SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

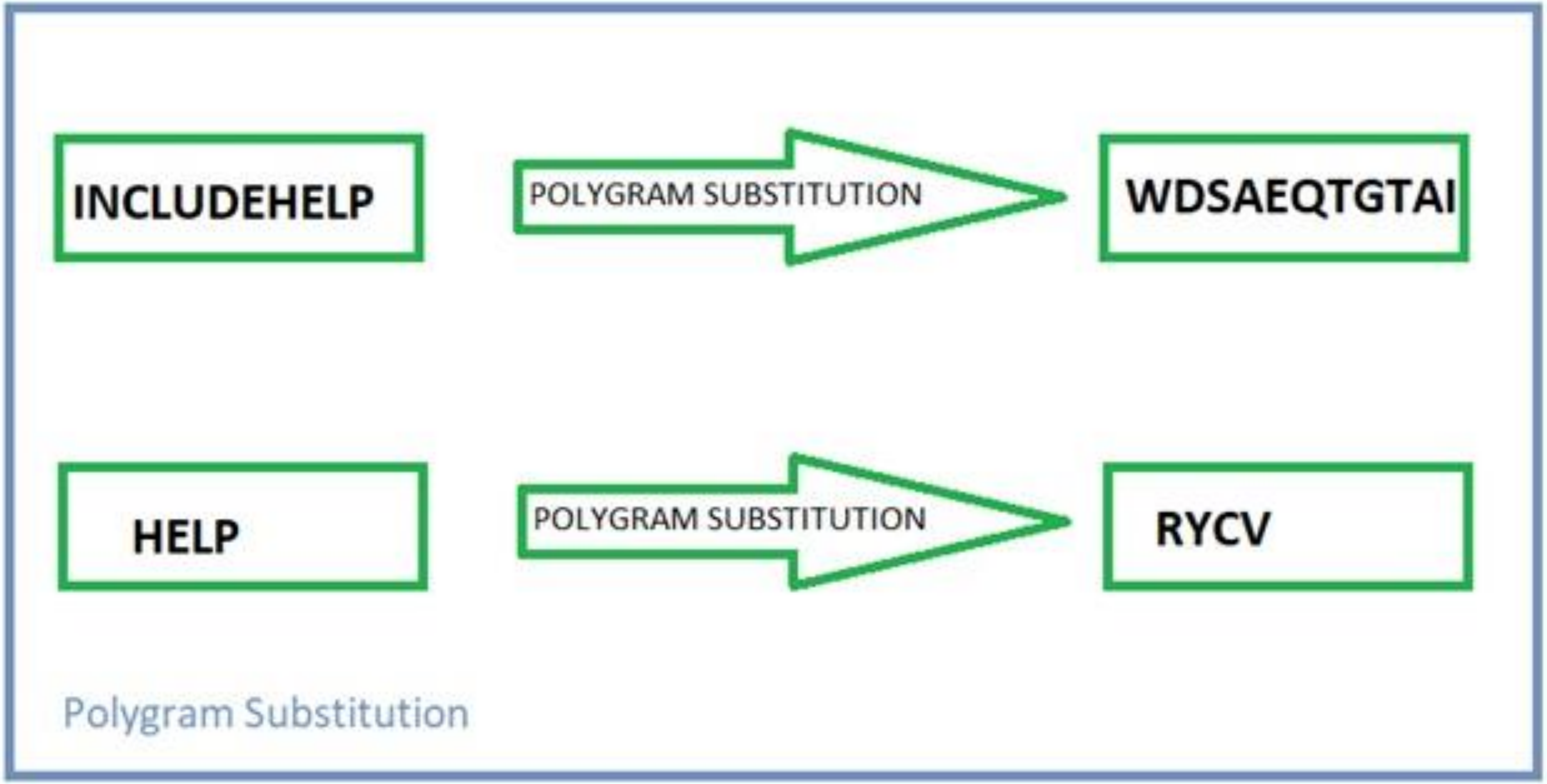
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME :19CS503-Cryptography and Network Security

III YEAR /V SEMESTER

Unit 1- Introduction

Topic : Classical encryptions techniques: substitution techniques



INCLUDEHELP → POLYGRAM SUBSTITUTION → WDSAEQTGTAI

HELP → POLYGRAM SUBSTITUTION → RYCV

Polygram Substitution

Recap

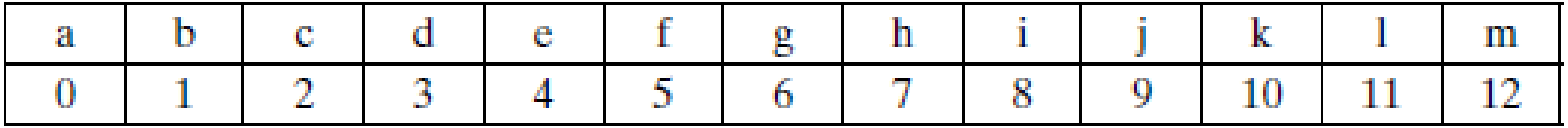
- □ Model for Network Security
- □ Network Access Security Model
- □ Simplified Model of Symmetric Encryption
- □ Terms in Cryptography
- □ Types of Attacks on Encrypted Messages

Substitution Techniques

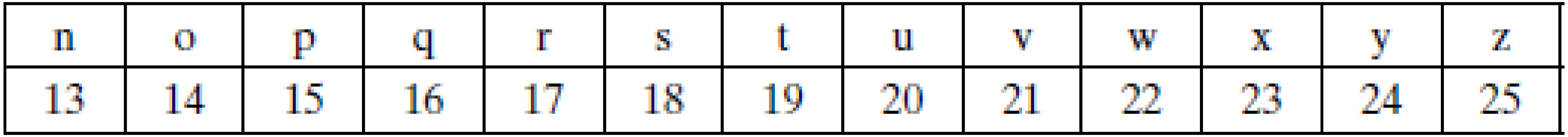
- A substitution technique is one in which the letters of plaintext are **replaced by other letters or by numbers or symbols.**
  - Caesar Cipher
  - Monoalphabetic Ciphers
  - Playfair Cipher
  - Hill Cipher
  - Polyalphabetic Ciphers
  - One-Time Pad

Caesar Cipher

- □ Earliest known substitution cipher by Julius Caesar
- □ First attested use in military affairs replaces each letter by 3rd letter



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

plain: meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB

Mathematical Relations

□ **Caesar cipher as:**

c = E(k, p) = (p + k) mod (26)

p = D(k, c) = (c – k) mod (26)

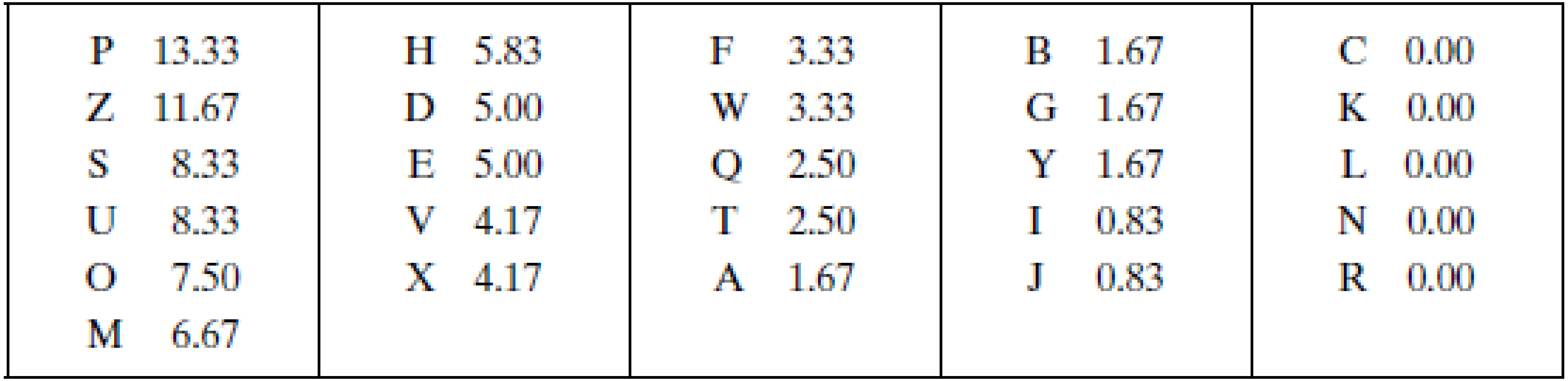
□ **Brute force Cryptanalysis**

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

Monoalphabetic Ciphers

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

Monoalphabetic Ciphers



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

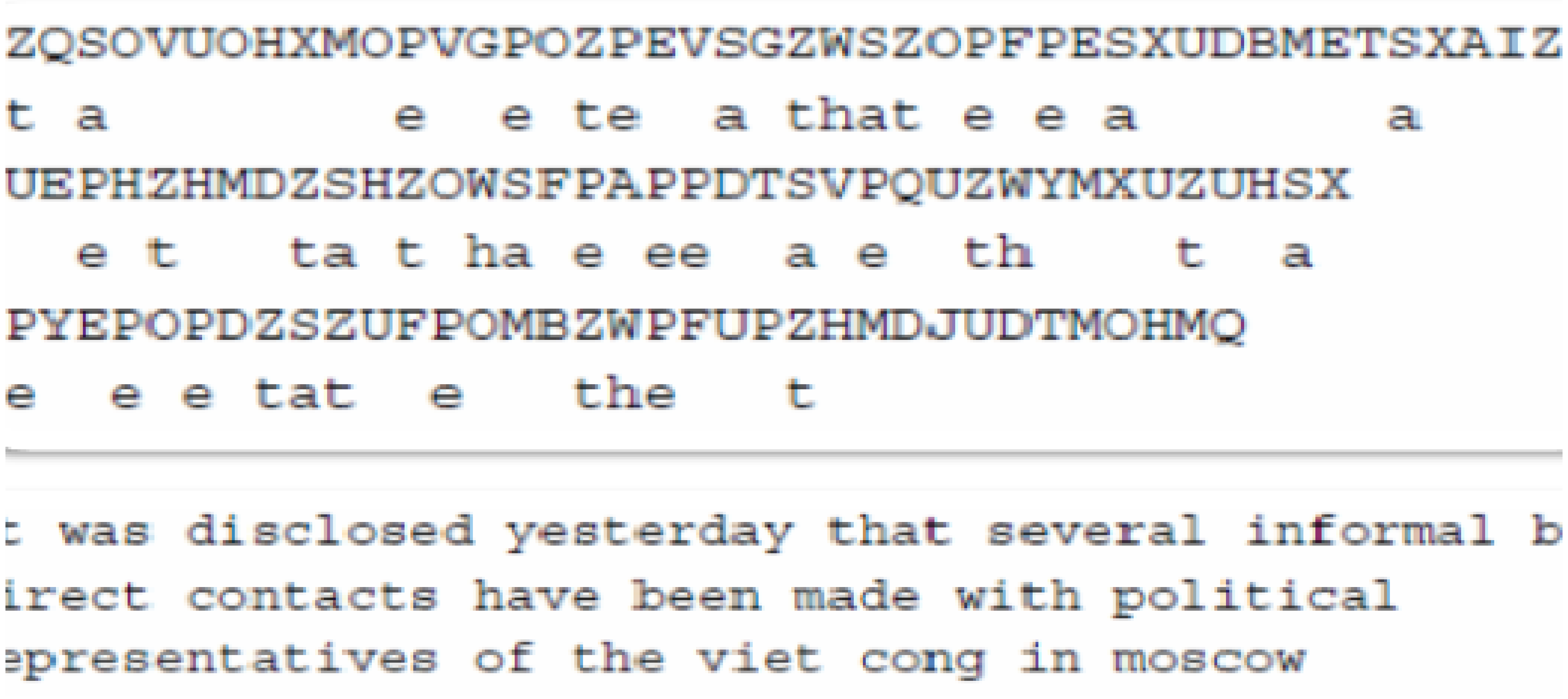
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Monoalphabetic Ciphers

Cipher Text	Equivalent
P Z	E T
S, U, O, M, and H	a, h, i, n, o, r, s
A, B, G, Y, I, J	b, j, k, q, v, x, z

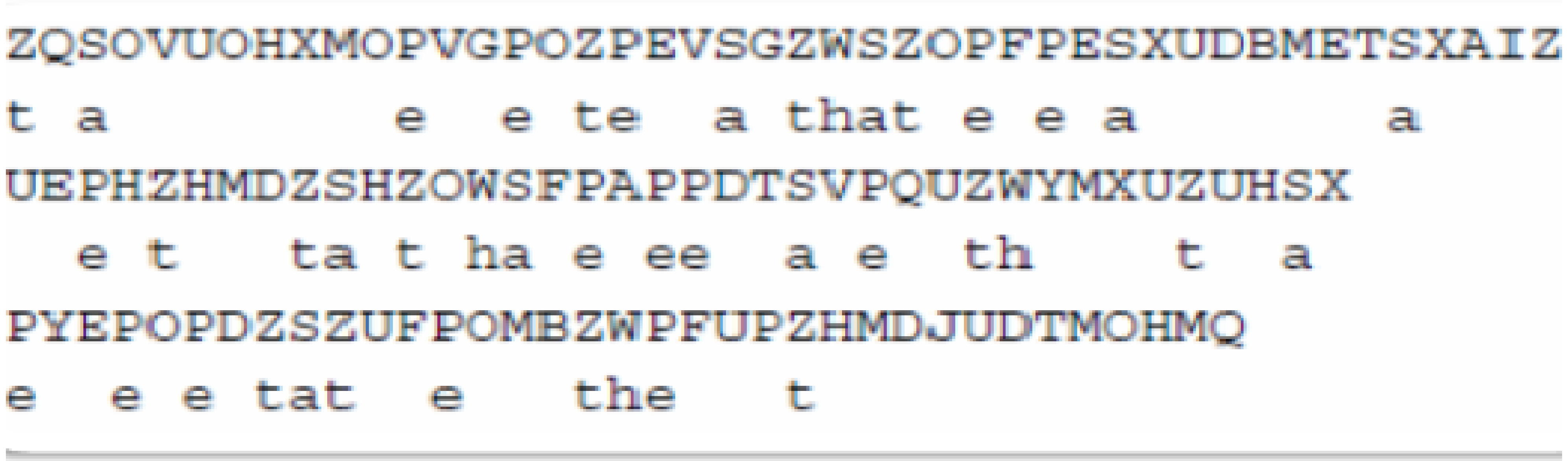


```
ZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
t a        e  e te  a that e e a       a
UEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  e t   ta t ha e ee   a e  th    t  a
PYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
e  e e tat  e   the   t
```

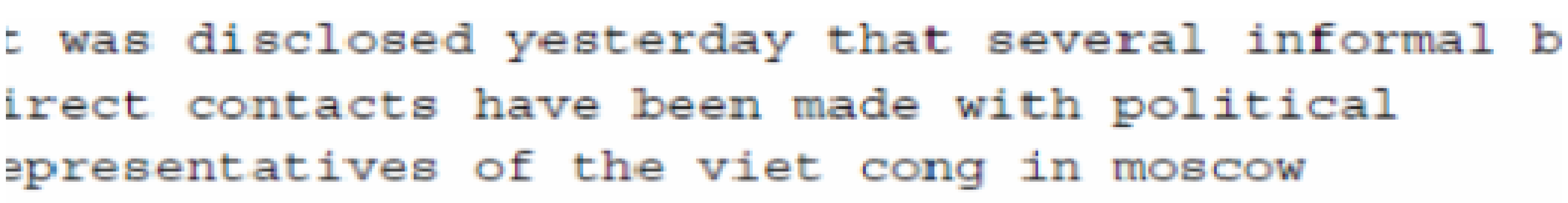
```
t was disclosed yesterday that several informal b
irect contacts have been made with political
epresentatives of the viet cong in moscow
```

Monoalphabetic Ciphers

Cipher Text	Equivalent
P Z	E T
S, U, O, M, and H	a, h, i, n, o, r, s
A, B, G, Y, I, J	b, j, k, q, v, x, z



```
ZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
t a        e  e te  a that e e a       a
UEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  e t   ta t ha e ee  a e  th    t  a
PYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
e  e e tat  e   the   t
```



```
t was disclosed yesterday that several informal b
irect contacts have been made with political
epresentatives of the viet cong in moscow
```

Activity

Playfair Cipher

□ Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- a 5X5 matrix with any Keyword
- Avoid duplicates

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

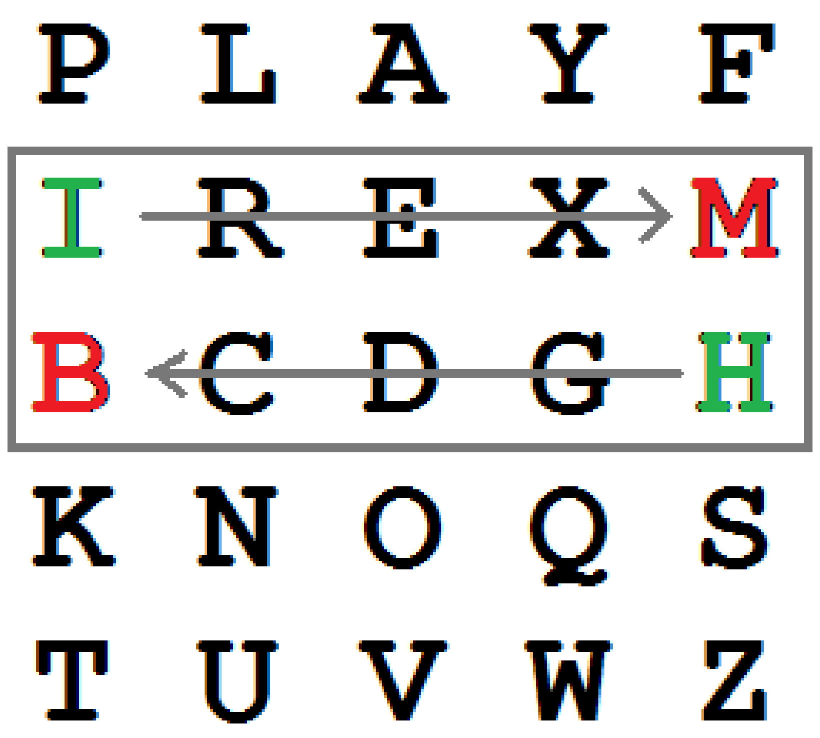
Rules

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

Examples

1. balloon - ba lx lo on
2. ar is encrypted as RM
3. mu is encrypted as 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

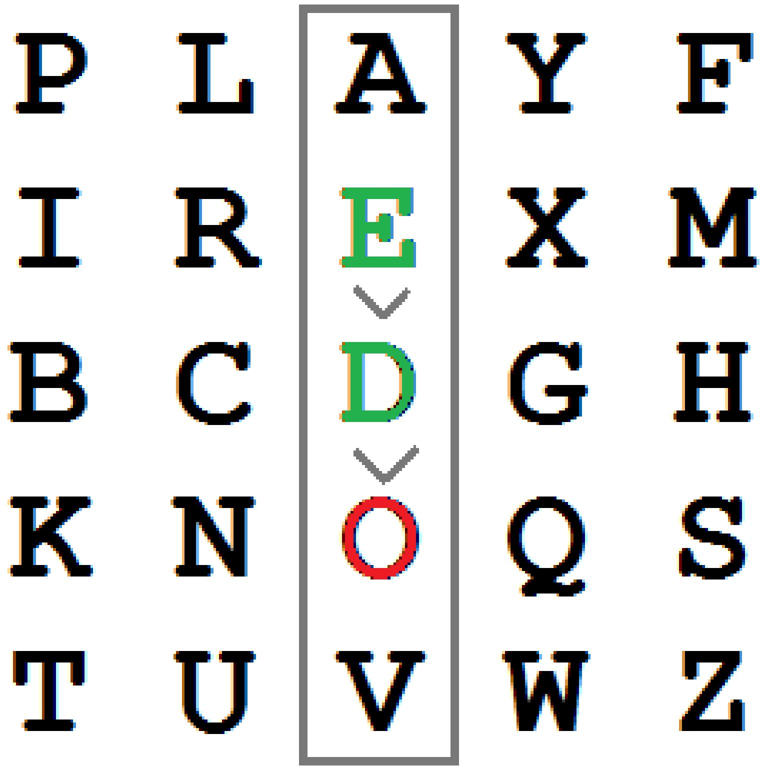


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

HI

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

BM

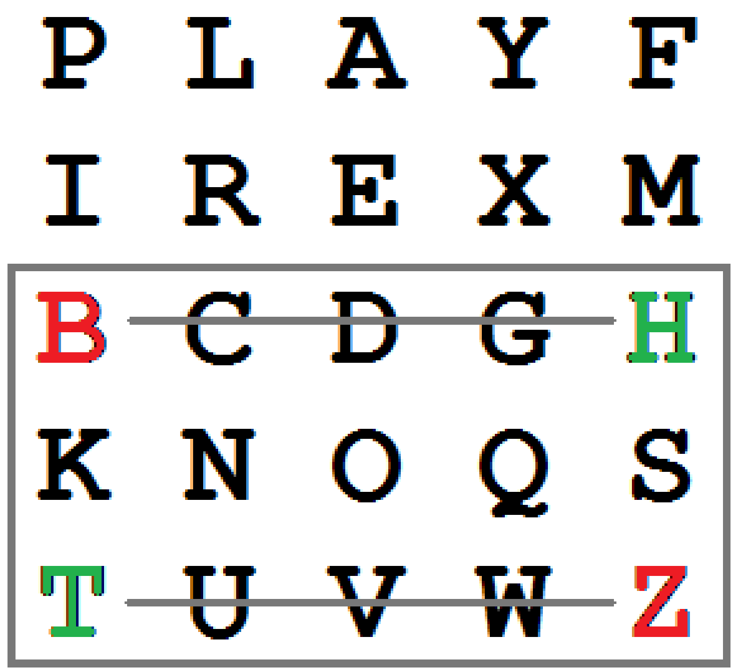


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

DE

Shape: Column
Rule: Pick Items Below Each
Letter, Wrap to Top if Needed

OD

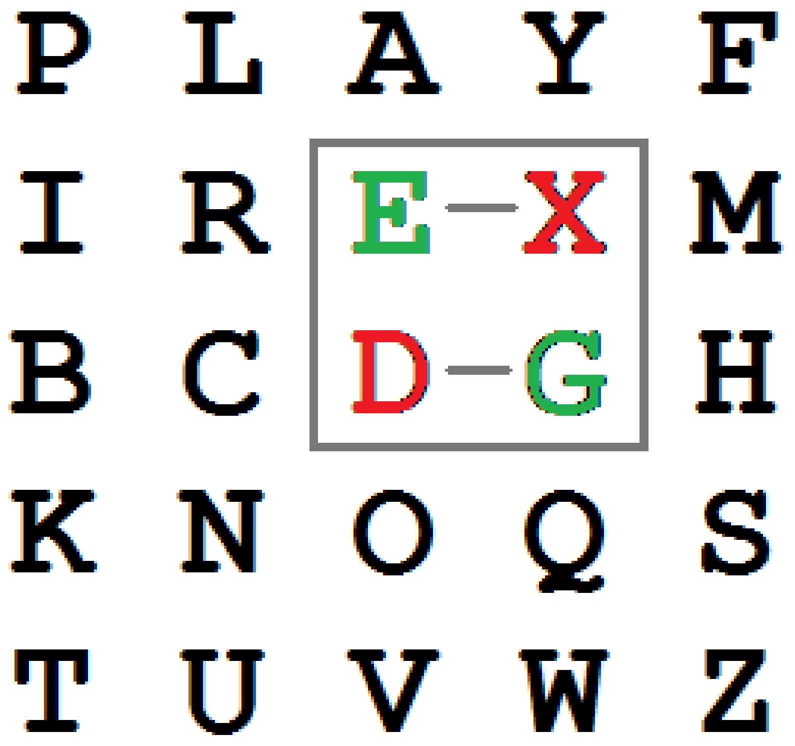


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

TH

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

ZB

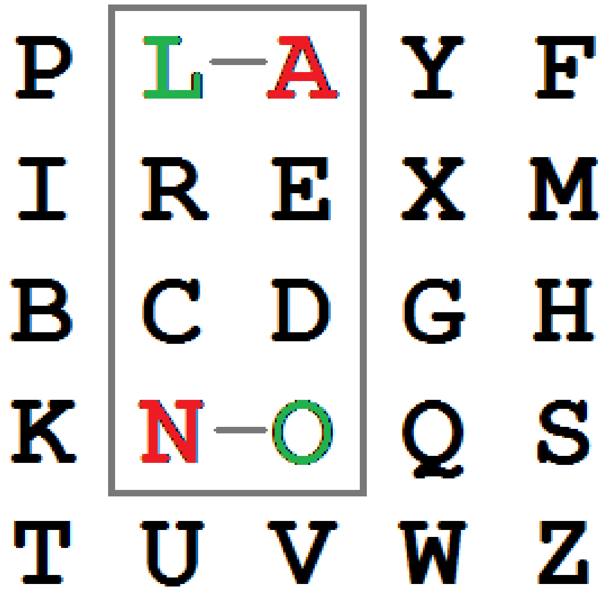


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

EG

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

XD

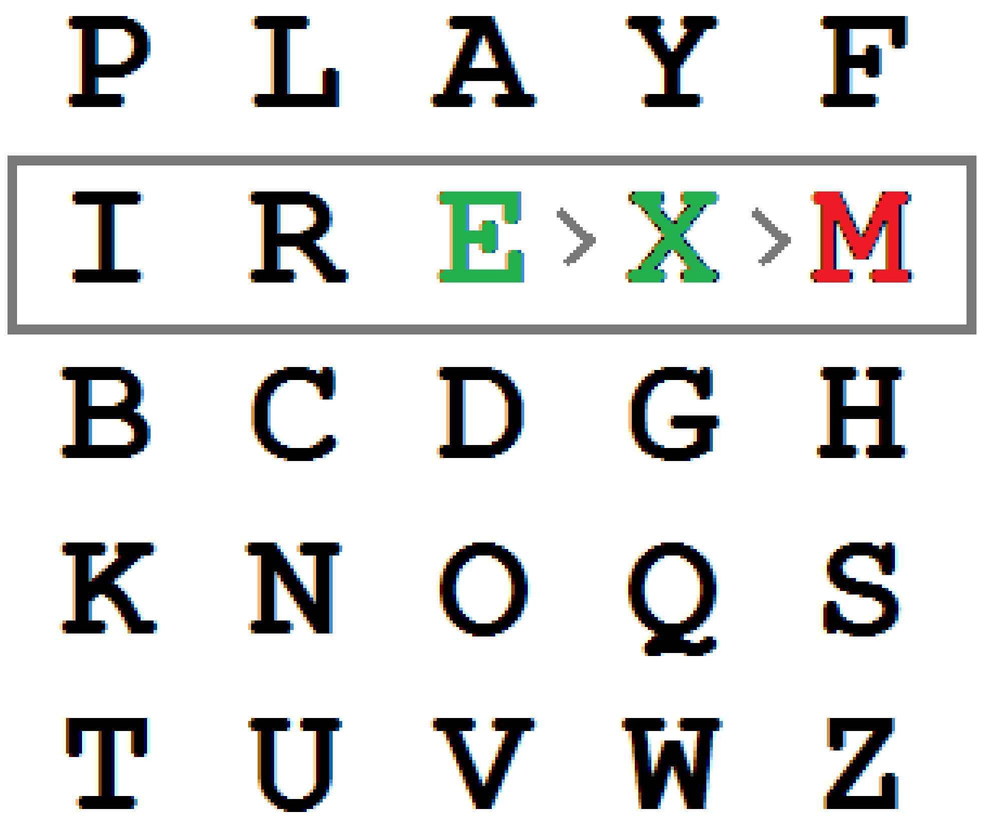


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

OL

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

NA



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

EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

Assessment 1

1. Caesar Cipher is an example of

a) Poly-alphabetic Cipher
b) Mono-alphabetic Cipher
c) Multi-alphabetic Cipher
d) Bi-alphabetic Cipher

2 Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

a) True
b) False

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.

THANK YOU