To decrypt, pick a letter in the ciphertext and its corresponding letter in the keyword, use the keyword letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plaintext letter.

additive cipher is a special case of Vigenere cipher in which *m* = 1.

Decryption using Vignere Table

- To decrypt a ciphertext with the keyword, generate the keystream by repeating the keywords until the length is same as that of ciphertext. Then find the column with the letter of the keystream at the top, and go down this column to find the ciphertext letter. The letter that is the row index, ie left of the table is the plaintext letter.

	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

VIGNERE CHALLENGE

- Encrypt the plaintext "a simple example" using the keyword *battista*.

Plaintext	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s

Vignere Cipher Example

Plaintext: T O B E O R N O T T O B E

Key: R E L A T I O N S R E L A

HILL CIPHER

- Developed by mathematician Lester S. Hill
- A polygraphic substitution cipher that works on multiple letters(more than 3 letters) at same time.
- Uses matrix multiplication concept.
- Encryption: **K* P Mod 26**
- Decryption: **K^{-1}* C Mod 26**
- Key is an invertible n × n matrix and plain text should be a block of n letters
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

How to select Key?

1. Not all matrices have an inverse . The matrix will have an inverse if and only if its **determinant is not zero**.
2. The **determinant** of the encrypting matrix **must not have any common factors with the modular base**.

- Ie, for modulo 26 by above 2 conditions, the determinant must be nonzero, and must not be divisible by 2 or 13.

How to find matrix inverse?

$$K^{-1} = d^{-1} \times adj(K)$$

Where d is the determinant of matrix K

EXAMPLE

- Let Plaintext: ACT Key: GYBNQKURP
- The key is 'GYBNQKURP' which can be written as the nxn matrix: $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$
- Plain Text is written as: $\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$
- Cipher Text = $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} * \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$ Mod 26= $\begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} *$ Mod 26

$$= \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

which corresponds the ciphertext 'POH'

Matrix Inverse of 2X2 Matrix

1. **Determinant of a 2 x 2 matrix.**

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

Example

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7 \times 11 - 8 \times 11 = -11 = 15 \bmod 26$$

2. **Find the multiplicative inverse of the determinant working modulo 26**. The answer is 7

$$15 \times x = 1 \bmod 26$$

Matrix Inverse of 2X2 Matrix

3. Find the Adjugate Matrix

$$adj\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Example

$$adj\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

4. Multiply the Multiplicative Inverse of the Determinant by the Adjugate Matrix

$$7 \times \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 165 & 49 \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \ mod\ 26$$

1. **Determinant of a 3 x 3 matrix.**

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a\begin{vmatrix} e & f \\ h & i \end{vmatrix} - b\begin{vmatrix} d & f \\ g & i \end{vmatrix} + c\begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

$$= a(ei - fh) - b(di - fg) + c(dh - eg)$$

$$= aei - afh - bdi + bfg + cdh - ceg$$

$$= (aei + bfg + cdh) - (afh + bdi + ceg)$$

Matrix Inverse of 3X3 Matrix

Adjugate of 3X3 Matrix

- **To find Adjugate:** Find the transpose of the cofactor matrix

$$cofactor\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} +\begin{vmatrix} e & f \\ h & i \end{vmatrix} & -\begin{vmatrix} d & f \\ g & i \end{vmatrix} & +\begin{vmatrix} d & e \\ g & h \end{vmatrix} \\ -\begin{vmatrix} b & c \\ h & i \end{vmatrix} & +\begin{vmatrix} a & c \\ g & i \end{vmatrix} & -\begin{vmatrix} a & b \\ g & h \end{vmatrix} \\ +\begin{vmatrix} b & c \\ e & f \end{vmatrix} & -\begin{vmatrix} a & c \\ d & f \end{vmatrix} & +\begin{vmatrix} a & b \\ d & e \end{vmatrix} \end{pmatrix}$$

Matrix Inverse of 3X3 Matrix

1. **Determinant of a 3x 3 matrix.**

Example

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7 \times 11 - 8 \times 11 = -11 = 15 \bmod 26$$

2. **Find the multiplicative inverse of the determinant working modulo 26**. The answer is 7

$$15 \times x = 1 \bmod 26$$

DECRYPTION

- $K^{-1} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$
- K^{-1}*C*Mod 26 = $\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} * \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$* Mod 26

= $\begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix}$* Mod 26 = $\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$ = "ACT"

How to compute inverse of a matrix?

1. Replace original matrix by adjoint of elements in matrix
2. Transpose the matrix
3. Divide every element by determinant of original matrix

HILL CIPHER CHALLENGES

Encrypt the plaintext message "short example" using the keyword *hill*

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}$$

Encrypt the plaintext message "retreat now" using the keyword *backup* ***NOTE:*** Notice that the key phrase is short of few letters, so we fill in the final elements with the start of the alphabet.

Solution

Key

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix} \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

Plain Text

$$\begin{pmatrix} s \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} \qquad \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} r \\ e \\ t \end{pmatrix} \begin{pmatrix} r \\ e \\ a \end{pmatrix} \begin{pmatrix} t \\ n \\ o \end{pmatrix} \begin{pmatrix} w \\ x \\ x \end{pmatrix} \qquad \begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix} \begin{pmatrix} 17 \\ 4 \\ 0 \end{pmatrix} \begin{pmatrix} 19 \\ 13 \\ 14 \end{pmatrix} \begin{pmatrix} 22 \\ 23 \\ 23 \end{pmatrix}$$

PLAY-FAIR CIPHER

- Playfair cipher is practical digraph substitution cipher invented by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher.

Playfair Cipher Encryption Algorithm:

1. Creation and population of key square matrix: Polybius Square

- The key is a 5×5 grid of alphabets where grid is created in such a way fill key in **5*5** matrix **row wise** from left to right by **dropping duplicates**. The remaining cells are filled from **rest of English alphabets A-Z excluding J**(as the table can hold only 25 alphabets). If the keyword text **contains J, then it is replaced by I**. ie each of the 25 alphabets must be unique

Examples

- Key: PLAYFAIR EXAMPLE
- Key: MONARCHY

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

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

2. Creating digraph Plaintext

- The plaintext is split into **pairs of two letters (digraphs)**. If the digraph consists of the same letter twice then insert the letter "X" between the same letters, and then continue with the rest of the steps. If there is only one letter left by itself at the end of the plaintext then add Z at the end.

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz‘

PlainText: 'hammer'

After Split: 'ha' 'mx' 'me' 'rz'.

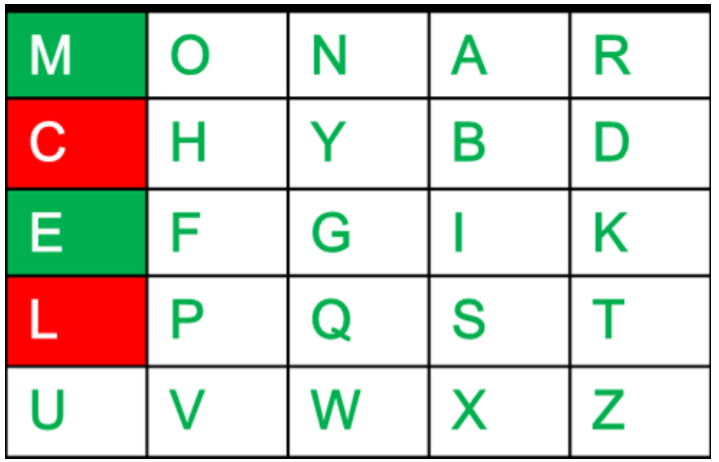
3. Rules for Encryption:

Refer key square matrix and identify digraphs

A. **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).

Diagraph: "me"

Encrypted Text: cl



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

B. **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

Diagraph: "st"

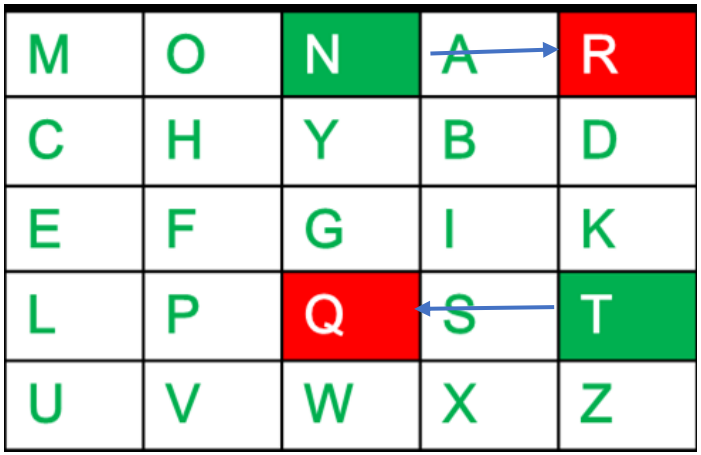
Encrypted Text: tl

A. **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle(being careful to maintain the order).

Diagraph: "tn"

Encrypted Text: qr

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



:

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

st:

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

ru:

M	O	N	A
C	H	Y	B
E	F	G	I
L	P	Q	S
U	V	W	X

:

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

nt:

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

sz:

M	O	N	A
C	H	Y	B
E	F	G	I
L	P	Q	S
U	V	W	X

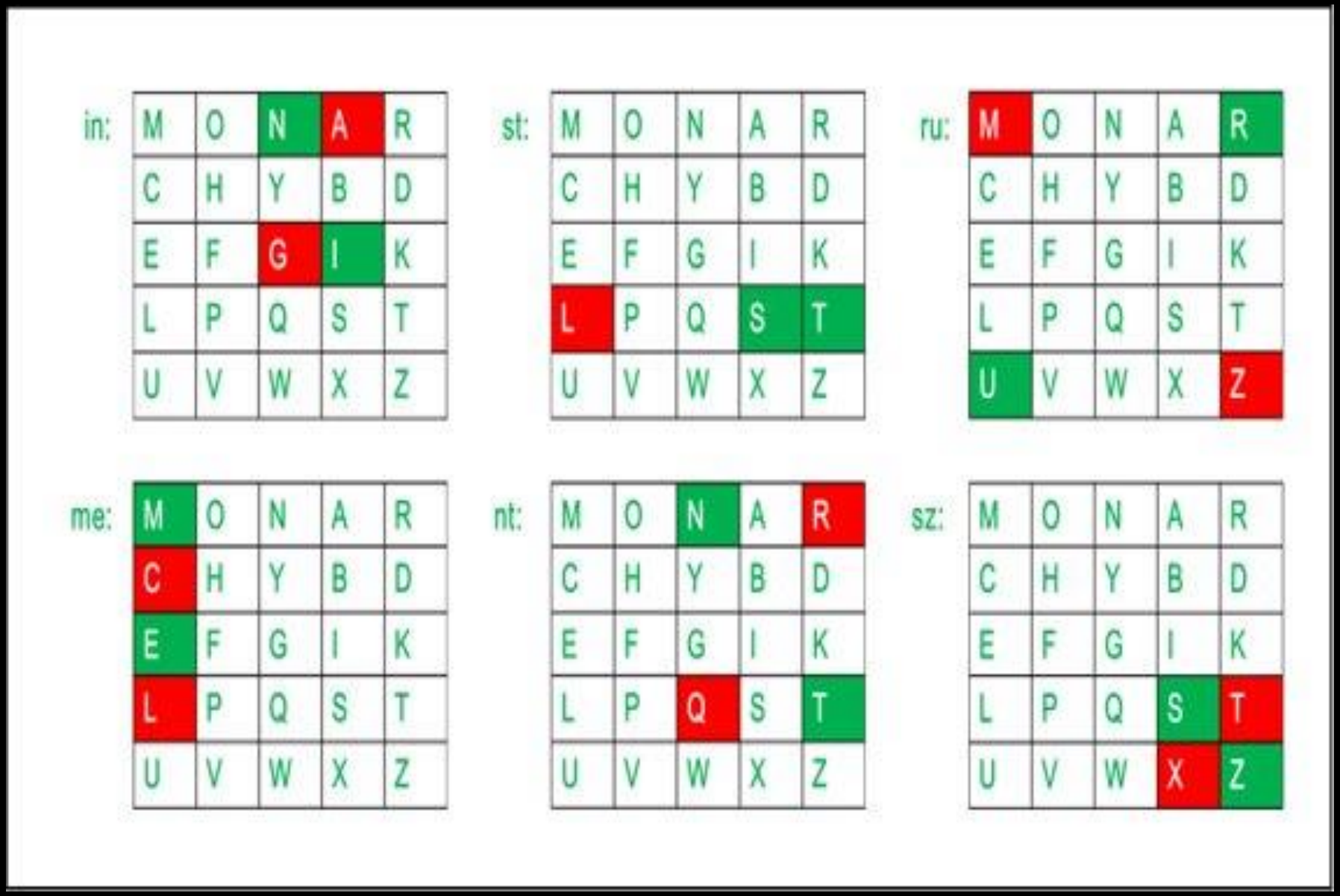
- **Plain Text: "instrumentsz“**
- **Encrypted Text: gatlmzclrqtx**

PLAYFAIR Cipher Challenge

- Encrypt the message "Hide the gold in the tree stump“ using play fair cipher by taking key as: “PLAYFAIR EXAMPLE”

DECRYPTION

1. **Generate the key Square(5×5) at the receiver's end.** F*or both* ***encryption*** *and* ***decryption****, the* ***same key*** *is to be used as per the same rule.*
2. The ciphertext is split into pairs of two letters (digraphs).
3. **For Decryption:**
   - **If both the letters are in the same column,** take the letter above each one ie letter at the top.
   - **If both the letters are in the same row,** take the letter to the left of each one
   - **If neither of the above rules is true, f**orm a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.


in:
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
st:
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
ru:
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
me:
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
nt:
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
sz:
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z

EXAMPLE

ALBERTI CIPHER

- The development of Polyalphabetic Substitution Ciphers was the cryptographers answer to **Frequency Analysis**. The first known polyalphabetic cipher was the *Alberti Cipher* invented by Leon Battista Alberti in around 1467
- Sometimes called a ***formula disk cipher***

ALBERTI CIPHER ENCRYPTION

- Two concentric disks with an equal number of different letters are assigned. The **outer disk** is called the ***stabilis*** disk because it cannot be moved and is used to mark **plain text** , the **inner disk** is the ***mobilis*** and it is used to mark **cipher text.**
- There are 20 letters and 4 digits on the outer disk, so letters such as H,J,K, U,W, Y and so on have to be removed or replaced in the plaintext. This design was used to additionally obfuscate the plaintext and eliminate common patterns.
- There are generally 2 methods given for encryption procedure
- Encryption uses a disk with two alphabets. By rotating a disk, it shifts an alphabet to the next letter.
- To encrypt, the disk is set in one position, the initial shift (which can be zero) corresponds to the number of letters shifted at the beginning

Encryption: Method 1

Q. Encrypt **plaintext: DCODE** with the parameters: **initial shift: 1, periodic increment: 2, period: 3**.Alphabets are aligned as

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

The period begins, **D** is coded by **e**, **C** by **d**, **O** by **p**, the period (length 3) ends, the disk is rotated by 2 letters. Alphabets are now aligned like this

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	x	x	y	z	a	b	c

The encrypted message is **edpgh**

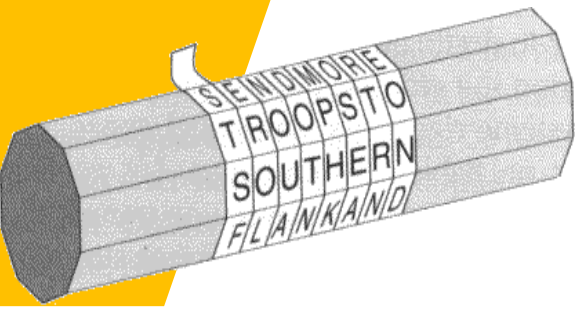
DECRYPTION

decryption needs the disk (or the 2 alphabets) and the parameters: initial position, period and shift.

To cipher a message, the disk is set with the corresponding initial shift. Each letter is identified on the inner disk, and is coded by the letter aligned in the outer disk.

By default, every 4 characters (4 = period), the disk is rotated counter-clockwise of 1 letter (1 = periodic increment).

TRANSPOSITION CIPHER



TRANSPOSITION CIPHERS

A transposition cipher rearranges(permutes) symbols in a block without altering actual values.

•It has the same frequency distribution as the original text . So easily recognizable.

•The letters or words of the plaintext are reordered in some way, fixed by a given rule (the key

EXAMPLE :

- Plaintext: *HELLO MY DEAR*
- Ciphertext: *ELHLMDOYAER*
- Plaintext: "*a simple example*"
- Ciphertext: *"ELPMAXE ELPMIS A"*

i)Simple columnar Transposition

- Write **plain text row by row** in a **predefined column size**
- Ciphertext is to **read the message column by column** as per the key in sorted fashion

A	U	T	H	O	R
1	6	5	2	3	4
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	S	A	V
E	Y	O	U	R	S
E	L	F	A	B	C

yields the cipher

W I R E E R O S U A E V A R B D E V S C A C D O F E S E Y L .

DECRYPTION

- The decryption process is significantly easier if nulls have been used to pad out the message in the encryption process.
- To decipher divide the column lengths by the message length. Write the message out in columns again, then re-order the columns by reforming the key word.

*Decrypt the ciphertext "**ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX**" given the keyword **potato**.*

1. 42 letters in the ciphertext, and the keyword has six letters, so we need 42 ÷ 6 = 7 rows.
2. start by filling in the columns in the order given by the alphabetical order of the keyword, starting with the column headed by "A".
3. continue to add columns in the order specified by the keyword. Read off the plaintext in row order

P	O	T	A	T	O
4	2	5	1	6	3
			A		
			R		
			E		
			S		
			A		
			S		
			X		

P	O	T	A	T	O
4	2	5	1	6	3
			A		
			R		
			E		
			S		
			A		
			S		
			X		

P	O	T	A	T	O
4	2	5	1	6	3
	O		A		O
	S		R		I
	T		E		I
	H		S		A
	E		A		I
	Y		S		E
	L		X		X

P	O	T	A	T	O
4	2	5	1	6	3
P	O	T	A	T	O
E	S	A	R	E	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	A	S	W	E
L	L	X	X	X	X

DECYPTION

DECRYPTION WITH NULLS

- When no nulls have been used , divide the length of the ciphertext by the length of the keyword. If its not a wholenumber then round the answer up to the next whole number and multiply this number by the length of the keyword, to find out how many boxes there are in total in the grid. Finally, take the length of the ciphertext away from this answer.

Eg: ***decrypt the ciphertext "ARESA SOSTH EYLOI IAIEP ENGDL LTAHT FATEN HMW"***, ***with the keyword potato.***

38 ÷ 6 = 6.3333, round this up to the next number, which is 7 rows

multiply 6 x 7 we get 42, and 42 - 38 = 4. Hence we need 4 placeholders in the last row.

P	O	T	A	T	O
4	2	5	1	6	3
P	O	T	A	T	O
E	S	A	R	E	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	A	S	W	E
L	L				

Simple Columnar Transposition Challenge

1. Encrypt the plaintext "The tomato is a plant in the nightshade family" using the key *tomato*.
2. Encrypt the plaintext "This is a columnar transposition" using the key *apple*.

DOUBLE TRANSPOSITION CIPHER

- During World War I and II, Double columnar transposition cipher was used by various agents and military forces.
- Double columnar transposition cipher is equivalent to using **two columnar transposition ciphers, with same or different keys.**
- **Plain text :** THIS IS A SECRET MESSAGE
  1st Columnar Key: LEONARDO
  2nd Columnar Key: DAVINCI

L E O N A R D O
4 3 6 5 1 8 2 7

T H I S I S A S
E C R E T M E S
S A G E

First cipher
text: **ITAEHCATESSEEIRGSSSM** **D A V I N C I**
3 1 7 4 6 2 5

I T A E H C A
T E S S E E I
R G S S S M
final cipher text: **TEGCE MITRE SSAIH ESASS**

Cryptanalysis of Transposition Cipher

- Both sender and receiver should share a common secret, usually a keyword, that determines the exact transpositions that should be applied to the text.
- Transposition ciphers usually require more memory and more complex operations, than substitution ciphers. That is why modern ciphers implemented pragmatically and electronically are usually based on substitutions, and less often on transpositions.

ii)Row Transposition Ciphers

- A transposition cipher where lettera are written out in row order over a specified number of columns define by the key. Then reorder the columns according to some key(sorted) before reading off the rows

Key:	**4**	**3**	**1**	**2**	**5**	**6**	**7**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Plaintext:	a	t	t	a	c	k	p	t	a	t	a	c	k	p
	o	s	t	p	o	n	e	t	p	s	o	o	n	e
	d	u	n	t	i	l	t	n	t	u	d	i	l	t
	w	o	a	m	x	y	z	a	m	o	w	x	y	z

Ciphertext: **TATACKPTPSOONENTUDILTAMOWXYZ**

Row transposition cipher challenges

- Encrypt the **Plaintext : THESIMPLESTPOSSIBLETRANSPOSITIONSXX** using row tranposition cipher with **Key (R): 2 5 4 1 3**
- Encrypt the Plain text: **ACONVENIENTWAYTOEXPRESSTHEPERMUTATION** using row tranposition cipher with **Key (R): C O M P U T E R**

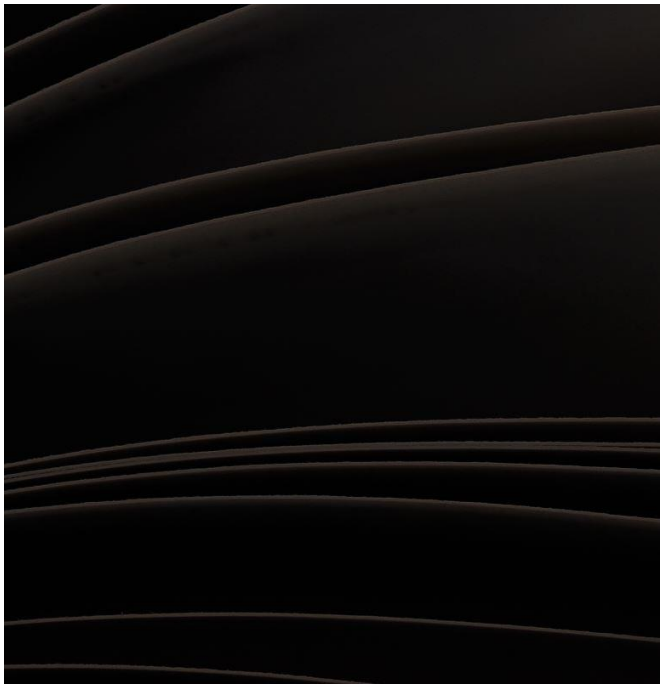
Plaintext T H I S I S A S E C R E T M E S S A G E

Rail Fence Encoding

key = 4

T						A						T						G	
	H				S		S				E		M				A		E
		I		I				E		R				E		S			
			S						C						S				

Ciphertext T A T G H S S E M A E I I E R E S S C S



iii)Rail Fence Technique

Plain text is written as a sequence of diagonals depending on the key and then read it as a squenc of rows.

Rail Fence Cipher Encryption

- Rail Fence cipher is also known as **zigzag cipher.**
- **ENCRYPTION:**

  For encryption write the message diagonally in zigzag form in a matrix having **total rows = key** and **total columns = message length**. Then r**ead the matrix row wise horizontally** to get encrypted message.

CHALLENGE: Encrypt the message '**WE ARE DISCOVERED FLEE AT ONC**E' using rail fence cipher where **key=3**

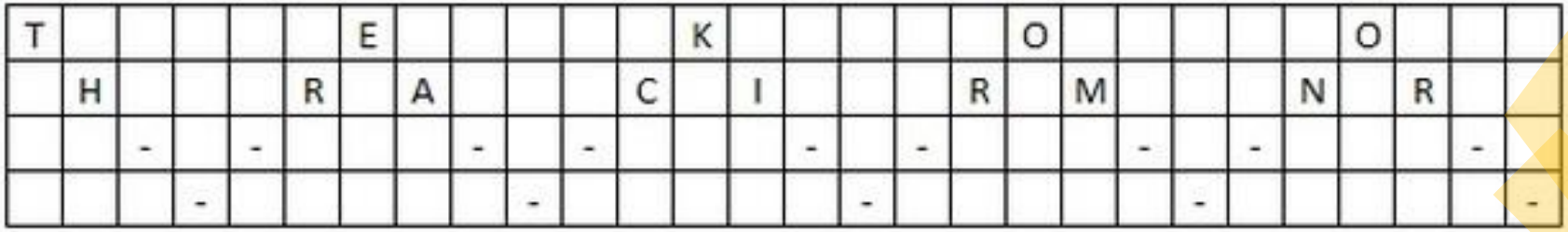
Rail Fence Cipher Decryption

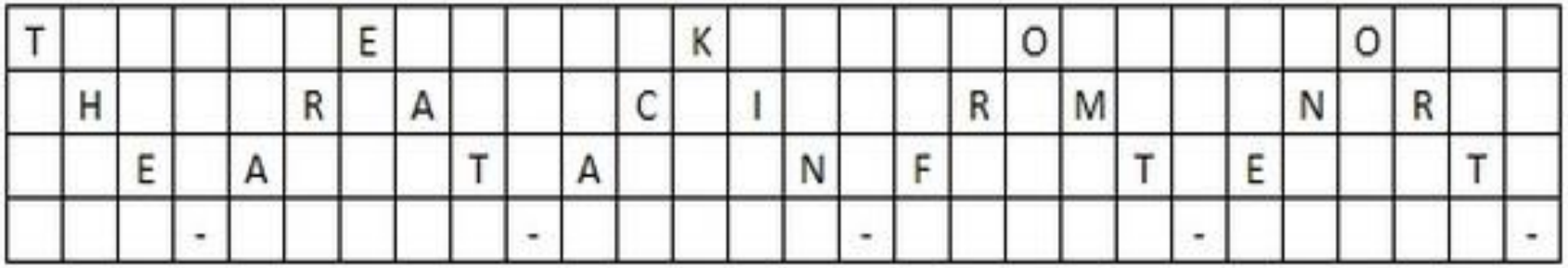
DECRYPTION

- Construct diagonal grid from things known
  - Number of columns in matrix = len(cipher-text)
  - Number of rows = key
- Once diagonal grid is ready sart filling characters horizontally, leaving a dash in place of the spaces yet to be occupied. Gradually, replace all the dashes with the corresponding letters, and read off the plaintext in zig zag from the table.
- Decrypt ciphertext **"TEKOOHRACIRMNREATANFTETYTGHH",** with a key of 4

T						E						K						O						O			
	-				-		-				-		-				-		-				-		-		
		-		-				-		-				-		-				-		-				-	
			-						-						-						-						-

Rail Fence Cipher Decryption





CHALLENGE: **Decrypt the ciphertext: TNDGHUIEKNDMETIO using key=3**

HOMOPHONIC SUBSTITUTION CIPHER

- Homophonic Substitution cipher is a substitution cipher in which single plaintext letters can be replaced by any of several different ciphertext letters ie one plain text alphabet can map to more than one cipher text alphabet
- The number of characters each letter is replaced by is part of the key

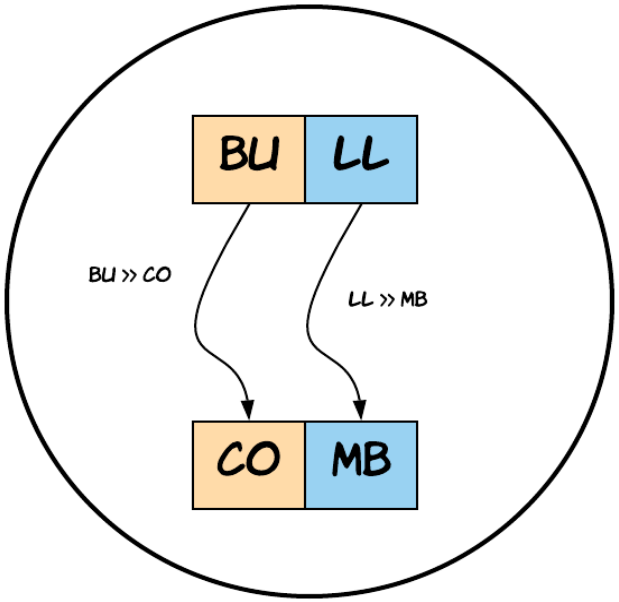
Example: Key Phrase:”18 fresh tomatoes and 29 cucumbers”. Homophonic Substitution is defined as:

Plaintext Alphabet	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
Ciphertext Alphabet	1	8	F	R	E	S	H	T	O	M	A	N	D	2	9	C	U	B	G	I	J	K	L	P	Q	V	W	X	Y	Z	0	3	4	5	6	7

Plain text: "run away, the enemy are coming"

Cipher Text: “Q0I 1486, YNH OGSB6 1QH RKB2GA

POLYGRAM SUBSTITUTION CIPHER



Polygram cipher systems are ciphers in which **group of letters are encrypted together,** and includes **enciphering large blocks of letters**.

Encryption includes substitution of a block of multiple letters from plaintext with the corresponding group of ciphertext.

For example the plaintext group "ABC" could be encrypted to "RTQ", "ABB" could be encrypted to "SLL", and so on

Example of such ciphers are **Playfair,** and **Hill ciphers.**

Attack models for Cryptanalysis

Total break: deducing and obtaining a secret key.

Global deduction: discovering an algorithm, which allows to decrypt many messages, without knowing the actual secret key.

Local deduction: discovering an original plaintext of the specific given ciphertext.

Information deduction: obtaining some information about the secret key or original message (for example, a few bits of the key or information about a plaintext format).

CRYPTANALYSIS ATTACKS-Theoretical Attack Models

1. **Known Plain Text Attack:** Attacker tries to collect all possible plaintext/ciphertext pairs and tries to find relationship among them. **Assumption:** Eve has plain text which has been made public by alice and use it for cryptanalysis of further message assuming alice hasn't changed key. During known-plaintext attacks, the attacker has access to the ciphertext and its corresponding plaintext. His goal is to guess the secret key (or several secret keys) or to develop an algorithm which would allow him to decrypt any further messages.Prone: Substitution ciphers, Enigma ciphers
2. **Chosen-Plaintext Attack:**During the chosen-plaintext attack, a cryptanalyst can choose arbitrary plaintext data to be encrypted and then he receives the corresponding ciphertext. He tries to acquire the secret encryption key or alternatively to create an algorithm which would allow him to decrypt any ciphertext messages encrypted using this key (but without actually knowing the secret key). This is a rather comfortable situation for the attacker. During breaking deterministic ciphers with the public key, the intruder can easily create a database with popular ciphertexts, for example with popular queries to the server. After that he will be able to find the meaning of many intercepted encrypted messages, by simply comparing them with his own database entries.

CRYPTANALYSIS ATTACKS-Theoretical Attack Models

1. **Known Ciphertext Attack(Cipher Text Only Attack:):** Eve has only access to cipher text and tries to find key and plain text. The goal is to recover as much plaintext messages as possible or (preferably) to guess the secret key. After discovering the encryption key, it will be possible to break all the other messages which have been encrypted by this key. **Assumption:** Eve knows algorithm and can intercept the message. he most important methods are: **Frequency Analysis, Attack on Two-Time Pad**
2. **Chosen-Ciphertext Attack:** During the chosen-ciphertext attack, a cryptanalyst can analyse any chosen ciphertexts together with their corresponding plaintexts. His goal is to acquire a secret key or to get as many information about the attacked system as possible. **Assumption:** Eve has access to Bob's Computer.
3. **Chosen-key attacks:** Chosen-key attacks are a bit different than other kinds of cryptographic attacks. Usually, they are intended to not just break a cipher but to break the larger system which relies on that cipher.

Cryptographic Attacks

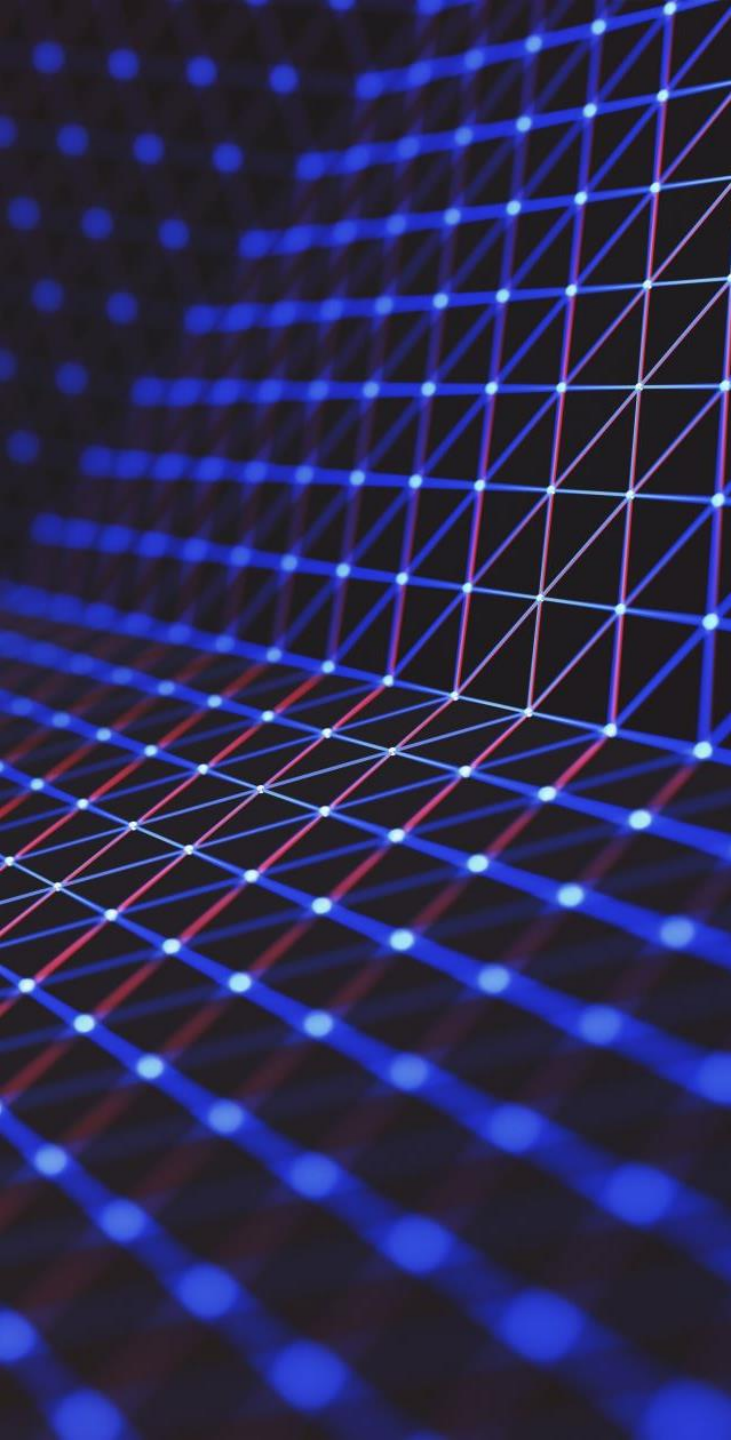
- **Replay Attack:** During replay attacks the intruder sends to the victim the same message as was already used in the victim's communication. The message is correctly encrypted, so its receiver may treat is as a correct request and take actions desired by the intruder. The attacker might either have eavesdropped a message between two sides before or he may know the message format from his previous communication with one of the sides. This message may contain some kind of the secret key and be used for authentication.
- **Brute Force Attack/Exahaustive-Key Search Attack:** During the brute-force attack, the intruder tries all possible keys (or passwords), and checks which one of them returns the correct plaintext. **Assumption:** Eve knows algorithm, knows key domain and can intercept the message. Using intercepted cipher Eve decrypts cipher text with all possible keys until plain text make sense. The amount of time that is necessary to break a cipher is proportional to the size of the secret key. The maximum number of attempts is equal to $\mathbf{2^{key\ size}}$, where **key size** is the number of bits in the key.
  - Eg: **Dictionary Attack** Dictionary attacks are a kind of brute-force attacks, in which the intruder attempts to guess a password by trying existing words or popular expressions.

Cryptographic Attacks

- **Frequency Analysis:** Attacker study the frequency of letters or groups of letters in a ciphertext. For each language proportions of appearance of all characters are slightly different, so texts written in a given language have some certain common properties, which allow to distinguish them from texts written in other languages. For example, in English there are often used vowels like e, o, a or a consonant t. On the other hand, there are some very rare letters, for example z or x.
- **Man in the Middle:** During the man-in-the-middle attack, the hidden intruder joins the communication and intercepts all messages.First, the attacker creates two secret keys. Then, he uses the first key to start the communication with the first side. The received answer is encrypted but the intruder can decrypt it easily, as he knows the key. He encrypts the message again, this time with the second key. The encrypted message is then send back to the second side. Then, after receiving the answer from the second side, he decrypts the message, reads it, encrypts by the first key and sends back to the first site. In this way, the whole communication moves through the attacker. He can receive a lot of information about the whole system and even successfully impersonate authorized persons and reach the access for hidden data.

Cryptographic Attacks

- **Meet in the middle:** The meet-in-the-middle attack is one of the types of known plaintext attacks. The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm.
- **Denial Of Service Attacks:** A Denial-of-Service attack (DoS attack) is an attack where an attacker attempts to disrupt the services provided by a host, by not allowing its intended users to access the host from the Internet. If the attack succeeds, the targeted computer will become unresponsive and nobody will be able to connect with it. It can be done by: **Reducing Performance, Exhausting**



Features of Symmetric Cryptoraphy

unconditional security

- no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

computational security

- given limited computing resources (eg time needed for calculations is greater than age of universe), the cipher cannot be broken

anooja@somaiya.edu

Thank You