Cryptography and Network Security 19ECS305

Module 1 – Part - 2

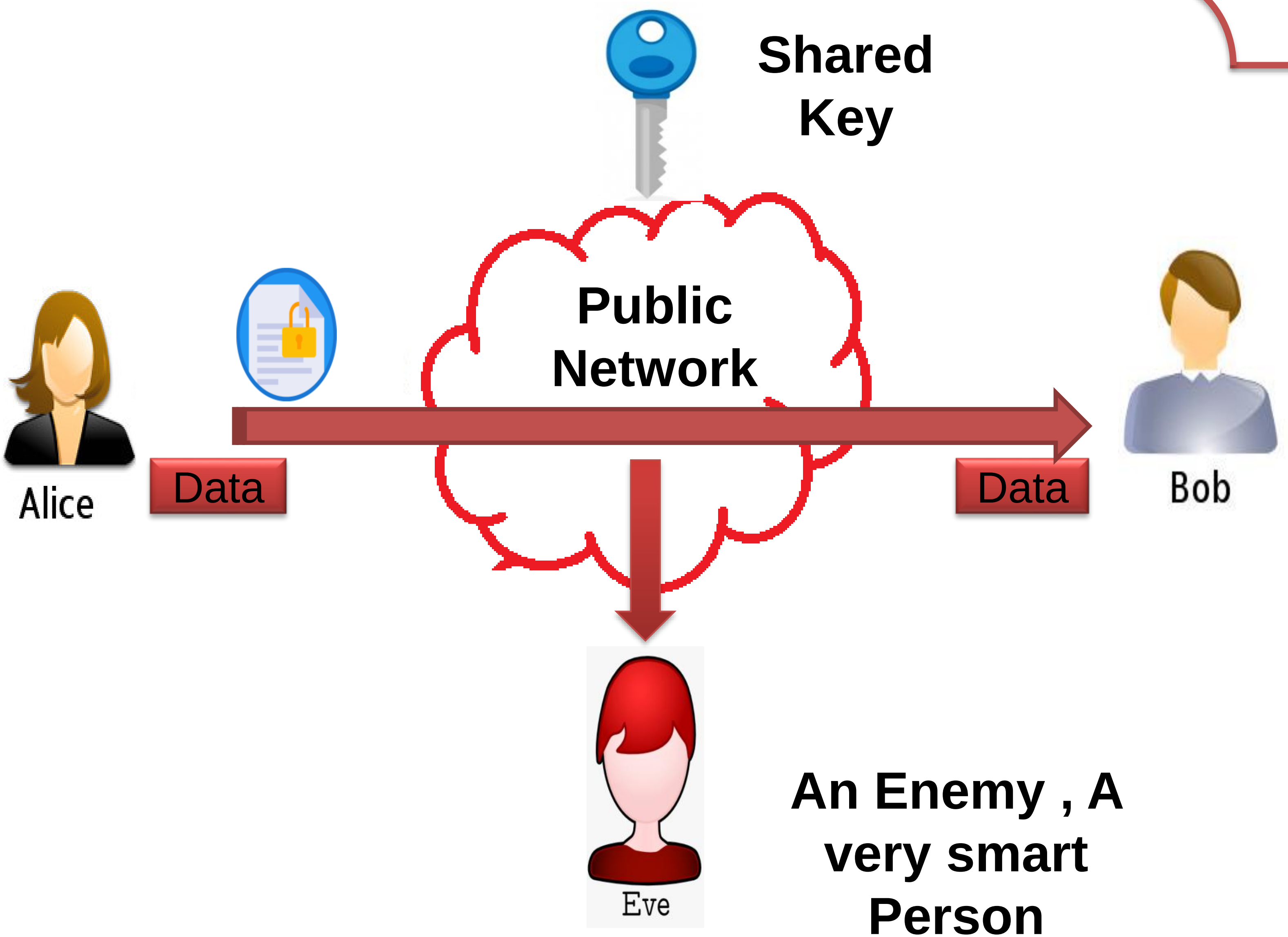
Classical Encryption Techniques: Substitution Techniques**,** Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Hill Cipher Polyalphabetic Ciphers.Transposition Techniques.

Arif Mohammad Abdul

GITAM

(Deemed to be University)

Symmetric Key Cryptography



Alice, Bob, Eve Framework

Introduction

Cryptography is the art of achieving security by encoding messages to make them non-readable

1. **Plain text**

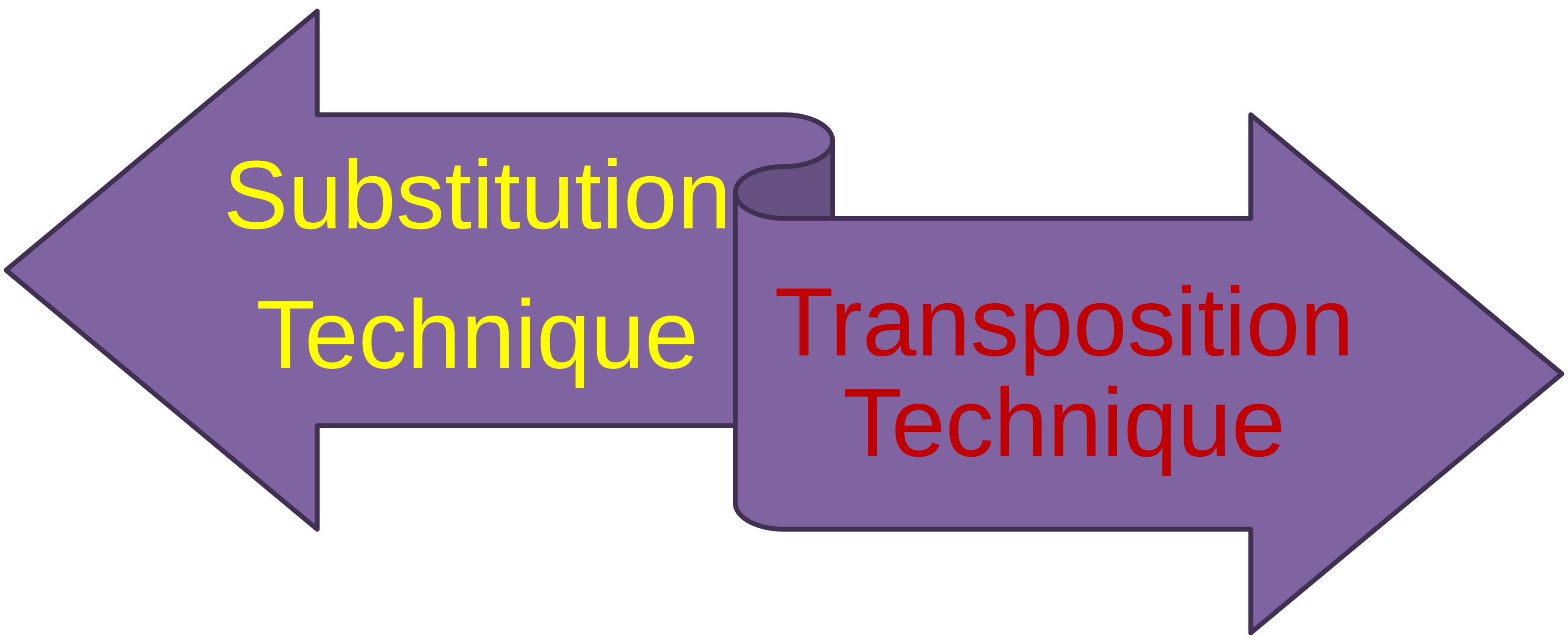
Clear text or plain text signifies that can be understood by the sender, the receiver, and also anyone else who gets an access to that message

2. **Cipher text**

When a plain text message is codifies using any suitable technique, the resulting message is called as cipher text.

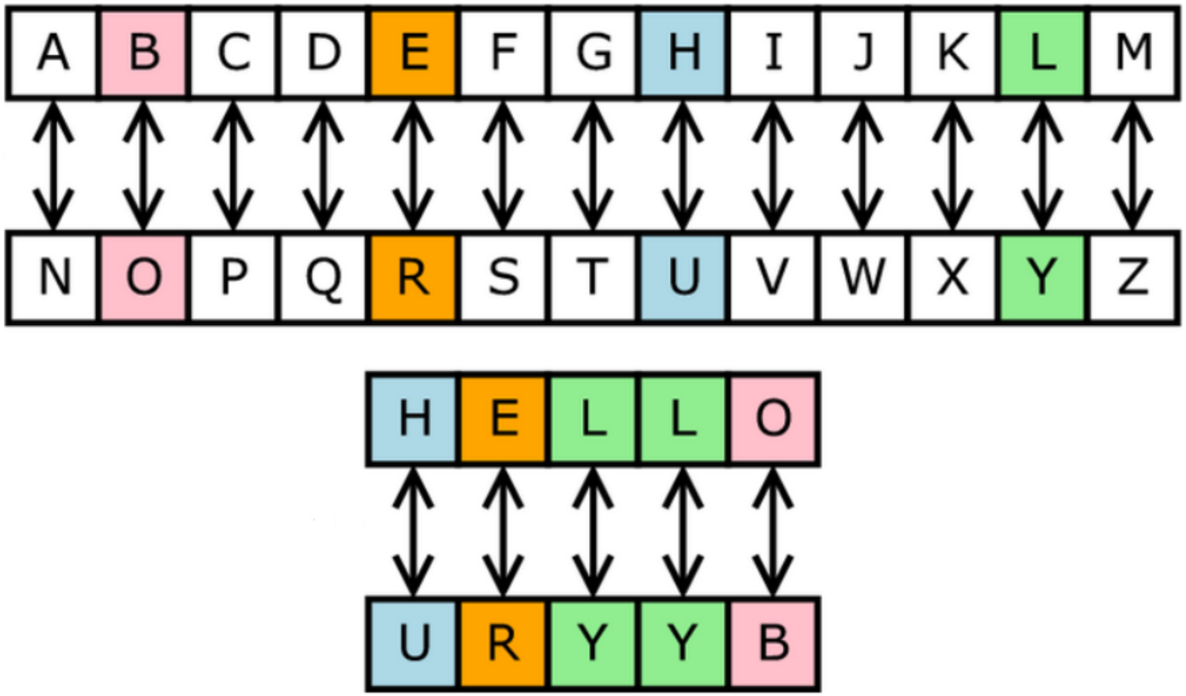
Classical Encryption Techniques

- Have two basic components of Classical techniques:



Substitution Techniques

- In the substitution cipher technique the characters of a plain text message are replaced by other characters, or numbers or symbols.



Types of Substitution Techniques

- Caesar Cipher
- Monoalphabetic Cipher
- Polyalphabetic Cipher
- Play fair Cipher
- Hill Cipher


The
Caesar cipher

Caesar Cipher

- Caesar Cipher replaces each alphabet with the alphabet after shifting “x” times to the right.
- The amount of the shift (x) is the encryption key.
- The shift is a cyclic shift (after the alphabet Z will follow the alphabet A).
- For decryption you reverse the process and replace the cipher text alphabet with the alphabet after doing a left shift by x alphabets.

Example of Caesar Cipher

- Let us assign a numerical equivalent to each other.

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

- Let's consider an example when the key is 2.

  If X = 2 is a key

  A $\longrightarrow$ C, B $\longrightarrow$ D and so on….

Example of Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Key = 2

- Plaintext : meet me later
- Ciphertext : OGGV OG NCVGT

Key = 3

Caesar Cipher with a shift of 3

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

Shift: 0

Plain Text: Hello

Cipher Text:

Example of Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

A shift may be of any amount, the general Caesar algorithm is:

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

If $k = 4$

$$C = E(gitam) = (g + 4) \bmod (26)$$

$$= (6 + 4) \bmod (26)$$

$$= (10) \bmod (26) = 10 = \mathbf{K}$$

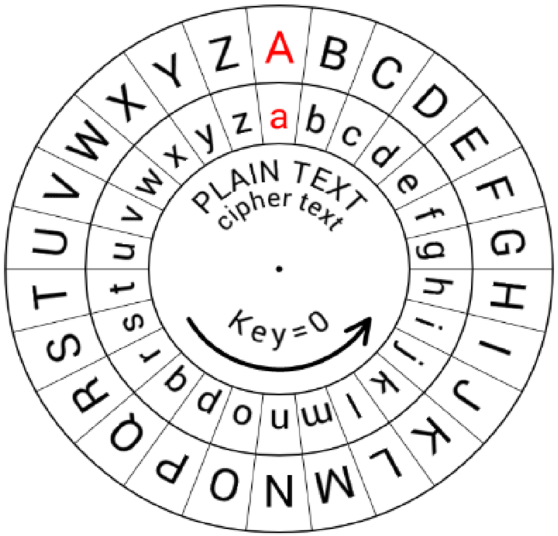
Plain text = **gitam**

Cipher text = **KMXEQ**

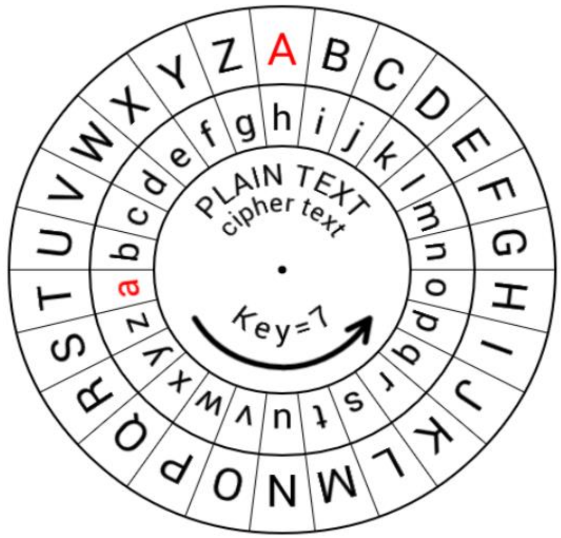
Example of Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

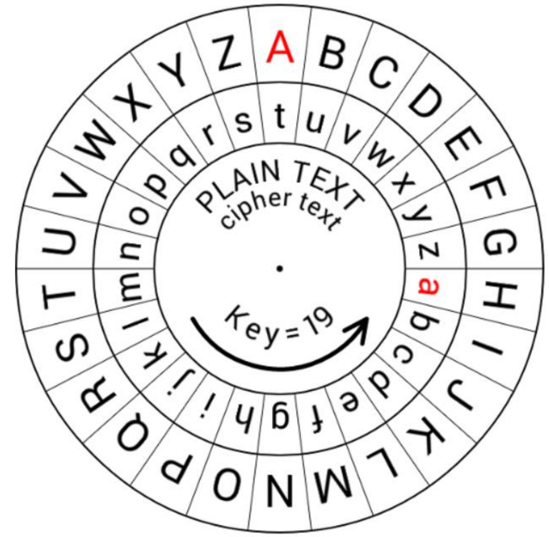
Shift of 0



Shift of 7



Shift of 19



Plaintext : meet me after toga party (Key = 3)

Ciphertext : ?


Brute Force
Attack

Characteristics

- Three important characteristics of Caesar Cipher enabled attacker to use a Brute-force attack.

  1. **The Encryption and Decryption algorithms are known.**
  2. **There are only 25 keys to try.**
  3. **The language of the plaintext is known.**


CODEBREAKING

Example

Plaintext:

Meet me after the toga party

Ciphertext: shift of 3

PHHW PH DIWHU WKH WRJD SDUWB

Applying Brute force attack on the above Ciphertext

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

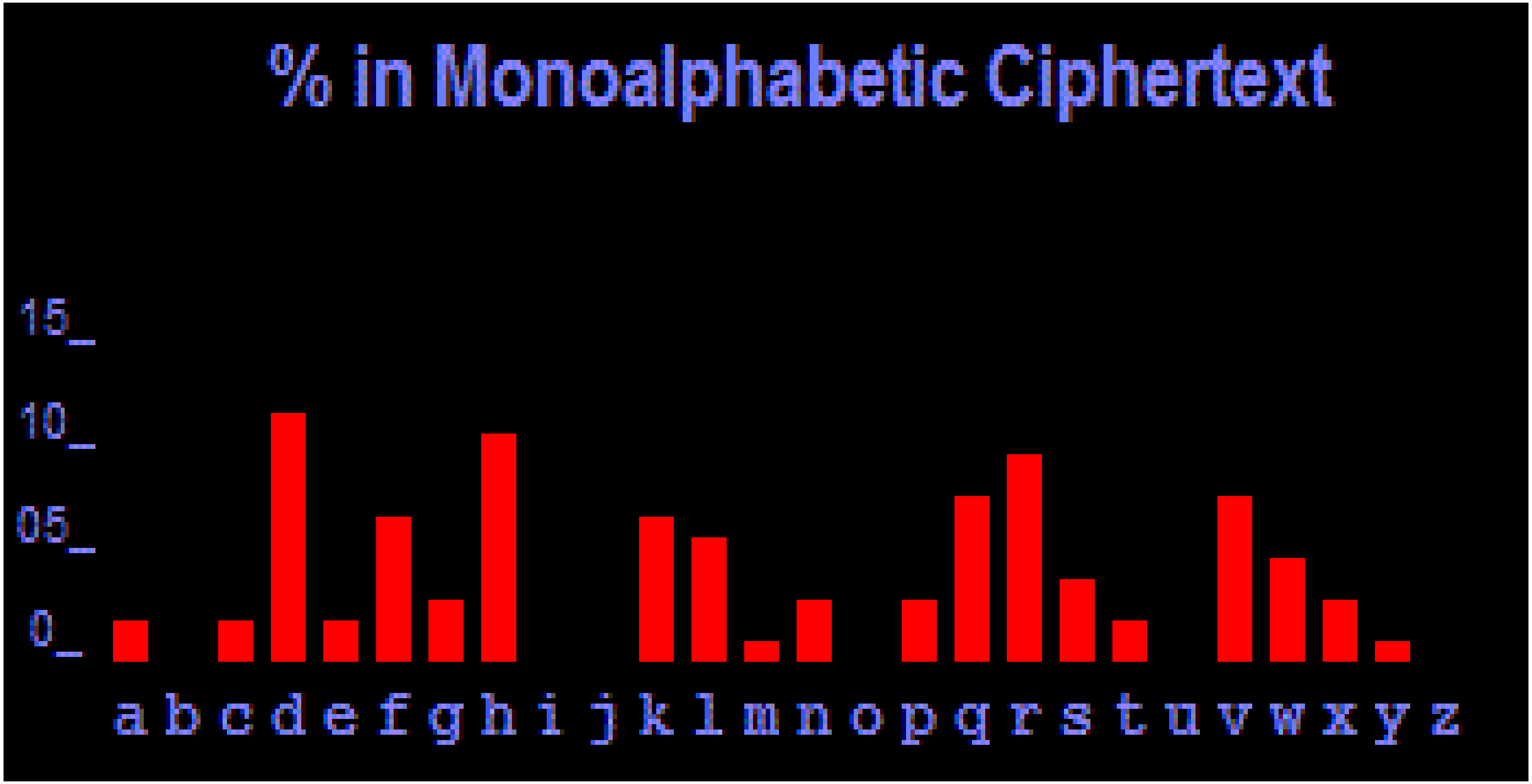
Questions

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

1. You agreed to use a Caesar cipher with a key of k=5 with a friend. While sitting in a group, the friend hands you over a message that says "QNGWFWD". Decrypt the message.

2. Suppose you actually forgot the key. How many decryption computations of the cipher text "QNGWFWD" do you need to perform to reach to the plaintext? (Consider the worst case.)

Monoalphabetic Cipher



Monoalphabetic Cipher

- When using Caesar cipher on English letters, the key size is limited to 26, the key size is 26.
- An attacker can easily brute force such cipher by trying all 26 possible options for the key.
- With only 26 possible keys, Caesar Cipher is far from secure.

Monoalphabetic Cipher

- Each plaintext alphabet is assigned to a different unique ciphertext alphabet.
- Key assigns the mapping for each alphabet.
- Key is a permutation of alphabet set

  (n! permutations for n-element set)

  $26! >= 4 * 10^{26}$

Monoalphabetic Cipher Example

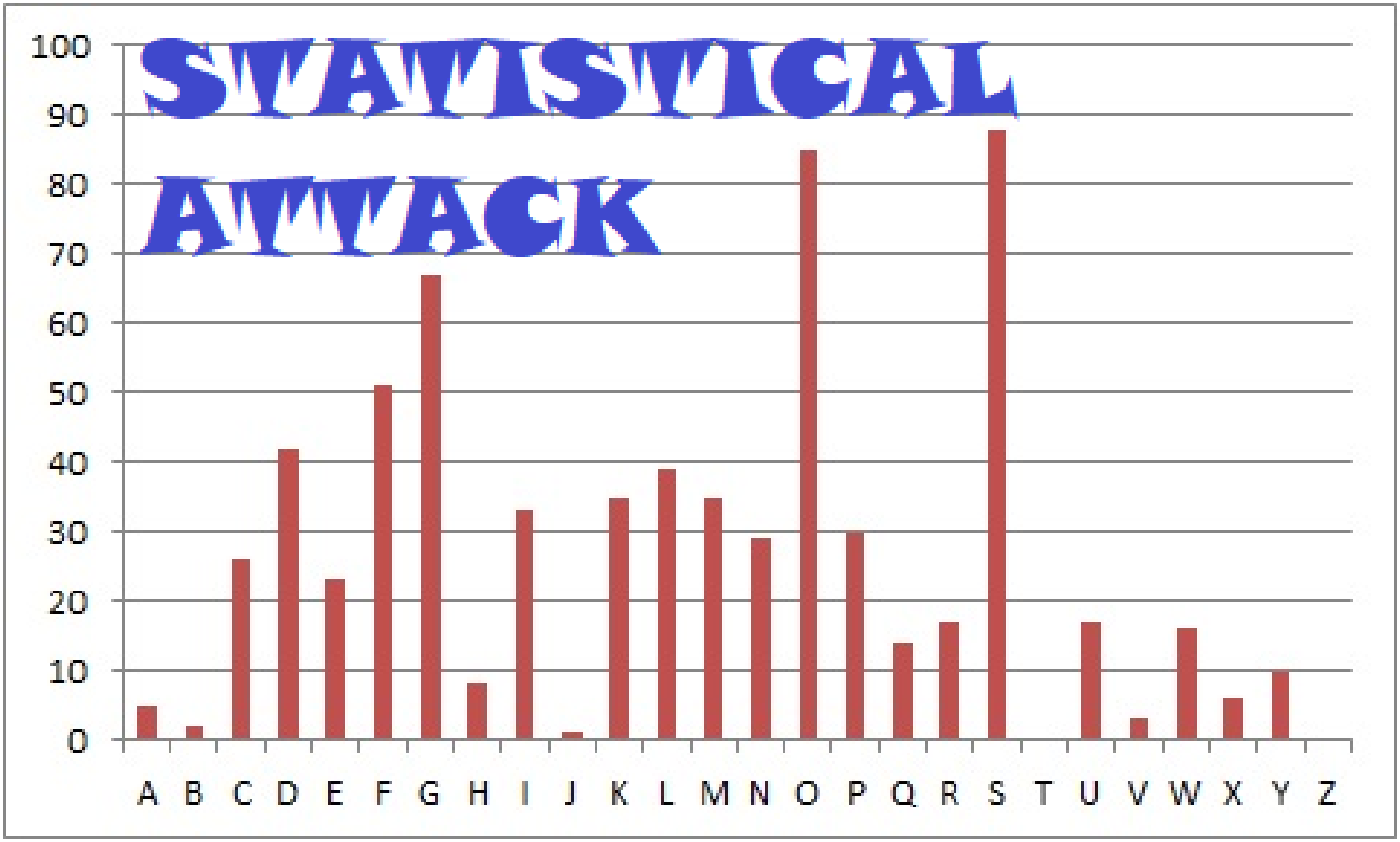
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key	D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

- Plaintext : **MEETMELATER**
- Ciphertext : ?

  DKVQFIBJWPESCXHTMYAUOLRGZN

- Ciphertext : **AOVVFAA**
- Plaintext : ?

Monoalphabetic Cipher



Monoalphabetic Cipher

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

- The Monoalphabetic ciphers do not change the frequency of characters in the ciphertext.
- Which makes the ciphers vulnerable to statistical attack.
- For example,
- **Using a pair of letters (digrams)**, the letter **H** is more likely to follow the letter **T** than others,
- While the letter **U** is likely to follow the letter **Q**.
- Also, **among the triplet (trigrams)** of letters **T**, **H**, **E** occur very often as well.
- Therefore, **such frequency based cryptanalysis technique** can also be used by **analyzing the sequence of alphabets**.

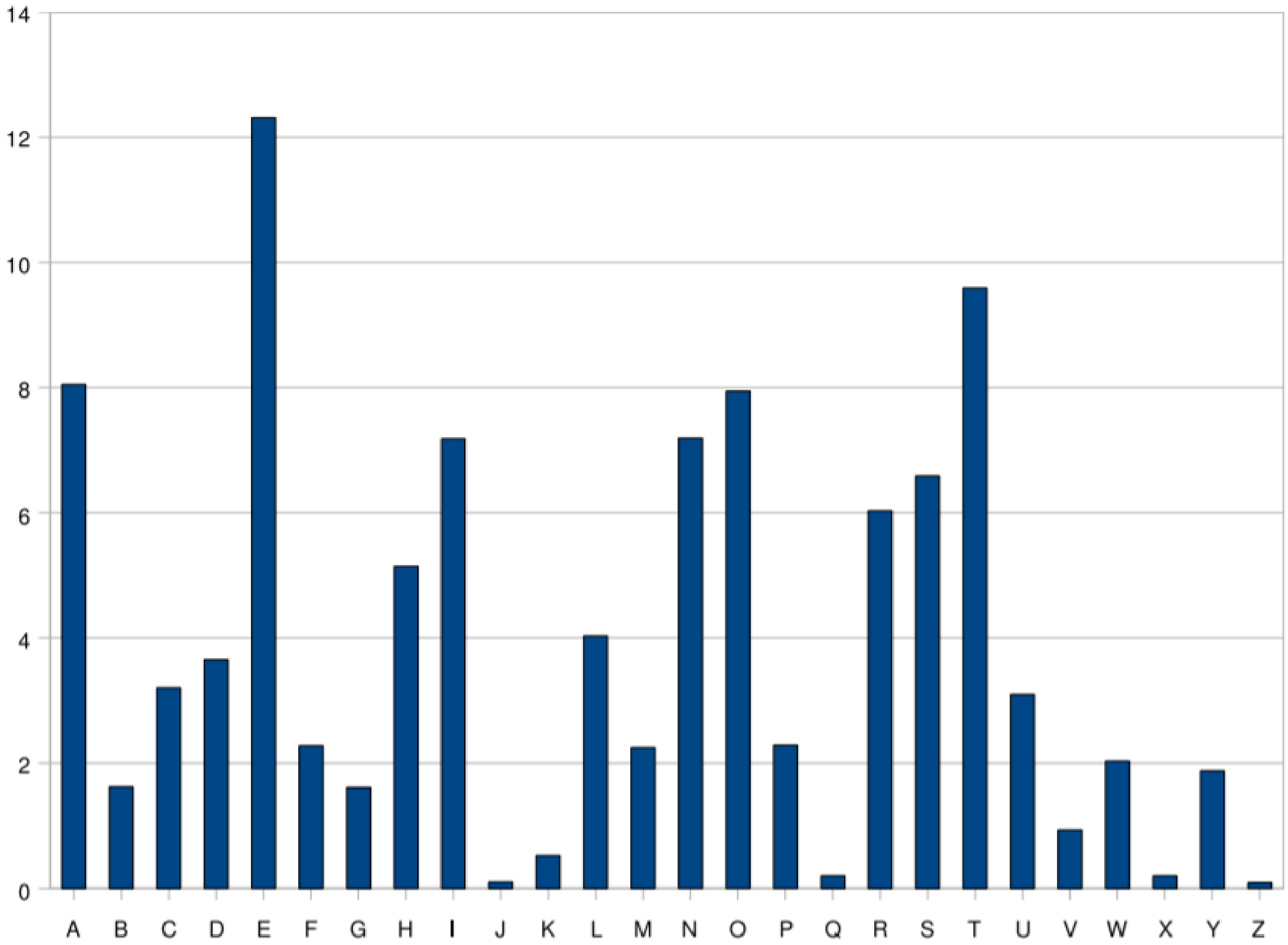
Monoalphabetic Cipher

- **For example,**
- The letter **E** occurs the most often, followed by the letter **T**. And, there are **other alphabets that occur less frequently**.

- **For example,**
- The letter **Z** occurs the **least frequently** and the letter **Q** is the **second to least frequent**.

- Such **alphabet frequency** biases that are natural in plaintext use, **can produce vulnerability** to the attacker who wishes to **break the cipher**.

Relative frequency of the letters in English text



For Example: Letter E is the most frequently used letter in English text

Early to bed, and early to rise, makes a man healthy, wealthy and wise.

Statistical Attack

- Below **Cipher text ZW** appears three times.
- Based on **alphabet frequency th** digram are more frequent then **Z** replace with **t** and **W** replace with **h**.
- Similarly in trigram along with **th** alphabet **e** is more frequent.

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that 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
```

- Only four letters have been identified, but already we have quite a bit of message.
- Continued analysis of frequencies plus trial and error should easily yield a solution.
- **The complete plaintext, with spaces added between words as follows:**

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


Polyalphabetic
cipher

Polyalphabetic Cipher

- As discussed, Monoalphabetic cipher is vulnerable to cryptanalysis using frequency analysis.
- To avoid producing the same biased frequency distribution for the ciphertext.
- Polyalphabetic cipher uses multiple substitution ciphers for plaintext alphabet.
- So that the same plaintext alphabet can be mapped into different ciphertext alphabets.
- **A key is used to specify such mapping.**
- **Vigenere cipher** is one of the simpler algorithms that implements polyalphabetic cipher.

Polyalphabetic Cipher Example

- **Key:** LEMON
- Plaintext : **MEET ME LATER**
- Ciphertext : **XIQH ZP PMHRC**

Plaintext	**M**	**E**	**E**	**T**	**M**	**E**	**L**	**A**	**T**	**E**	**R**
Key	**L**	**E**	**M**	**O**	**N**	**L**	**E**	**M**	**O**	**N**	**L**
Ciphertext	**X**	**I**	**Q**	**H**	**Z**	**P**	**P**	**M**	**H**	**R**	**C**

- The repeated key, LEMON LEMON LEMON and so on, until the last alphabet of the plaintext.
- **How will get this ciphertext?**

How will get this ciphertext?

- Apply Caesar Cipher using the corresponding key alphabet.
- The first letter is encrypted using the key alphabet **L**, which corresponds to shifting plaintext letter **M** by **11** alphabets to become the letter **X**.
- The next alphabet **E** is encrypted using the key alphabet **E**, which corresponds to 4 shifts and will produce the letter **I** .
- The third plaintext letter which is also **E** is encrypted with the key letter **N** and produces the ciphertext alphabet **Q**.

Polyalphabetic Cipher Example

Plaintext	M	E	E	T	M	E	L	A	T	E	R
Key	L	E	M	O	N	L	E	M	O	N	L
Ciphertext	X	I	Q	H	Z	P	P	M	H	R	C

- Encryption:

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$

$$= (p_1 + k_{1 \bmod 5}) \bmod 26$$

$$= (M + L) \bmod 26$$

$$= (12 + 11) \bmod 26$$

$$= (23) \bmod 26$$

$$= 23 \;\; = X$$

Examples

1. Key : GITAM

- Plaintext : **online classes**
- Ciphertext : ?

2. Key : LEMON

- Plaintext :**?**
- Ciphertext :LXFOPVEFRNHR

VIGNERE CIPHER

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
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	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	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	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	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	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	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	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	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

Vigenere Table

KEY

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
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

Key : GITAM

Plaintext: **security**

Ciphertext:?

Key: DECEPTIVE

Plaintext: **we are discovered save yourself**

Ciphertext:?

Which attack is possible to Eve on Polyalphabetic Cipher?

- Given the **modulus n** ($C_i = (p_i + k_{i \bmod m}) \bmod 26$**)** and a key length m,
- The number of possible keys attempts on Vigenere Cipher is n^m.
- To improve the difficulty grows exponentially with m.
- In the **LEMON example**, the key is 5 alphabet long i.e., possible keys attempts 26^5. The brute force difficulty for the attacker, is only (26^5).
- To improve the security, increases the key length m, the brute force difficulty grows exponentially with m.
- Increasing the key length **alphabet frequency** also improves Which makes the ciphers vulnerable to statistical attack.

Questions

- Eve has intercepted the Ciphertext : UVACLYFZLJBYL. Show how eve can use a brute-force attack to break the cipher.
- Use the Vigenere cipher with keyword "HEALTH" to encipher the message "life is full of surprises".
- If keyword length is 7 then how many possible key attempts require to break in Polyalphabetic cipher.

One-Time Pad

Vernam Cipher

OTP

One-Time Pad

- Developed by Gilbert Vernam in 1918, another name: ***Vernam Cipher***
- The key
  - a truly random sequence of 0's and 1's
  - the same length as the message
  - use one time only
- The encryption
  - adding the key to the message modulo 2, bit by bit.

Encryption $c_i = m_i \oplus k_i \qquad i = 1,2,3,\ldots$

Decryption $m_i = c_i \oplus k_i \qquad i = 1,2,3,\ldots$

m_i : plain-text bits.
k_i : key (key-stream) bits
c_i : cipher-text bits.

OTP

- The one-time pad (OTP) is valid for only one login session or transaction.
- Random key that was truly as long as the message, with no repetitions.
- OTP is unbreakable.
- Each key should be used once and destroyed by both sender and receiver.
- OTP provides perfect secrecy.

Vernam Cipher

Vernam proposed a bit-wise exclusive or of the message stream with a truly random zero-one stream which was shared by sender and recipient.

Example:

SENDING -------

message: 0 0 1 0 1 1 0 1 0 1 1 1 ...

pad: 1 0 0 1 1 1 0 0 1 0 1 1 ...

XOR --------------------------

cipher: 1 0 1 1 0 0 0 1 1 1 0 0 ...

RECEIVING ---------

cipher: 1 0 1 1 0 0 0 1 1 1 0 0 ...

pad: 1 0 0 1 1 1 0 0 1 0 1 1 ...

XOR --------------------------

message: 0 0 1 0 1 1 0 1 0 1 1 1 ...

Question

- Suppose a message gets encrypted using a bit-by-bit XOR with a key, i.e., the key bit of one flips the message bit at the corresponding location. For example, if p=010, and k=110, then c=100.
- If Alice wants to send a 1-Byte message, p=01100011, and Alice and Bob agrees on the key, k=11010001, then what is the ciphertext, c?

PlayFair Cipher

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

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

Playfair Cipher

As we discussed in early sessions,

- With only 25 possible keys, the **Caesar cipher** is far from secure.
- **Monoalphabetic cipher** is easy to break because they reflect the frequency data.
- **Polyalphabetic cipher** is suspected, security strength depends on the length of keyword.
- An improvement is achieved over the **Playfair cipher**.

Playfair Cipher

- Multiple letter encryption cipher.
- **Digrams** in the plaintext as **single units** and translates these into ciphertext.
- It is based on the use of **5 * 5 matrix** of letters constructed using a **keyword**.

F	I	V	E	*
F	I	V	E	M
A	T	R	I	X
O	F	L	E	T
T	E	R	S	.

Playfair Cipher Rules

1. The matrix is constructed by **filling in the letters of the keyword** (Minus duplicate) from left to right and from top to bottom. Example Key is **MONARCHY**
2. Then filling in the remainder of the matrix with the **remaining letters** in alphabetic order.
3. Letter I and J count as **one letter**

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

Rules

4. Plaintext is encrypted **two letters** at a time.

5. **Two plaintext letters** that fall in the same row of the matrix are each replaced by the letter to **the right.**

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

Example: ar in the plaintext that falls in the same row then ciphertext will be RM

Rules

6. **Two plaintext letters** that fall in the **same column** are each replaced by the letter beneath.

Example: mu in the plaintext that falls in the same column then ciphertext will be CM

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

Rules

7. Otherwise, each plain text letter in a pair is replaced by the letter that **lies in its own row and column** occupied by the other plain text letter.

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

Example: hs in the plaintext becomes BP and ea becomes IM

Rules

8. If the two letters of plaintext in a **pair** are the **same**, a **bogus letter** is **inserted** to separate them.

Example: balloon is a plaintext by inserting a bogus letter, plaintext become **ba lx lo on**

Example: hello is a plaintext by inserting a bogus letter, plaintext become **he lx lo**

Rules

9. If the number of characters in the plaintext is **odd**, one extra **bogus letter** is **added** at the end to make the number of characters **even**.

Example: **gitam** is a plaintext by adding a bogus letter at end, plaintext become **gitams**

Playfair Cipher Example

Key : MONARCHY

Plaintext : herole

Ciphertext : CFMNUL

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

Key : MONARCHY

Plaintext : balloon

Ciphertext : ?

Playfair Cipher Example

Key : PLAYFAIR

Plaintext : Secure

Plaintext : Education

Ciphertext :?

Key : KEYWORD

Plaintext : Crypt

Plaintext : Secret Message

Ciphertext :?

Hill Cipher

Hill Cipher

- Another interesting **multiple letter cipher** is the **Hill cipher.**
- Invented by L. S. Hill in 1929.
- Inputs : String of English letters, A,B,…,Z.

  Identify A=0, B=1, C=2, …, Z=25.

  An $n \times n$ matrix **K**, with entries drawn from 0,1,…,25.
  (The matrix **K** serves as the secret key.)
- Divide the input string into blocks of size n.
- **Encryption:** Multiply each block by **K** and then reduce mod 26.
- **Decryption:** Multiply each block by the inverse of **K**, and reduce mod 26.

Hill Cipher Encryption

3 * 3 Matrix

$$C_1 = (k_{11} p_1 + k_{12} p_2 + k_{13} p_3) \bmod 26$$

$$C_2 = (k_{21} p_1 + k_{22} p_2 + k_{23} p_3) \bmod 26$$

$$C_3 = (k_{31} p_1 + k_{32} p_2 + k_{33} p_3) \bmod 26$$

This can be expressed in terms of columns vectors and matrices: **C = KP mod26**

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod 26$$

Hill Cipher Encryption

Example:

Plaintext	**: pay more money**
Key	**: rrtvsvcct**
Ciphertext	**: LNSHDLEWMTRW**

How will get the Ciphertext?

- Divide the input string into blocks of size n

Plaintext : pay more money

p	m	e	n
a	o	m	e
y	r	o	y

Key : rrtvsvcct

$$\begin{bmatrix} r & r & t \\ v & s & v \\ c & c & t \end{bmatrix}$$

3 * 3

How will get the Ciphertext?

Identify A=0, B=1, C=2, …, Z=25 for plaintext.

Plaintext : pay more money

$$\begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix} \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix}$$

Key : rrtvsvcct

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

3 * 3

How will get the Ciphertext?

Multiply each block of plaintext with key **K**

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} * \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} = \begin{bmatrix} 17*15 + 17*0 + 5*24 \\ 21*15 + 18*0 + 21*24 \\ 2*15 + 2*0 + 19*24 \end{bmatrix} \text{mod26}$$

$$= \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \text{mod } 26$$

$$= \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \begin{bmatrix} L \\ N \\ S \end{bmatrix}$$

Hill Cipher Decryption

Ciphertext : LNSHDLEWMTRW

Multiply each block by the inverse of **K.**

How to calculate inverse of K?

$$K^{-1} = \left[\frac{1}{\det K} * \mathrm{Adj}\,(K) \right] \bmod 26$$

det = Determinant

Adj = Adjoint

Determinants

2 * 2 Matrix

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

3 * 3 Matrix

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}$$

$$a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31})$$

Determinant

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

$= 17(18 * 19 - 21 * 2) - 17(21 * 19 - 2 * 21) + 5(21 * 2 - 18 * 2)$

$= 17(342 - 42) - 17(399 - 42) + 5(42 - 36)$

$= 17(300) - 17(357) + 5(6)$

$= 5100 - 6069 + 30$

$= 5130 - 6069$

$= -939 \bmod 26 = 23$

How will get 23?

To convert negative to positive

$$n = q * m + r$$

where n = (-ve)value, q = Quotient, m = modulus and
r = remainder

$$-939 = q * 26 + r$$

$$-939 = -37 * 26 + r$$

(**selected q value multiplies with m the value must be < n**)

$$-939 = -962 + r \quad \mathbf{(-962 < -939)}$$

$$-939 + 962 = r$$

$$23 = r$$

Multiplicative Inverse

$$K^{-1} = \left[\frac{1}{\det K} * \mathrm{Adj}\,(K)\right] \bmod 26$$

$$K^{-1} = \left[23^{-1} * \mathrm{Adj}\,(K)\right] \bmod 26$$

- **Find the multiplicative inverse of 23?**
- Just try all 26 possibilities for n :

$$23 * n \bmod 26 = 1$$

(we can also do with Euclidean distance, see in further session)

$$23 * 17 \bmod 26 = 1$$

$$391 \bmod 26 = 1$$

Adjoint of K

$$K^{-1} = \left[\frac{1}{\det K} * \text{Adj}(K)\right] \bmod 26$$

cofactors

$$K^{-1} = \frac{1}{\det K} \underbrace{\begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix}}_{\text{Usually called the adjoint of } K} \begin{array}{l} \rightarrow \text{Row 1} \\ \rightarrow \text{Row 2} \\ \rightarrow \text{Row 3} \end{array}$$

Cofactor

The cofactor of the (i,j)-entry of a matrix **K**, denoted by C_{ij}, is defined as $(-1)^{i+j}\,K_{ij}$, where **K** is the determinant of the sub-matrix obtained by removing the i-th row and the j-th column.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \quad \text{mod } 26$$

Row 1 = **(18 * 19 – 21 * 2) = 300**

(21 * 19 – 2 * 21) = 357

(21 * 2 – 18 * 2) = 6

Row 2 = (17 * 19 – 2 * 5) = 313

(17 * 19 – 2 * 5) = 313

(17 * 2 – 2 * 17) = 0

Row 3 = (17 * 21 – 5 * 18) = 267

(17 * 21 – 21 * 5) = 252

(17 * 18 – 21 * 17) = -51

Substitution

- **Substitute Rows values in the following matrices:**

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

$$\begin{bmatrix} 300 & -357 & 6 \\ -313 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix}$$

Transpose

Transpose change columns of matrix in to rows.

$$\begin{bmatrix} 300 & -357 & 6 \\ -313 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix} = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix}$$

Remove –negative values from above matrix by using:

$$n = q * m + r$$

$$\begin{bmatrix} 300 & 25 & 267 \\ 7 & 313 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

Inverse of K

$$K^{-1} = \left[\frac{1}{\det K} * \text{Adj}(K) \right] \bmod 26$$

$$K^{-1} = 17 * \begin{bmatrix} 300 & 25 & 267 \\ 7 & 313 & 8 \\ 6 & 0 & 1 \end{bmatrix} \bmod 26$$

$$K^{-1} = \begin{bmatrix} 5100 & 425 & 4539 \\ 119 & 5321 & 136 \\ 102 & 0 & 17 \end{bmatrix} \bmod 26$$

Inverse of K

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

The inverse K^{-1} of a matrix K **is defined by the equation**

$$K * K^{-1} = K^{-1} * K = I$$

Multiply K and inverse of K ?

I is a matrix that is all zeros except for ones along the main diagonal from upper left to lower right.

Hill Cipher Decryption

$$P = D_K(C) = K^{-1} C \bmod 26$$

Try ?

Example

- Plain text: "LOVE", Secret Key: $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$
- "LO" → $\begin{bmatrix} 20 & 3 \\ 51 & 7 \end{bmatrix} \begin{bmatrix} 11 \\ 14 \end{bmatrix} = \begin{bmatrix} 262 \\ 263 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \mod 26$
- "VE" → $\begin{bmatrix} 20 & 3 \\ 51 & 7 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix} = \begin{bmatrix} 432 \\ 343 \end{bmatrix} = \begin{bmatrix} 16 \\ 5 \end{bmatrix} \mod 26$
- 2, 3, 16, 5 are transformed to cipher text "CDQF"

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

How to decode?

- Given "CDQF", and the Secret key is $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$

- How do we decrypt?
  - We need to compute the inverse of $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$

- Remind that all arithmetic are mod 26.

Determinant

- The determinant of $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$ equals 20(7)-3(15), which is 17 mod 26.
- Find the multiplicative inverse of 17 mod 26, i.e., find integer n such that 17 * n mod 26 =1

  (17* n = 1 mod 26)
- Just try all 26 possibilities for n :

17×1 = 17 mod 26	17×8 = 6 mod 26	17×15 = 21 mod 26	17×22 = 10 mod 26
17×2= 8 mod 26	17×9= 23 mod 26	17×16= 12 mod 26	17×23= 1 mod 26
17×3 = 25 mod 26	17×10 = 14 mod 26	17×17 = 3 mod 26	17×24 = 18 mod 26
17×4 = 16 mod 26	17×11 = 5 mod 26	17×18 = 20 mod 26	17×25 = 9 mod 26
17×5 = 7 mod 26	17×12 = 22 mod 26	17×19 = 11 mod 26	17×0 = 0 mod 26
17×6 = 24 mod 26	17×13 = 13 mod 26	17×20 = 2 mod 26	
17×7 = 15 mod 26	17×14 = 4 mod 26	17×21 = 19 mod 26	

Computing the inverse mod 26

- From $17 \times 23 = 1 \bmod 26$, we know that the multiplicative inverse of 17 mod 26 is 23.
- Using the formula for 2×2 matrix inverse

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

we get

Replace $(17)^{-1}$ mod 26 by 23

$$\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}^{-1} = (17)^{-1} \begin{bmatrix} 7 & -3 \\ -15 & 20 \end{bmatrix} = 23 \begin{bmatrix} 7 & 23 \\ 11 & 20 \end{bmatrix} = \begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix} \bmod 26$$

Decryption

- Given the ciphertext "CDQF", we decrypt by multiplying by

$$\begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 37 \\ 92 \end{bmatrix} = \begin{bmatrix} 11 \\ 14 \end{bmatrix} \mod 26$$

$$\begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix} \begin{bmatrix} 16 \\ 5 \end{bmatrix} = \begin{bmatrix} 125 \\ 394 \end{bmatrix} = \begin{bmatrix} 21 \\ 4 \end{bmatrix} \mod 26$$

- 11, 14, 21, 4 = "LOVE".

Examples

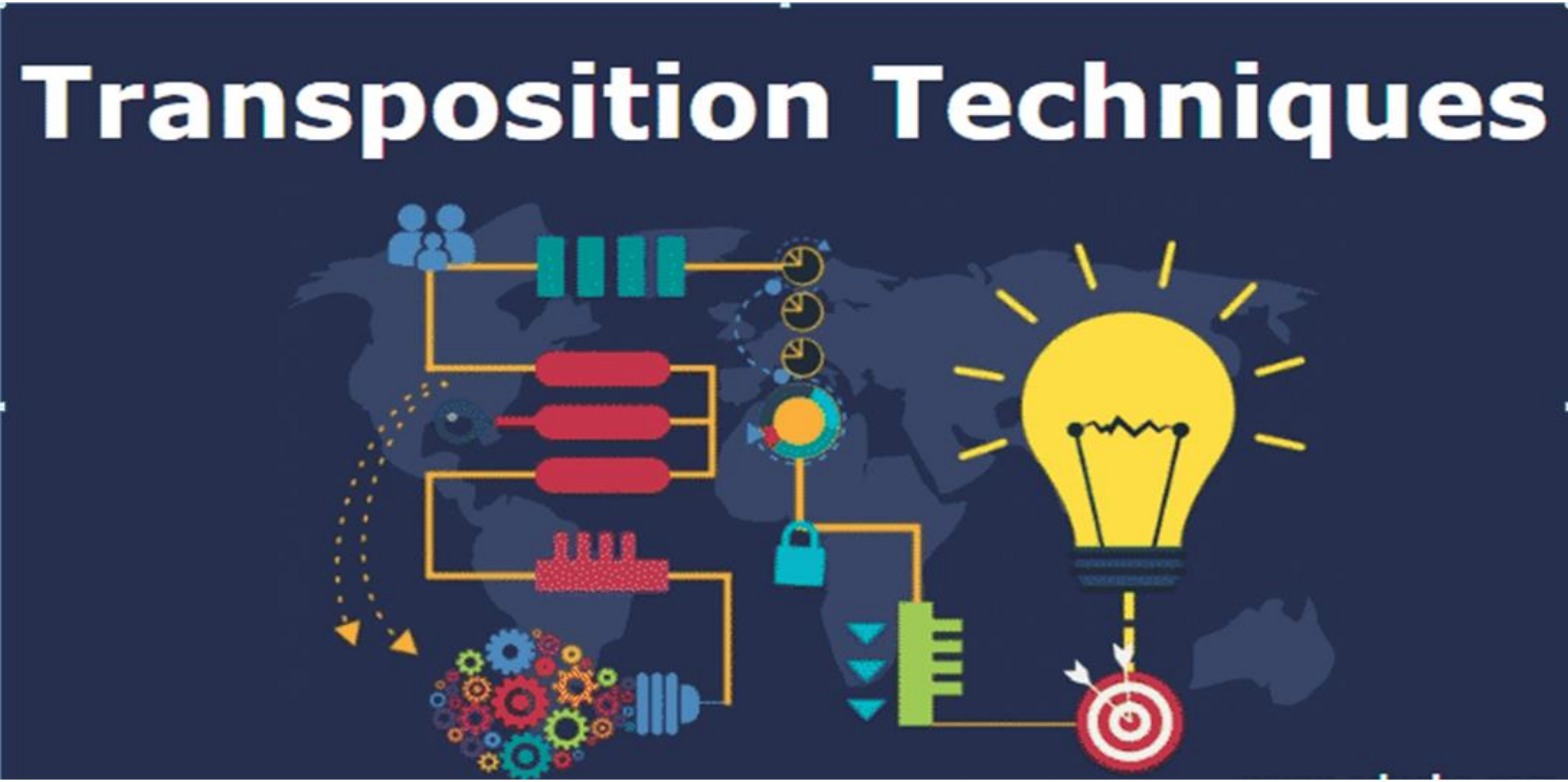
- Secret key = DDCE
- Plaintext = friday
- Ciphertext = ?

- Secret key = VIEW
- Plaintext = attack
- Ciphertext = ?

Disadvantages

Hill cipher is harder to crack than Playfair cipher?

- Both hill cipher and Playfair cipher are less vulnerable to frequency analysis.
- But hill cipher is quite vulnerable and less secure than **Playfair cipher**.
- A main drawback of this algorithm is that it encrypts identical plaintext blocks to identical **ciphertext** blocks.


Transposition Techniques

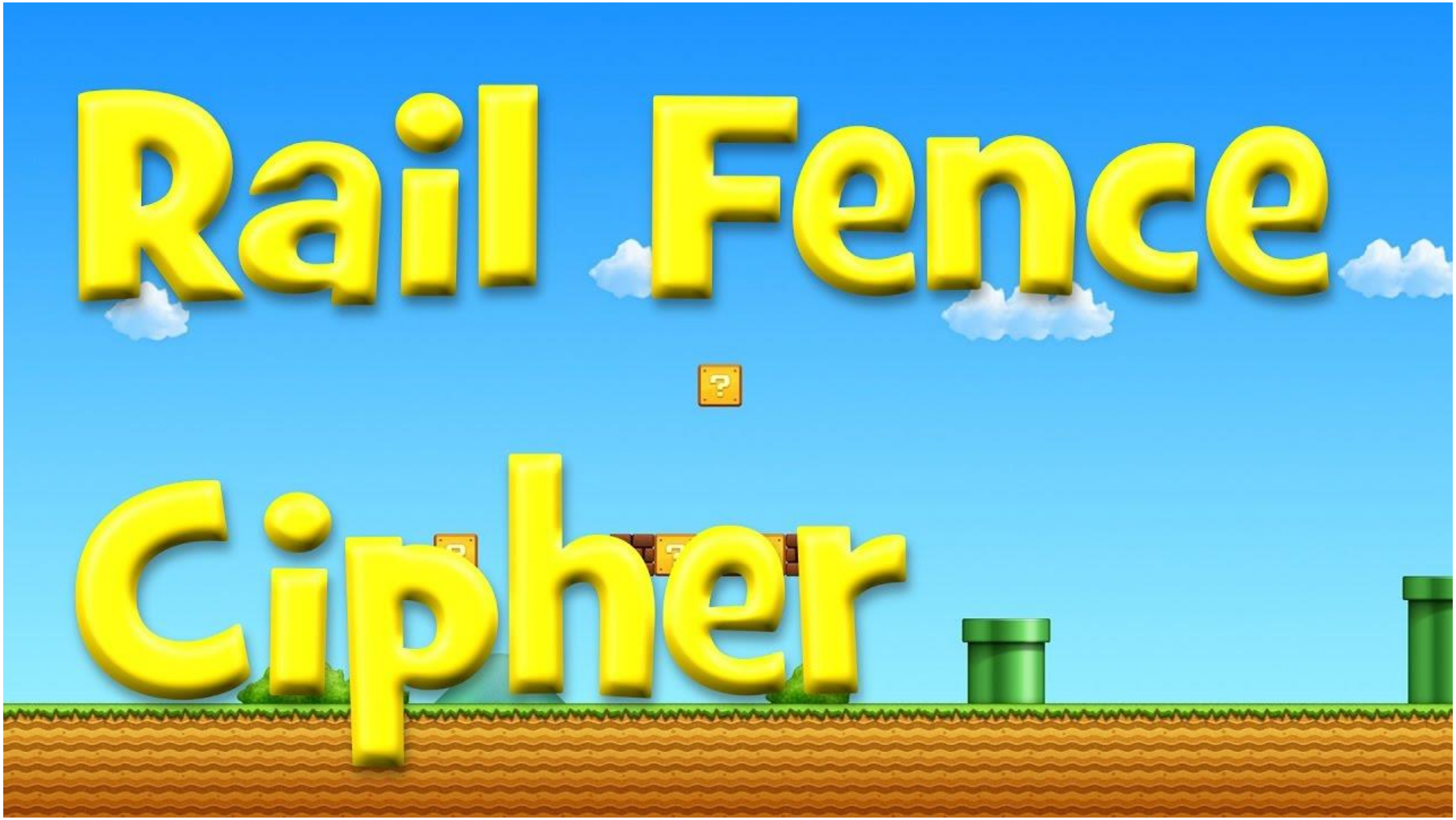
Transposition Techniques

- A transposition or permutation cipher is one in which the order is changed to obscure the message.
- Re-arrange the order/positions of the alphabets without altering their values.

Types of Transposition Techniques

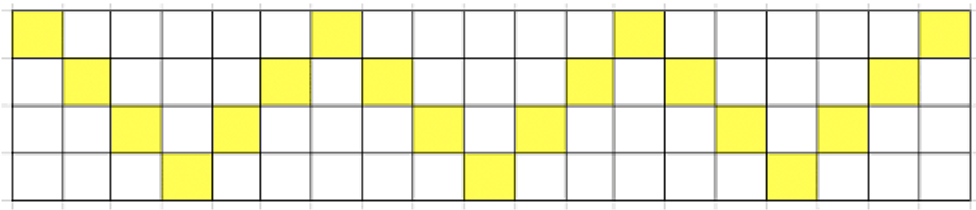
Rail Fence

Columnar Transposition


Rail Fence
Cipher

Rail fence

- Plaintext is written down as a sequence of diagonals in a zigzag pattern.



- Read off as a sequence of rows.
- Ciphertext is based on rail fence of depth.
- The security of the cipher can be improved by choosing rail fence depth more than 2.

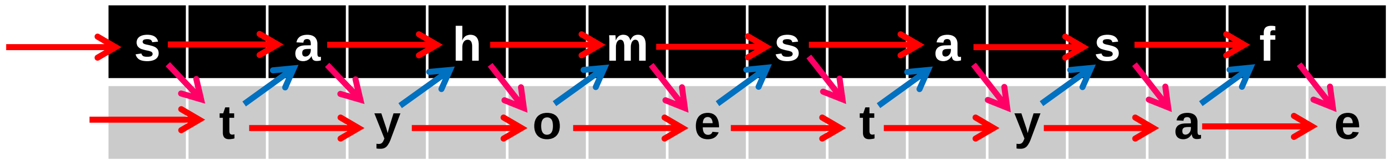
Rail fence

Example:

Plaintext : stay home stay safe

Depth : 2

Ciphertext : SAHMSASFTYOETYAE



Rail Fence Encryption

The security of the cipher can be improved by choosing rail fence depth more than 2.

Plaintext : **This is a secret message**

Rail fence Depth : **4**

Ciphertext : **?**

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

Rail Fence Encoding

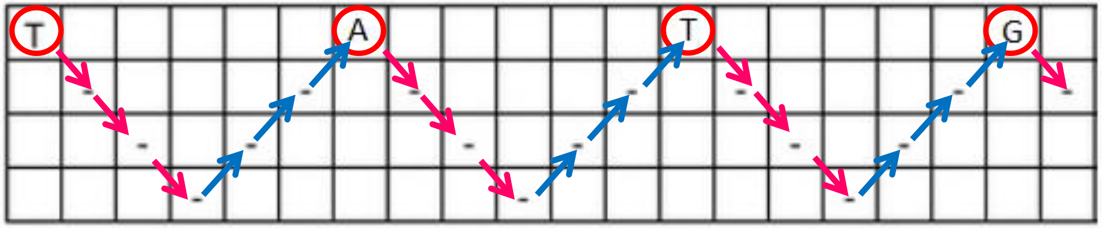
key = 4

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

Rail Fence Decryption

- Cipher Text: **TATGHSSEMAEIIERESSCS**
- Retrieve Plaintext row by row.
- Start by placing the "first character" of ciphertext in the first square.
- Then dash the diagonal down spaces until you get back to the top row.
- Continuing to fill the top row you get the pattern below.

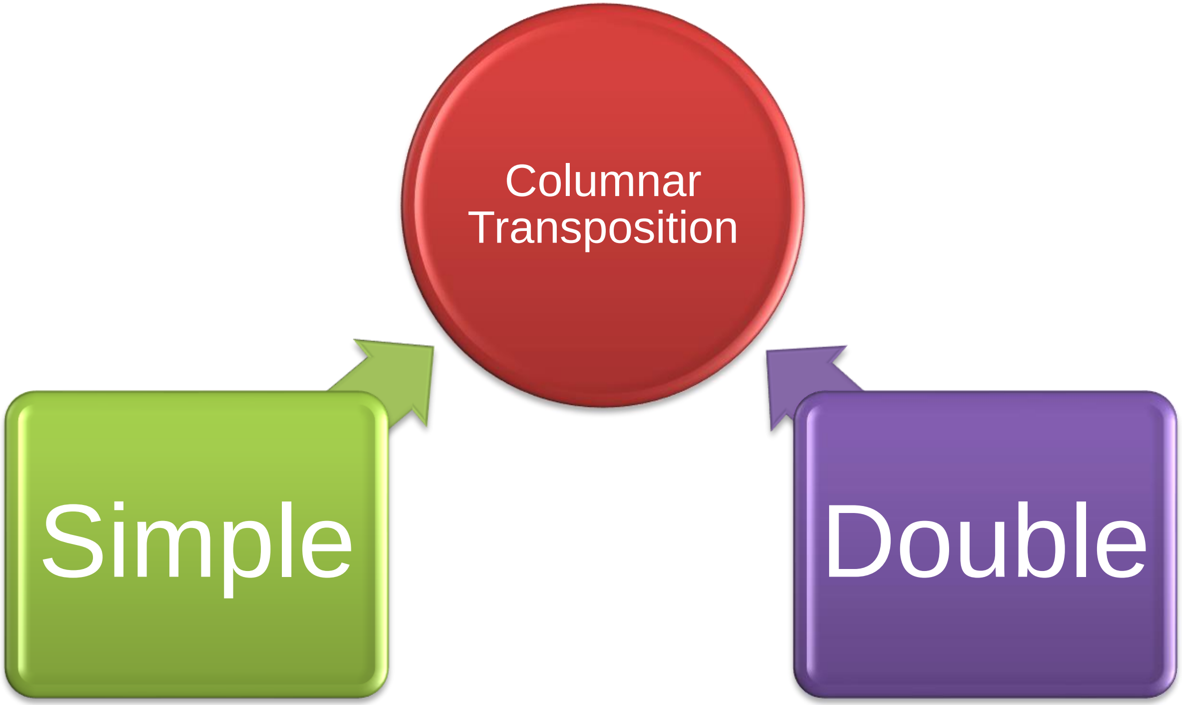


Examples

- Plaintext : cns exam is on tenth
- Depth : 2 / 4
- Ciphertext : ?

- Plaintext : ?
- Depth : 2 / 4
- Ciphertext : MEMATRHTGPRYETEFETEOAAT

Columnar Transposition



Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

Simple Columnar Transposition

- In this method the message is written in **rows** of fixed length and then read out column by column.
- **Column** are selected in some scrambled order.
- The number of columns are defined by the **length of key.**
- **STEPS:**

1. Write the plaintext message **row by row** in a rectangle of predefined size.(**length of key**)
2. Read the message **column by column** according to the selected order thus obtained message is a ciphertext.

Simple Columnar Encryption

Example:

Plaintext : meet me later

Key : 4312

Ciphertext : ELRTAXEEEMMT

KEY	4	3	1	2
	M	E	E	T
	M	E	L	A
	T	E	R	X

Simple Columnar Decryption

- **STEPS:**

1. Write the ciphertext **column by column** in a rectangle of predefined size.(**based on order of key**)
2. Read the message **row by row** according to the selected order thus obtained message is a plaintext.

Example:

Ciphertext : **ELRTAXEEEMMT**

Key : **4312**

Plaintext : **meet me later**

KEY	4	3	1	2
	M	E	E	T
	M	E	L	A
	T	E	R	X

Double Columnar Transposition

- Single columnar transposition can be attack by guessing possible column lengths.
- Therefore to make it stronger double transposition is used.
- This is simple columnar transposition technique applied twice.
- Here same key can be used for transposition or two different keys can be used.

Double Columnar Encryption

Example:

Plaintext : **meet me later**

Key : **4312**

Ciphertext Single : **ELRTAXEEEMMT**

Ciphertext Double : **REMTETLXMEAE**

KEY	4	3	1	2
	M	E	E	T
	M	E	L	A
	T	E	R	X

4	3	1	2
E	L	R	T
A	X	E	E
E	M	M	T

Double Columnar Encryption

Example:

Plaintext : ?

Key : 4312

Ciphertext Single : ELRTAXEEEMMT

Ciphertext Double : REMTETLXMEAE

Try?

Examples

- Plaintext : cns exam is on twenty first
- Key : 4312567
- Ciphertext : ?

- Plaintext : ?
- Key (single) : 4312567
- Ciphertext : NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

known/chosen plaintext attack

The alphabet values do not change

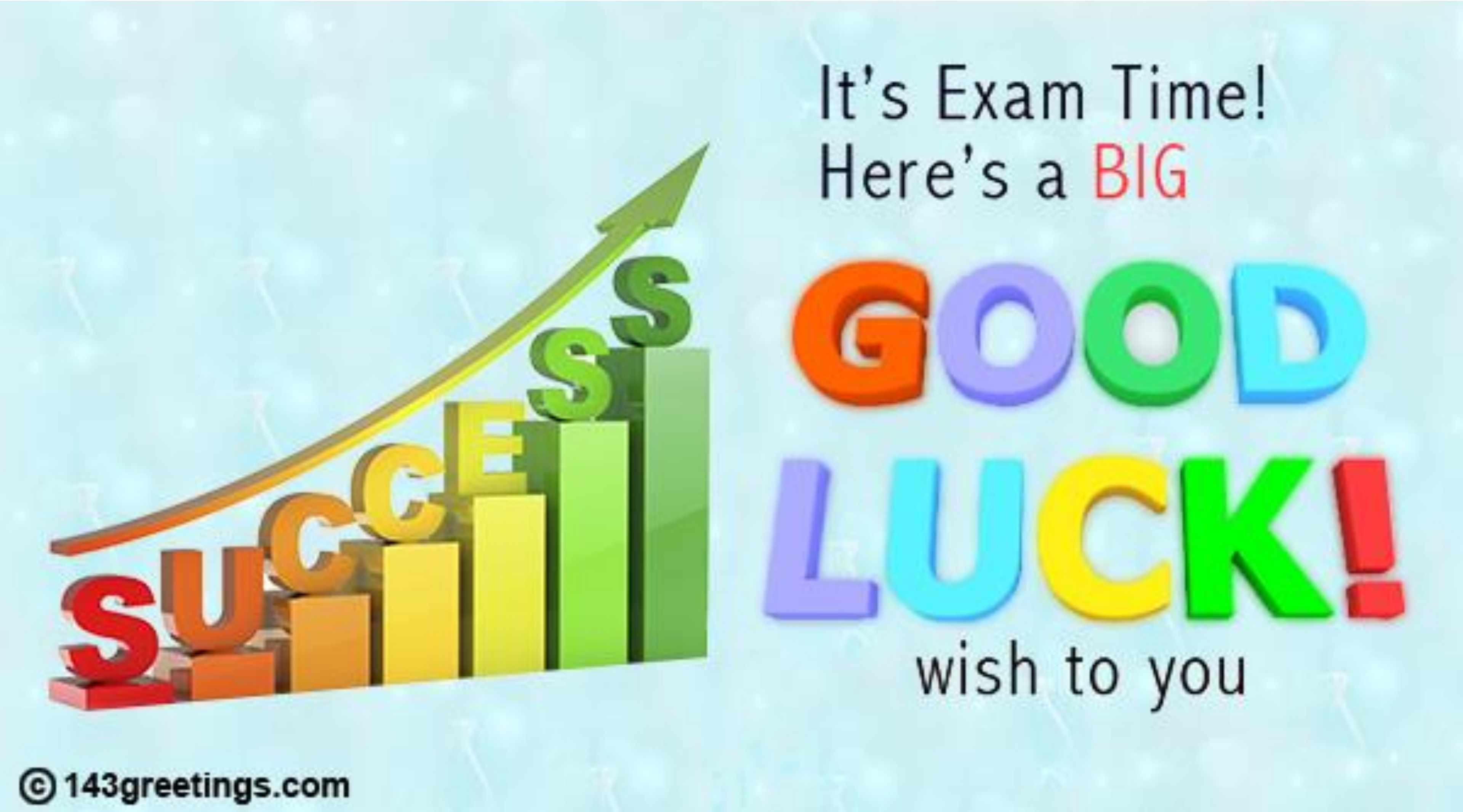
- The frequency distribution is the same Vulnerable to cryptanalysis.
- The attack performed on ciphertext by **known/chosen plaintext attack.**

Improve security

- Combinations of substitution ciphers and transposition ciphers in succession.
- This combination called **Product cipher.**

Questions?

- The plaintext MEETMELATER gets processed by a Permutation Cipher or transposition cipher (with a key of [2 3 5 4 1] and no padding with extra letters. What is the corresponding ciphertext?
- The plaintext MEETMELATER gets processed by a Permutation Cipher (with a key of [2 3 5 4 1] and with padding using the letter "**x**" (Alice and Bob agree to use the letter z for padding). What is the corresponding ciphertext?
- The plaintext MEETMELATER gets processed by a product cipher, comprised of Caesar Cipher (with a key of 23) and Permutation Cipher (with a key of [5 3 1 4 2] and no padding with extra letters). What is the corresponding ciphertext?


SUCCESS
It's Exam Time!
Here's a BIG
GOOD
LUCK!
wish to you
© 143greetings.com