Unit 2

Classical Encryption Techniques

Presented by:
Dr. Mohammed Y.Alkhanafseh
Computer Science Department
Birzeit University

Definitions

Plaintext
- An original message

Ciphertext
- The coded message

Enciphering/encryption
- The process of converting from plaintext to ciphertext

Deciphering/decryption
- Restoring the plaintext from the ciphertext

Cryptography
- The area of study of the many schemes used for encryption

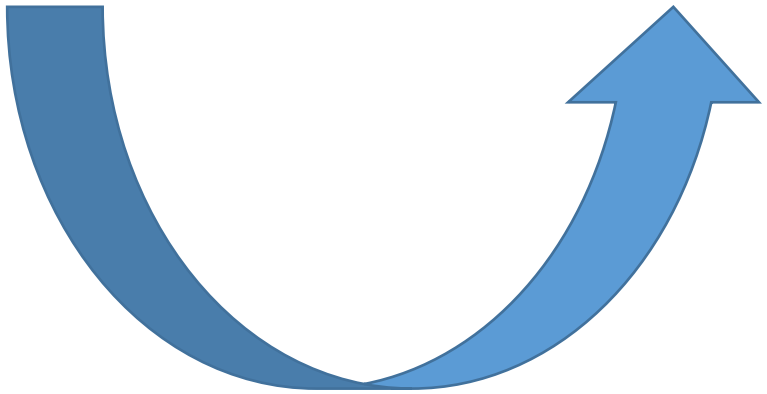
Cryptographic system/cipher
- A scheme

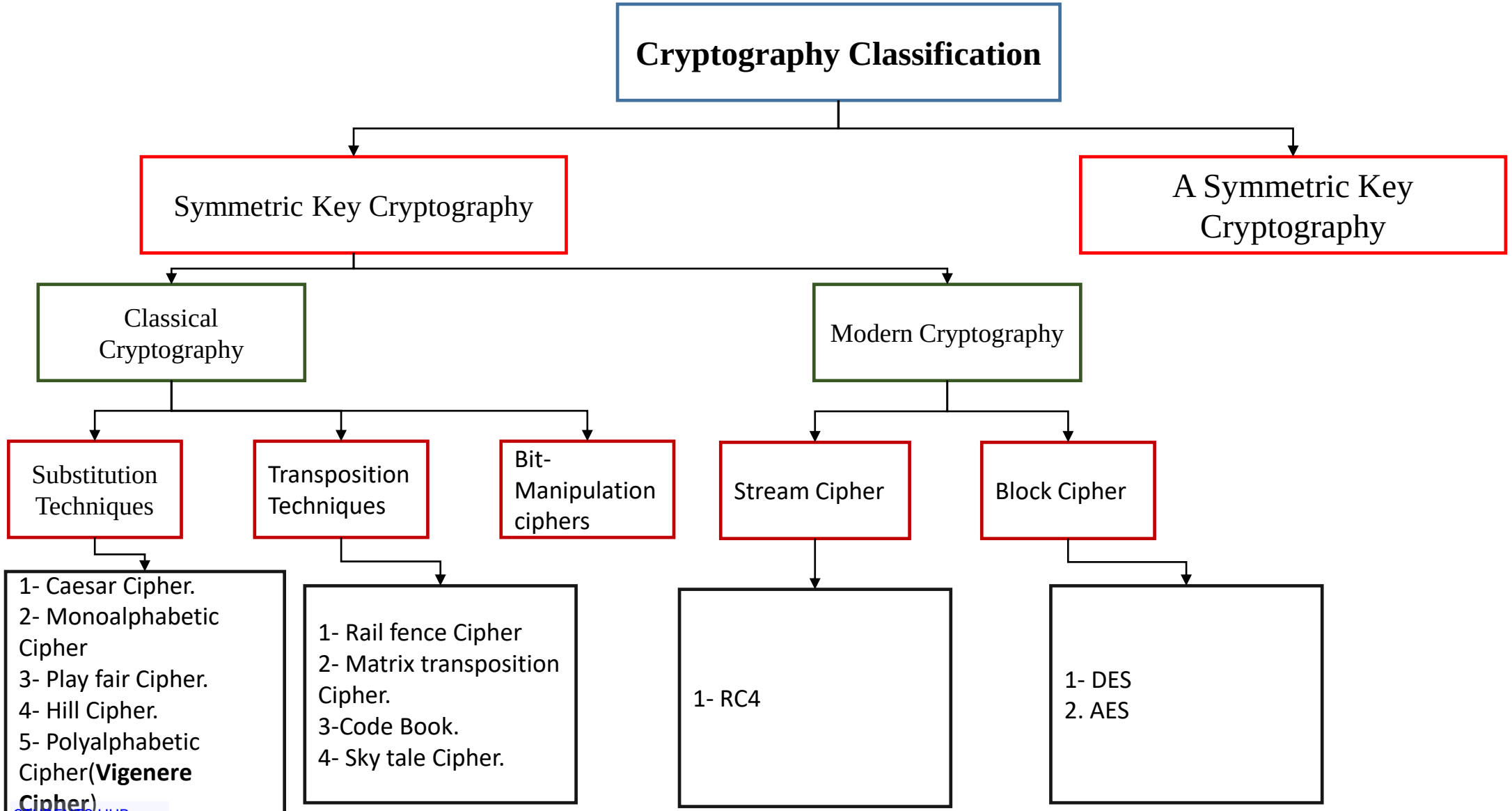
Cryptanalysis
- Techniques used for deciphering a message without any knowledge of the enciphering details

Cryptology
- The areas of cryptography and cryptanalysis

2.1 Cryptography Classification

Next >>>





Substitution Techniques:

1. Caesar Cipher.
2. Monoalphabetic Cipher
3. Play fair Cipher.
4. Hill Cipher.
5. Polyalphabetic Cipher (**Vigenere Cipher**)

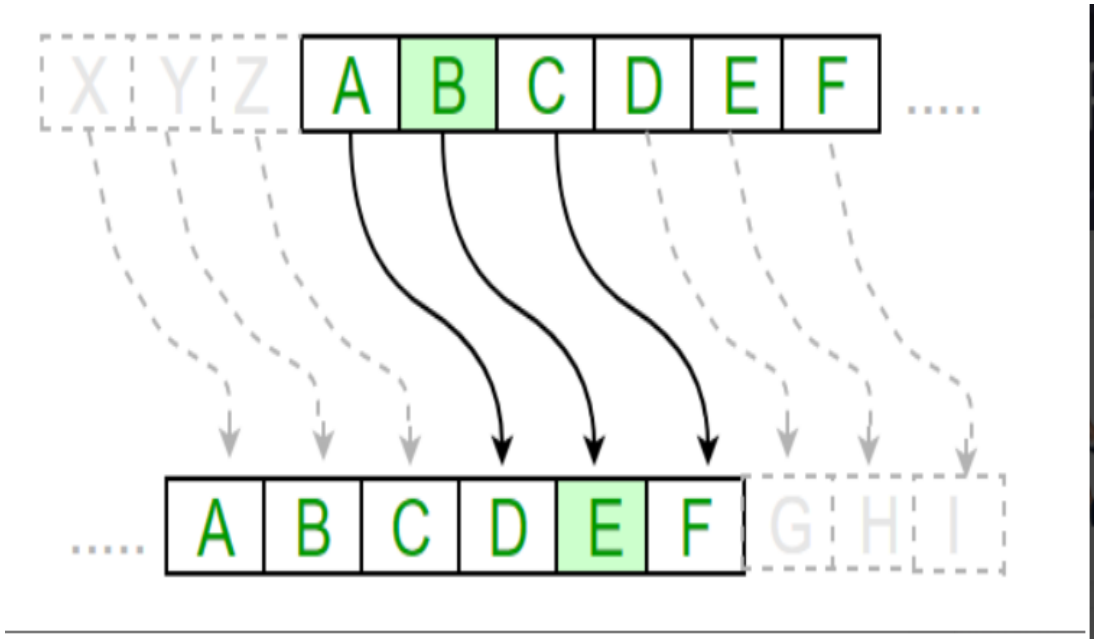
1. Caesar Cipher.

- Simplest and earliest known use of a substitution cipher
- Used by Julius Caesar
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A

plain text: meet me after the yoga party

Key :3 (1-26)

cipher: PHHW PH DIWHU WKH WRJD SDUWB



Strongest and weakness Points for Caesar Cipher Algorithm

Caesar cipher as any encryption algorithm, have a weak and strongest points. Strongest points for this algorithm as follows:

- **Ease of Implementation:** Simple to understand and implement.
- **Speed:** It's a fast encryption method, ideal for quick encoding and decoding.
- **Education:** Used as an introductory example for teaching encryption concepts.
- **Obscurity:** Effective against casual snooping or simple algorithms.

Weakness Points for Caesar Cipher as follows:

- **Security:** Easily broken using brute force (trying all possible shifts) due to its limited key space (only 25 possible shifts in the English alphabet).
- **Frequency Analysis:** Vulnerable to frequency analysis as it preserves the frequency distribution of letters in the plaintext.
- **Known Plaintext Attacks:** Susceptible if the attacker knows some plaintext-ciphertext pairs.
- **Lack of Key Management:** The key (shift) is often shared or predictable, making it less secure.

Suggest Solutions to Enhance the Security Level of Caesar Cipher

Different solutions can be applied to original Caesar cipher encryption algorithm to enhance the overall security level as follows:

- **Randomizing the shift for each character,** which refer to the process of select random number of shift for each character in the plain text content. This technique refers to Variant Caesar Cipher encryption or Random Shift Cipher.
  - **Proposed Randomizing shift for each character can enhance the complexity and make it more challenging for attacker to decipher the cipher text.**
  - **Proposed solution can reduce vulnerability for frequency analysis**, since the variability in shifts disrupts the frequency distribution, making frequency analysis less effective.
  - This solution to enhance the security for Caesar cipher have limitations regarding to key management, since Handling and managing the random shifts can be complex, especially for decryption without the proper key.
- Use the idea of block cipher in Caeser Cipher, whereas the shift will be for block of character not just for single character.

Caesar Cipher Algorithm

- Can define transformation 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

  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

- Mathematically give each letter a number

  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

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

- Algorithm can be expressed as:

  $c = E(3, p) = (p + 3) \bmod (26)$

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

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

- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

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

Figure 3.3

Brute-Force Cryptanalysis of Caesar Cipher

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

Exercise #1

Caesar Cipher.

Plain: Encryption Theory is very interesting and I hope get high score in this course
key 5, 8, 12

Cipher text: Mvkzgxbqwv Bpmwzg qa dmzg qvbmzmabqvo ivl Q pwxm omb pqop akwzm qv bpqa kwczam (key= 8)

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
				j			m	n					s					x	y						

2- Monoalphabetic Cipher

- The Monoalphabetic cipher is a basic substitution cipher where each letter in the plaintext is consistently replaced by a corresponding fixed letter in the ciphertext. This means that each occurrence of a particular letter in the plaintext will always be substituted by the same letter in the ciphertext.
- There are various types of Monoalphabetic ciphers, and the most common one is the Caesar cipher, which involves shifting each letter of the alphabet by a fixed number of positions. For instance, if you shift each letter in the alphabet by three positions, 'A' becomes 'D', 'B' becomes 'E', and so on.

Atbash Cipher as Another Example for Monoalphabetic

- It's a simple substitution cipher where each letter is replaced by its counterpart in the reverse of the alphabet. In other words, 'A' is replaced by 'Z', 'B' by 'Y', 'C' by 'X', and so on.
- Plain text: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- CipherText: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Advantages and Disadvantages

- **Advantages**
  - **Easy Implementation:** Simple to understand and implement, making it accessible for educational purposes and basic encryption.
  - **Encryption Speed:** Fast encryption and decryption processes due to the direct substitution of letters.
  - **Obscurity:** Initially difficult for novice attackers to decipher without knowledge of the substitution key.
  - **Teaching Tool:** Often used as an introductory example to demonstrate the concept of substitution ciphers in cryptography.
- **Disadvantages**
  - **Vulnerability to Frequency Analysis:** Retains the frequency distribution of letters from the plaintext, making it susceptible to frequency analysis. Common letters in the plaintext can be linked to common letters in the ciphertext.
  - **Known Plaintext Attacks:** Vulnerable if the attacker has access to or can predict portions of the plaintext and their corresponding ciphertext.
  - **Lack of Security:** Once the substitution pattern is identified, the entire message becomes easily decipherable.

Frequency Analysis

- Frequency analysis is a cryptanalysis technique used to break classical ciphers, especially those based on substitution, by analyzing the frequency of letters or symbols in a ciphertext.
- How Frequency analysis Work
  - **Frequency of Letters:** In any language, certain letters appear more frequently than others. For instance, in English, 'E' is the most used letter.
  - **Frequency Distribution:** By analyzing a large enough ciphertext, one can observe patterns in the frequency of letters. The most frequently occurring letters in the ciphertext likely correspond to the most common letters in the plaintext.
  - **Mapping to Language Statistics:** Cryptanalysts use statistical information about the language being used (such as letter frequency in English) to identify potential correspondences between ciphertext and plaintext letters.
  - **Guesswork and Testing:** Armed with the knowledge of common letters, the cryptanalyst makes educated guesses about potential letter substitutions in the ciphertext.
  - **Iterative Process:** As the cryptanalyst makes these educated guesses and substitutions, they start to build the partial decryption of the message. This partial decryption helps them make further deductions about other letters.
  - **Repetition and Confirmation:** The process continues iteratively, with repeated substitutions and confirmations, gradually revealing more of the plaintext.

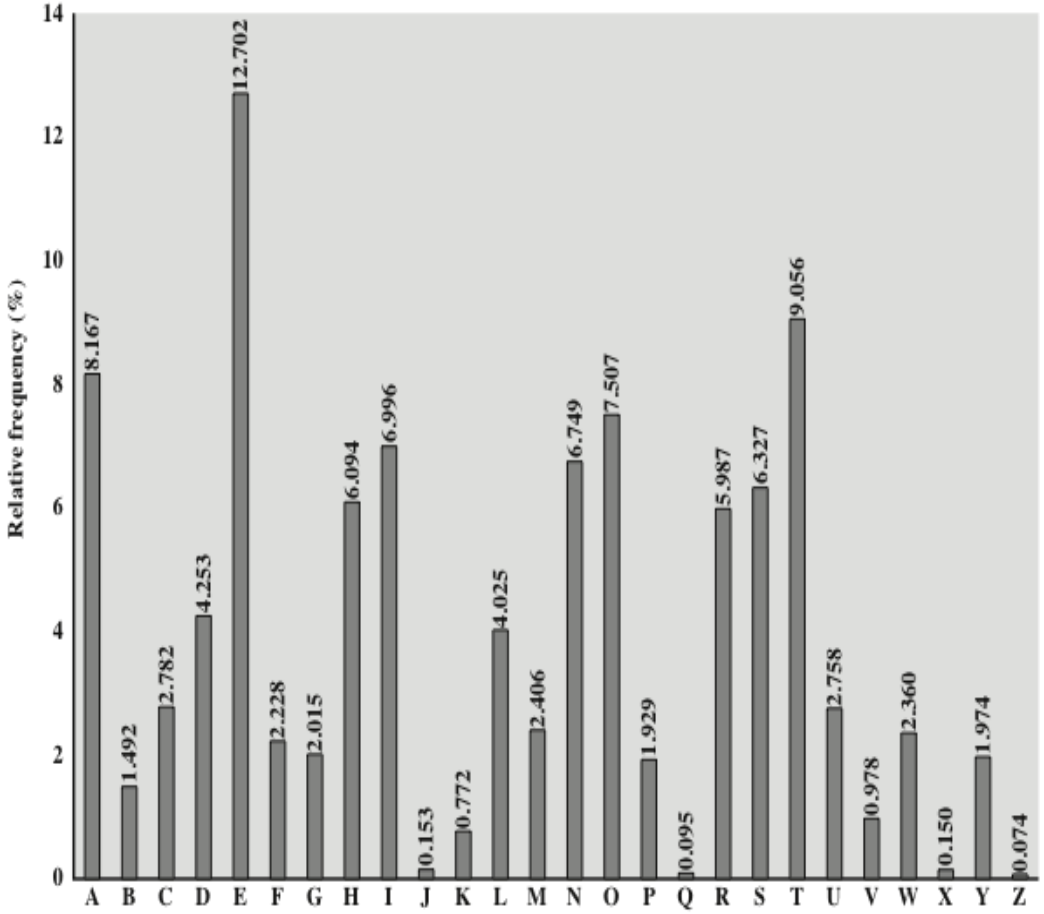


Figure 3.5 Relative Frequency of Letters in English Text

Letter	Count	Letter	Frequency
E	21912	E	12.02
T	16587	T	9.10
A	14810	A	8.12
O	14003	O	7.68
I	13318	I	7.31
N	12666	N	6.95
S	11450	S	6.28
R	10977	R	6.02
H	10795	H	5.92
D	7874	D	4.32
L	7253	L	3.98
U	5246	U	2.88
C	4943	C	2.71
M	4761	M	2.61
F	4200	F	2.30
Y	3853	Y	2.11
W	3819	W	2.09
G	3693	G	2.03
P	3316	P	1.82
B	2715	B	1.49
V	2019	V	1.11
K	1257	K	0.69
X	315	X	0.17
Q	205	Q	0.11

Frequency Analysis Example

- Lets take this cipher text: VWDQGDQW LQ SODB VXSHUHV
- First step refers to count the frequency of each character in the cipher text.
- V: 3, W: 2, D:3, Q:3, G:1, L:1, S:2, O:1, B:1, X:1, H:2, U:1
- Compare the frequency of letter in given cipher text with corresponding language letter frequency, such as in English in our example.
- In English, the most frequent character in use refers to the following:
  - E T A O I N S H R D L C U M W F G Y P B V K X J Q Z
- Based on that the characters in ciphertext V,W,D,Q will be mapped to the characters E,T,A, or O
- By iterative for finding the number of character substitution it finally will reach to the cipher text.

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

Plain : I am going to the university

Cipher : t gv putdp eu enk zdthkxwtea

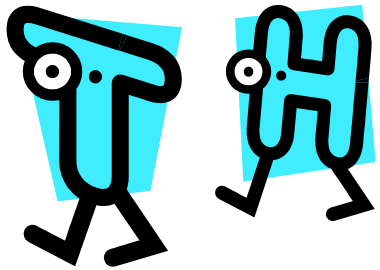
Exercise #2 (en) (K)

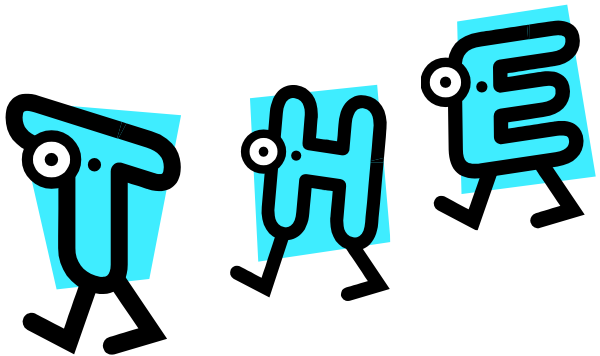
Plain : I did not have time to write a short letter so I wrote a long one instead

Cipher :t oto due nghk etvk ……

Monoalphabetic Ciphers

- Easy to break because they reflect the frequency data of the original alphabet
- Countermeasure is to provide multiple substitutes (homophones) for a single letter
- Digram
  - Two-letter combination
  - Most common is *th*
- Trigram
  - Three-letter combination
  - Most frequent is *the* *(bvd)*





3. Playfair Cipher

- Best-known multiple-letter encryption cipher
- Treats diagrams in the plaintext as single units and translates these units into cipher-text diagrams
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- Invented by British scientist Sir Charles Wheatstone in 1854
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II
- It represent another example for substitution-based encryption.

Advantages Over Som Other Classic Algorithms

- **Resistance to Frequency Analysis:** Unlike simple substitution ciphers like the Caesar cipher, the Playfair cipher obscures letter frequencies. This makes it more resistant to frequency analysis, where common letters in a language are exploited to crack a code

- **Complexity in Cryptanalysis:** Breaking the Playfair cipher without the key or key table is more challenging compared to simpler ciphers. It requires more sophisticated techniques than basic frequency analysis, adding a layer of complexity for cryptanalysis.

- **Handling Repeated Letters:** By using a filler letter ('X') for repeated or odd letters in pairs, it introduces an additional layer of confusion, making it harder to discern the original plaintext from the ciphertext.

- **Key Variability:** The key or keyword used to generate the table adds variability to the encryption process. Changing the keyword changes the arrangement of the key table, enhancing security by altering the encryption pattern.

Playfair Key Matrix

- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
- Using the keyword MONARCHY:
- Hi

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:

Key : MONARCHY
Plain text :instruments

Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

```
Plain Text: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
```

Rules for Encryption:

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

```
Diagraph: "me" Encrypted Text: cl
Encryption:
 m -> c e -> l
```

Example:

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).**For example:**

Diagraph: “ST" **Encrypted Text:** TL
Encryption:
s -> t t -> l

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.
For example:
Diagraph: "nt“
Encrypted Text: rq
Encryption: n -> r t -> q

Plain Text: "instrumentsz"
Encrypted Text: ga tl mz cl rq tx

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

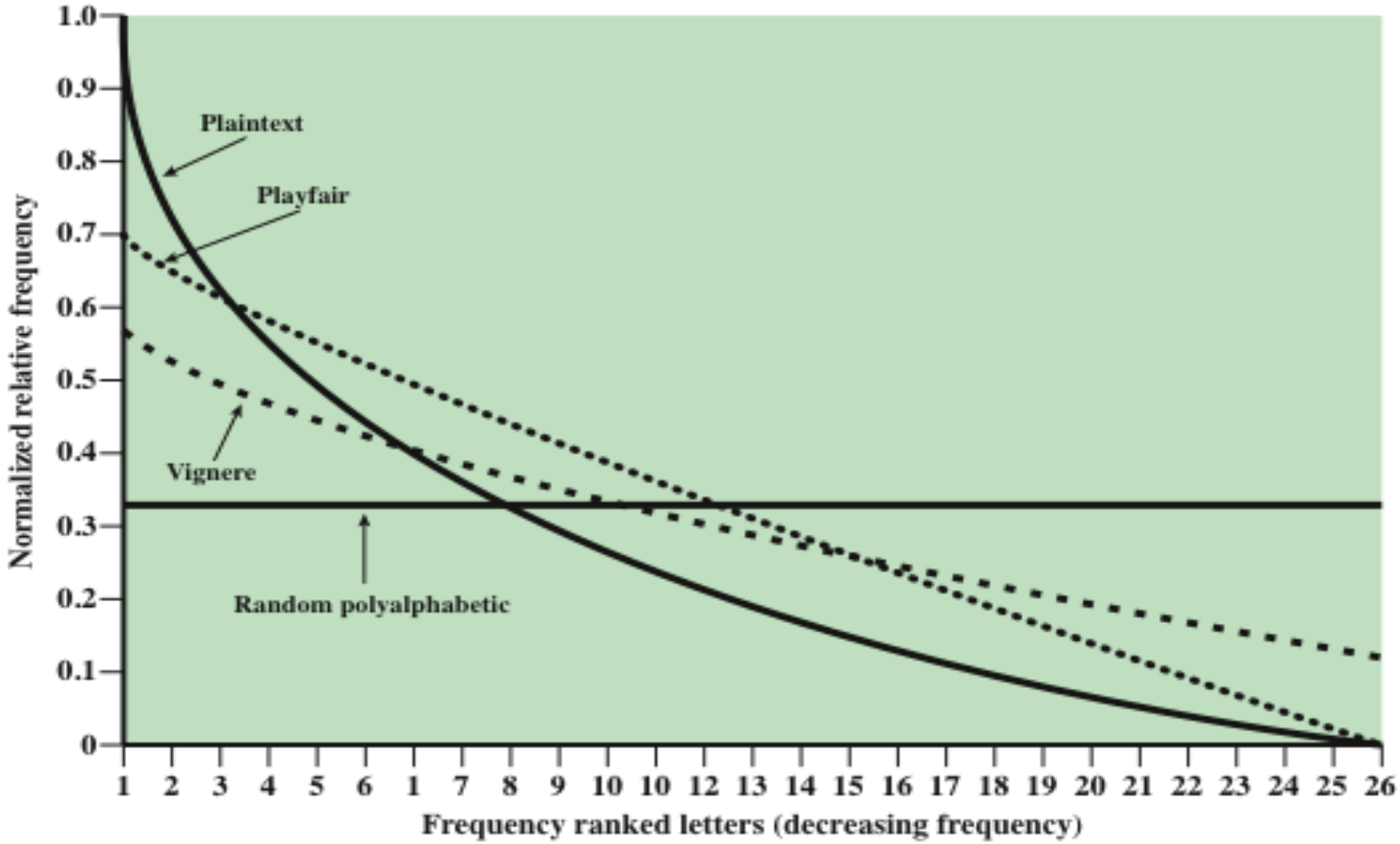


Figure 3.6 Relative Frequency of Occurrence of Letters

Playfair Key Matrix Example

Key : Hello students
Plain text :encryption
en cr yp ti on

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

Cipher: ou i/jm xq ab ng

Playfair Decryption Process

The process of Decryption is an opposite of the process of

- First point refers to divide the cipher text into blocks, each block with two letters.
- When two character at same column, shift up must be done here
- When two character of cipher text at same column, shift left must be done here.
- When both character at different line and column, the original method is applied in the decryption process

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

4. Hill Cipher

- Developed by the mathematician Lester Hill in 1929
- Strength is that it completely hides single-letter frequencies
  - The use of a larger matrix hides more frequency information
  - A 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information
- Strong against a cipher-text only attack but easily broken with a known plaintext attack

Determinant	1	3	5	7	9	11	15	17	19	21	23	25
Reciprocal Modulo 26	1	9	21	15	3	19	7	23	11	5	17	25

Hill Cipher Steps

Encryption:

1. Obtain a plaintext message to encode in Standard English with no punctuation.
2. Create an enciphering matrix.
a. Form a square 2x2 or 3x3 matrix with nonnegative integers each less than 26.
b. Check that its determinant does NOT factor by **2 or 13**. If this is so, return to Step **a**

3. Group the plaintext into pairs. If you have an odd number of letters, repeat the last letter.
4. Replace each letter by the number corresponding to its position in the alphabet i.e. A=0, B=1, C=2…Z=25.
5. Convert each pair of letters into plaintext vectors.
6. Multiply the enciphering matrix by each plaintext vector.
7. Replace each new vector by its residue modulo 25 if possible
8. Convert each entry in the cipher text vector into its corresponding position in the alphabet.
9. Align the letters in a single line without spaces. The message is now enciphered.

Cipher text = K*P mod 26

Where **k** is a key matrix that should not a singular matrix and P= plaintext

Decryption

Cipher text = (P* K^{-1}) mod 26

2*2

Key=$\begin{bmatrix} c & d \\ b & d \end{bmatrix}$

Key=$\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix}$

D= 2.3-1.3= 3

K= $\begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix}$

D=2.4-5.3=7

K= $\begin{bmatrix} 2 & 3 \\ 1 & 8 \end{bmatrix}$

D= 2.8-1.3= 13

Key =$\begin{matrix} g & y & b \\ n & q & k \\ u & r & p \end{matrix}$ Key =$\begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix}$

D=6 (16.15-10.17)-24(13.15-10.20)+1(13.17-20.16)

420+120-99=441 =Oi $\begin{bmatrix} 14 \\ 8 \end{bmatrix}$

Exmple1 si =$\begin{matrix} 18 \\ 8 \end{matrix}$ =$\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix}$ * $\begin{matrix} 18 \\ 8 \end{matrix}$ =$\begin{bmatrix} 60 \\ 42 \end{bmatrix}$ mod 26 =$\begin{matrix} 8 \\ 16 \end{matrix}$ = iq

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

Hill Cipher Example (Encryption)

Plaintext : Network

Where N=13 , E=4, t=19 ,W=22 ,O=14 ,R=17 , K=10.

1.Key= $\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix}$

2. ne= $\begin{matrix} 13 \\ 4 \end{matrix}$ **tw =** $\begin{matrix} 19 \\ 22 \end{matrix}$ **or =** $\begin{matrix} 14 \\ 17 \end{matrix}$ **kx=** $\begin{matrix} 10 \\ 23 \end{matrix}$

ne

$\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix} * \begin{bmatrix} 13 \\ 4 \end{bmatrix} = \begin{bmatrix} (13*2+4*3) \\ (13*1+4*3) \end{bmatrix} = \begin{bmatrix} 38 \\ 25 \end{bmatrix}$

38 mod 26=12 n=m

25 mod 26 =25 e =z

tw

$\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix} * \begin{bmatrix} 19 \\ 22 \end{bmatrix} = \begin{bmatrix} (19*2+22*3) \\ (19*1+22*3) \end{bmatrix} = \begin{bmatrix} 104 \\ 85 \end{bmatrix}$

104 mod 26=0 t=a

85 mod 26 =7 w =h

or

$\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix} * \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} (14*2+17*3) \\ (14*1+17*3) \end{bmatrix} = \begin{bmatrix} 79 \\ 65 \end{bmatrix}$

79 mod 26=1 o=b

65 mod 26 =13 r =n

kx

$\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix} * \begin{bmatrix} 10 \\ 23 \end{bmatrix} = \begin{bmatrix} (10*2+23*3) \\ (10*1+23*3) \end{bmatrix} = \begin{bmatrix} 89 \\ 79 \end{bmatrix}$

89 mod 26=11 k=l

79 mod 26 =1 x =b

Ciphertext : mz ah bn lb

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

Hill Cipher Example (Decryption)

Cipher text = (P* K^{-1}) mod 26

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

Determinant (K) = (2*3)-(1*3) =3

3 Inverse = 9

adj $\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 3 & -3 \\ -1 & 2 \end{bmatrix}$

$\begin{bmatrix} 3 & -3 \\ -1 & 2 \end{bmatrix}$ ***9** mod 26

$= \begin{bmatrix} 27 & -27 \\ -9 & 18 \end{bmatrix}$ mod 26

$K^{-1} = \begin{bmatrix} \mathbf{1} & \mathbf{25} \\ \mathbf{17} & \mathbf{18} \end{bmatrix}$

Ciphertext : mz ah bn lb

Mz $= \begin{bmatrix} \mathbf{12} \\ \mathbf{25} \end{bmatrix}$

$\begin{bmatrix} 1 & 25 \\ 17 & 18 \end{bmatrix} * \begin{bmatrix} \mathbf{12} \\ \mathbf{25} \end{bmatrix} = \begin{bmatrix} \mathbf{637} \\ \mathbf{654} \end{bmatrix}$

637 mod 26=13 m=n

654 mod 26 =4 z =e

ah $= \begin{bmatrix} \mathbf{0} \\ \mathbf{7} \end{bmatrix}$

$\begin{bmatrix} 1 & 25 \\ 17 & 18 \end{bmatrix} * \begin{bmatrix} \mathbf{0} \\ \mathbf{7} \end{bmatrix} = \begin{bmatrix} \mathbf{175} \\ \mathbf{126} \end{bmatrix}$

175 mod 26=19 a=t

126 mod 26 =22 h=w

bn $= \begin{bmatrix} \mathbf{1} \\ \mathbf{13} \end{bmatrix}$

$\begin{bmatrix} 1 & 25 \\ 17 & 18 \end{bmatrix} * \begin{bmatrix} \mathbf{11} \\ \mathbf{13} \end{bmatrix} = \begin{bmatrix} \mathbf{326} \\ \mathbf{251} \end{bmatrix}$

326 mod 26=14 b=o

251 mod 26 =17 n=r

lb $= \begin{bmatrix} \mathbf{11} \\ \mathbf{1} \end{bmatrix}$

$\begin{bmatrix} 1 & 25 \\ 17 & 18 \end{bmatrix} * \begin{bmatrix} \mathbf{11} \\ \mathbf{1} \end{bmatrix} = \begin{bmatrix} \mathbf{36} \\ \mathbf{205} \end{bmatrix}$

36 mod 26=10 l=k

205 mod 26 =23 b=x

Plaintext : ne tw or kx

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

Hill Cipher 3*3 Encryption

Plaintext : Sara
Plaintext : sar axx
where : s=18 , a=0 , r=17 , a=0 , x=23
Key : d k u
u j r
j e r

Key : 3 10 20
20 9 17
9 4 17

D = (3 (9(17) – 4(17))

- (10 (20(17) – 9(17))

+ (20 (20(4) - 9(9))

= -1635

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

Hill Cipher 3*3 Encryption

sar

$$\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \\ 17 \end{bmatrix} \text{ Mod 26}$$

$$\begin{bmatrix} (3)(18) + (10)(0) + (20)(17) \\ (20)(18) + (9)(0) + (17)(17) \\ (9)(18)+(4)(0) + (17)(17) \end{bmatrix} = \begin{bmatrix} 394 \\ 649 \\ 451 \end{bmatrix} \text{ mod26 } = \begin{bmatrix} 4 \\ 25 \\ 9 \end{bmatrix} = \begin{bmatrix} e \\ z \\ j \end{bmatrix}$$

Hill Cipher 3*3 Encryption

axx

$$\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 0 \\ 23 \\ 23 \end{bmatrix} \text{ Mod 26} = \begin{bmatrix} (3)(0) + (10)(23) + (20)(23) \\ (20)(0) + (9)(23) + (17)(23) \\ (9)(0) + (4)(23) + (17)(23) \end{bmatrix} \text{ mod 26}$$

$$= \begin{bmatrix} 690 \\ 598 \\ 483 \end{bmatrix} \text{ Mod 26} = \begin{bmatrix} 14 \\ 0 \\ 15 \end{bmatrix} = \begin{bmatrix} o \\ a \\ p \end{bmatrix}$$

Ciphertext : ezj oap

Hill cipher Decryption 3*3 Example

Key : 3 10 20
20 9 17
9 4 17

D = -1635

-1635 mod 26 = 3 = **9** we can call it adj(key) or K^{-1}

Ciphertext : ezj oap

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

Step 1: Matrix transpose

3	10	20		3	20	9
20	9	17	→	10	9	4
9	4	17		20	17	17

Hill cipher Decryption 3*3 Example cont…

Step 2 : cofactor

(9*17) – (4*17) = 85

(4*20) – (10*17) = -90

(10*17) – (9*20) = -10

(17*9) – (17*20) = -187

(17*3) – (20*9) = -129

(20*20) – (17*3) = 949

(20*4) – (9*9) = -1

(9*10) – (3*4) = 78

(3*9) – (20*10) = -173

85	-90	-10
-187	-129	394
-1	78	-173

Hill cipher Decryption 3*3 Example cont…

Step 3 :

The formula we have here is: K^{-1}

= Det key^{-1} * adj key

= 9

85	-90	-10
-187	-129	349
-1	78	-173

Mod 26 =

765	-810	-90
-1683	-1161	3141
-9	702	-1557

Mod 26 =

K^{-1} =

11	22	14
7	9	21
17	0	3

Hill cipher Decryption 3*3 Example cont…

The formula we have here is: K^{-1} = Det key^{-1} * adj key

= 9 *

85	-90	-10
-187	-129	394
-1	78	-173

Mod 26 =

765	-810	-90
-1683	-1161	3141
-9	702	-1557

Mod 26 =

K^{-1} =

11	22	14
7	9	21
17	0	3

Hill cipher Decryption 3*3 Example cont…

$P = (K^{-1} * C)$

$$\begin{matrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{matrix} * \begin{matrix} 4 \\ 25 \\ 9 \end{matrix}$$

First part: ezj

(4*11) + (25*22) + (9*14) = 720 mod 26 = 18 equal to S
(4*7) + (25*9) + (9*21) = 442 mod 26 = 0 equal to A
(4*17) + (25*0) + (9*3) = 95 mod 26 = 17 equal to R

$$\begin{matrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{matrix} * \begin{matrix} 14 \\ 0 \\ 15 \end{matrix}$$

Second part: **oap**

(14*11) + (0*22)+ (15*14) = 364 mod 26 = 0 equal to A
(14*7) + (0*9)+ (15*21) = 413 mod 26 = 23 equal to X
(14*17) + (0*0)+ (15*3) = 283 mod 26 = 23 equal to X

First part: sar , second part: axx
So now we have the full plain text which is : saraxx.

Hill Cipher Exercise #4

Plaintext : Network

$$\text{Key} = \begin{matrix} g & y & b \\ n & q & k \\ u & r & p \end{matrix} \qquad \text{Key} = \begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix}$$

D=441

$$\text{Net} = \begin{matrix} 13 \\ 4 \\ 19 \end{matrix} \qquad \text{Wor} = \begin{matrix} 22 \\ 14 \\ 17 \end{matrix} \qquad \text{kxx} = \begin{matrix} 10 \\ 23 \\ 23 \end{matrix}$$

1) $\begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix} * \begin{matrix} 13 \\ 4 \\ 19 \end{matrix} = \begin{matrix} 193 \\ 423 \\ 613 \end{matrix}$

2) $\begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix} * \begin{matrix} 22 \\ 14 \\ 17 \end{matrix} = \begin{matrix} 485 \\ 680 \\ 933 \end{matrix}$

3) $\begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix} * \begin{matrix} 10 \\ 23 \\ 23 \end{matrix} = \begin{matrix} 635 \\ 728 \\ 936 \end{matrix}$

Hill Cipher Exercise #4

A. (193mod26) = 11 = l
B. (423mod26) = 7 = h
C. (613mod26) = 15 = p

== lhp

A. (485mod26) = 17 = r
B. (680mod26) = 4 = e
C. (933mod26) = 23 = x

== rex

A.(635mod26) = 11 = l
B.(728mod26) = 0 = a
C.(936mod26) = 0 = a

==laa

Ciphertext = lhprexlaa
Key (3*3)

Ciphertext : mzahbnlb
key (2*2)

Transposition Techniques.

Transposition Ciphers are ciphers in which the plaintext message is rearranged by some means agree upon by the sender and receiver

5. Polyalphabetic Ciphers

- Polyalphabetic substitution cipher
  - Improves on the simple monoalphabetic technique by using different monoalphabetic substitutions as one proceeds through the plaintext message

All these techniques have the following features in common:
• A set of related monoalphabetic substitution rules is used • A key determines which particular rule is chosen for a given transformation

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

Encryption using Polyalphabetic cipher. Plaintext M=Security
The Key dependent through encryption process as follow

- Shift The first letter three position to the right.
- Shift the Second letter five position to its right.
- Shift the Third letter seven position to its right.

Original plain text message will be divided based on the number of roll used.
Plain text: Security
First part is Sec the encryption value is vjj.
Second Part is uri the encryption value is xwp.
Third part is tyx the encryption value for this part is wde.
Cipher text is vjjxwpwde
After that apply the rolls in each part of original message.

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

Decryption using Polyalphabetic cipher. Cipher test C=vhfzwnafe.
The Key dependent through encryption process as follow

- Shift The first letter three position to the left.
- Shift the Second letter five position to its left.
- Shift the Third letter seven position to its left.

the cipher message will be divided based on the number of roll used.
Cipher text: vjjxwpwde
First part is sec.
Second Part is uri.
Third part is tyx.
After that apply the rolls in each part of cipher message.

5. Vigenère Cipher

- The Vigenère cipher is the kind of polyalphabetic cipher.
- It was design by Blaise de Vigenère, a 16th century French mathematician.
- It was used in the American civil war and was once believed to be unbreakable.
- A Vigenère cipher uses a different strategy to create the key stream. The key stream is a repetition of an initial secret key stream of length m, where we have 1<=m<=26.
- The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.
- The Vigenère cipher uses multiple mixed alphabets, each is a shift cipher.

5. Vigenère Cipher

Plain text: $P = P_1 P_2 P_3 \ldots$

Cipher text: $C = C_1 C_2 C_3 \ldots$

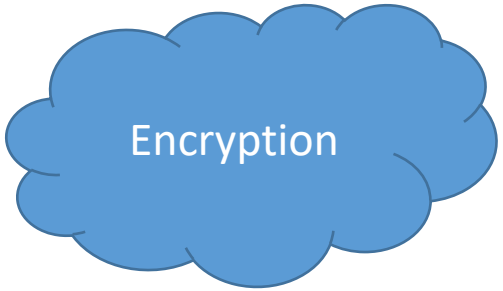
Key stream: $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: C= P+K

Decryption: $P_i = C_i - k_i$

5. Vigenère Cipher Example 1

- To find the cipher text for the plaintext **"she is listening "** using the word **"PASCAL"** as the key
- Ciphertext :hhwkswxslgntcg

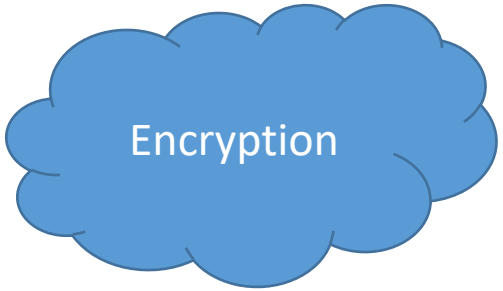


Plaintext	S	h	e	i	s	l	i	s	t	e	n	i	n	g
Key	p	a	s	C	a	l	p	a	s	c	a	l	p	a
(P+K)mod26	(18+15) mod26	(7+0) mod26	(4+18) mod26	(8+2) mod26	(18+0) mod26	(11+11) mod26	(8+15) mod26	(18+0) mod26	(19+18) mod26	(4+2) mod26	(13+0) mod26	(8+11) mod26	(13+15) mod26	(6+0) mod26
result	7	7	22	10	18	22	23	18	11	6	13	19	2	6
ciphertext	h	h	w	k	S	w	x	s	l	g	n	t	c	g

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

5. Vigenère Cipher Example 1

- To find the cipher text for the plaintext **"she is listening "** using the word **"Ali"** as the key
- Ciphertext :ssmidtidbeyqnr

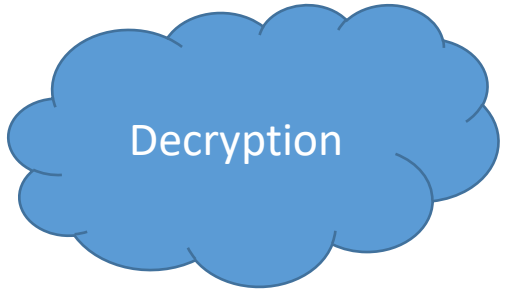


Plaintext	S	h	e	i	s	l	i	s	t	e	n	i	n	g
Key	A	l	i	A	l	i	A	l	i	A	L	l	A	L
(P+K)mod26	(18+0) mod26	(7+11) mod26	(4+8) mod26	(8+0) mod26	(18+11) mod26	(11+8) mod26	(8+0) mod26	(18+11) mod26	(19+8) mod26	(4+0) mod26	(13+11) mod26	(8+8) mod26	(13+0) mod26	(6+11) mod26
result	18	18	12	8	3	19	8	3	1	4	24	16	13	17
ciphertext	s	s	m	i	d	t	i	d	b	e	y	q	n	r

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

5. Vigenère Cipher Example

- To find the cipher text for the ciphertext **"hhwkswxslgntcg"** using the word **"PASCAL"** as the key



ciphertext	h	h	w	k	S	w	x	s	l	g	n	t	c	g
Key	p	a	s	C	a	l	p	a	s	c	a	l	p	a
(C-K)mod26	(7-15+26) mod26	(7-0) mod26	(22-18) mod26	(10-2) mod26	(18-0) mod26	(22-11) mod26	(23-15) mod26	(18-0) mod26	(11-18+26) mod26	(6-2) mod26	(13-0) mod26	(19-11) mod26	(2-15+26) mod26	(6-0) mod26
result	18	7	4	8	18	11	8	18	19	4	13	8	13	6
plaintext	s	h	e	i	s	l	i	s	t	e	n	i	n	g

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

5. Vigenère Cipher Example2

To find the cipher text for the plaintext **"she is listening "** using the word **"osama"** as the key

Plaintext	s	h	e	i	s	l	i	s	t	e	n	i	n	g
Key	o	s	a	m	a	o	s	a	m	a	o	s	a	m
(P+K) mod 26	(18+14) Mod 26	(7+18) Mod 26	(4+0) Mod 26	(8+12) Mod 26	(18+0) Mod 26	(11+14) Mod 26	(8+18) Mod 26	(18+0) Mod 26	(19+12) Mod 26	(4+0) Mod 26	(13+14) Mod 26	(8+18) Mod 26	(13+0) Mod 26	(6+12) Mod 26
Result	6	25	4	20	18	25	0	18	5	4	1	0	13	18
Cipher Text	g	z	e	u	s	z	a	s	f	e	b	a	n	s

5. Vigenère Cipher Exercise

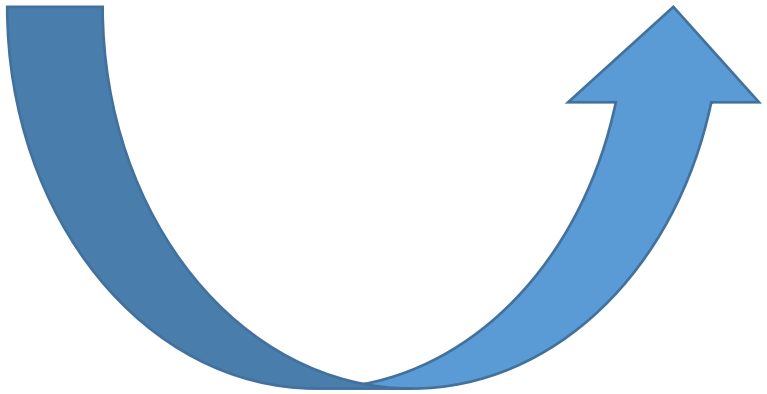
Find the cipher text for the Plaintext **“Ali wants to go to the restaurant ”** using the word **“Sameer ”** as the key

Ciphertext ????

2.2.2 Transposition Techniques.

- **Rail fence Cipher.**
- **The Route Cipher**

Next >>>



1. Rail fence Cipher.

- Simplest transposition cipher
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- To encipher the message
- “meet me after the toga party”
- with a rail fence of depth 2, we would write:

M		e		m		a		t		r		h		t		g		p		r		y
	E		t		e		f		e		t		e		o		a		a		t	

Encrypted message is:
ciphertext :MEMATRHTGPRYETEFETEOAAT

1. Rail fence Cipher(Decryption)

- The decryption process for Rail fence depends totally on the depth of encryption process.
- Based on the depth the total cipher text will be divided over depth, as example if we have 23 character at cipher text, the first row in generated plain text will contain 12 character and second row will contain remain charachters.

  Encrypted message is:

  ciphertext :MEMATRHTGPRYETEFETEOAAT

  Plain text will be at row one M E M A T R H T G P R Y

  The plain text at row two is E T E F E T E O A A T

M		e		m		a		t		r		h		t		g		p		r		y
	E		t		e		f		e		t		e		o		a		a		t	

1. Rail fence Cipher. Example 2

with a rail fence of depth 3 we would write:“meet me after the toga party”

M				m				t				h				g				r		
	e		t		e		f		e		t		e		o		a		a		t	
		e				a				r				t				p				y

Encrypted message is:
mmthgretefeteoaateartpy

She is listening
sstnhilseigein

S				S				T				N										
	h		I		l		S		E		I		g									
		E				I				N												

Rail fence Cipher. Example 3

Suppose we want to encrypt the message "buy your books in August" using a rail fence cipher with encryption key 3.

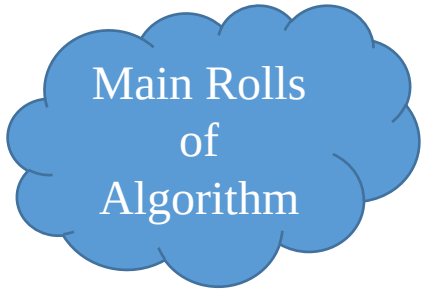
Here is how we would proceed. i. Arrange the plaintext characters in an array with 3 rows (the key determines the number of rows), forming a zig-zag pattern:

b				o				o				i				g			
	u		y		u		b		o		s		n		u		u		t
		Y				r				k				a				s	

ii. Then concatenate the non-empty characters from the rows to obtain the

ciphertext: BOOIGUYUBOSNUUTYRKAS

The Row Cipher Algorithm



1. From top-right corner clockwise to the center
2. The process of writing is done row by row.
3. From top-right corner anticlockwise to the center
4. The process of reading for the cipher text is done column by column
5. The Rectangle size is specified based on sender and receiver
6. The Algorithm is more complicated than previous algorithm.
7. The Key refers to the order of the columns.

The Row Cipher Algorithm

Encryption Example

Make the Statement using 5 columns :
Plain text : the simplest possible transpositions
Key : 41532

1	2	3	4	5
T	H	E	S	I
M	P	L	E	S
T	P	O	S	S
I	B	L	E	T
R	A	N	S	P
O	S	I	T	I
O	N	S	X	X

4	1	5	3	2
S	T	I	E	H
E	M	S	L	P
S	T	S	O	P
E	I	T	L	B
S	R	P	N	A
T	O	I	I	S
X	O	X	S	N

The Row Cipher Algorithm (Method two)

Encryption Example

Make the Statement using 5 columns :
Plain text : Attack postponed untill two am
Key : 4312567
In generated matrix No.Rows = No.character/ digits of key
The encryption process depends on dividing the plain text in the matrix based on the numbers, starting from column one, the column two and so on

1	2	3	4	5	6	7
4	**3**	**1**	**2**	**5**	**6**	**7**
A	T	T	A	C	K	P
O	S	T	P	O	N	E
D	U	N	T	I	L	L
T	W	O	A	M	X	x

The Cipher text here is:
TTNO APTA TSUW AODT COIM KNLX PELX

The Row Cipher Algorithm

Encryption Example

In the case the key is alphabetic not digits as previous example, the distribution of text under columns depends here on the rank of alphabetic, such as if the key is Security, the number one is c number two e and so on
Text = Attack postponed untill two am
NO.ROWS = 26/8 = 3.25, WHICH MEAN FOUR ROWS WILL BE GENERATED

S	E	C	U	R	I	T	Y
		A					
		T					
		T					
		A					

The Route Cipher

The Route Cipher is a **transposition cipher** where the key is which route to follow when reading the ciphertext from the block created with the plaintext. The plaintext is written in a grid, and then read off following the route chosen

First, we write the plaintext in a block of reasonable size for the plaintext. Part of your key is the size of this grid, so you need to decide on either a number of columns or number of rows in the grid before starting. Once the plaintext is written out in the grid, you use the Route assigned.
This could be spiraling inwards from the

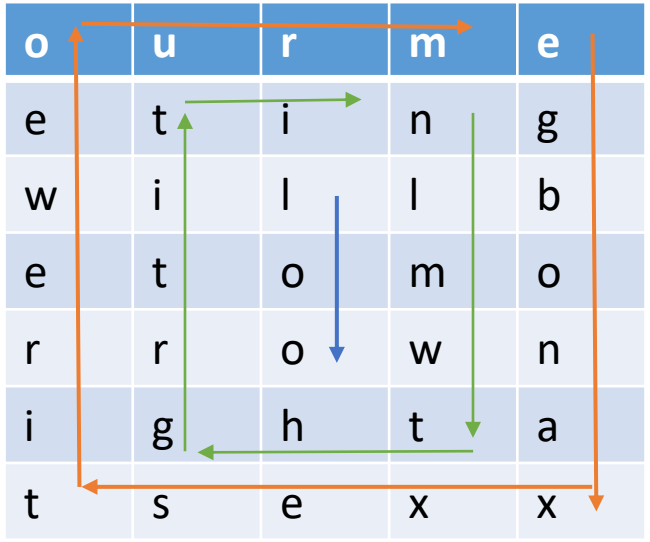
- **Top right corner in a clockwise direction,**
- **zigzagging up and down**.

The Route Cipher Example

Key size =5

Plain text: our meeting will be tomorrow night at six

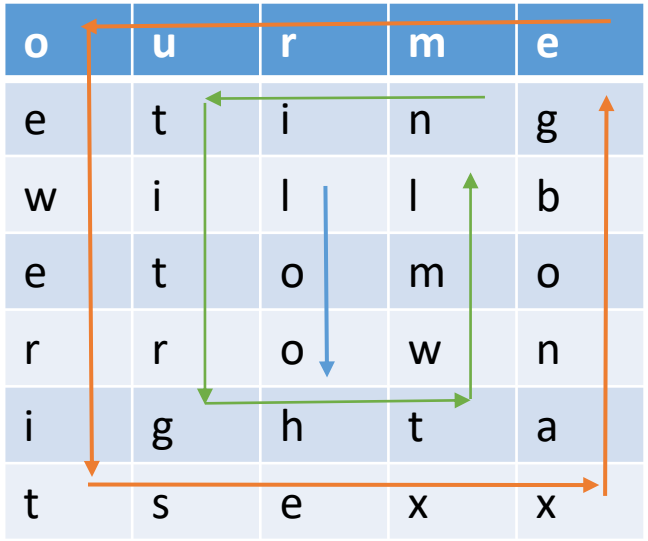
1. From top-right corner clockwise to the center



o	u	r	m	e
e	t	i	n	g
w	i	l	l	b
e	t	o	m	o
r	r	o	w	n
i	g	h	t	a
t	s	e	x	x

cipher text:egbonaxxestireweourmnlmwthgrtitiloo

2. From top-right corner anticlockwise to the center



o	u	r	m	e
e	t	i	n	g
w	i	l	l	b
e	t	o	m	o
r	r	o	w	n
i	g	h	t	a
t	s	e	x	x

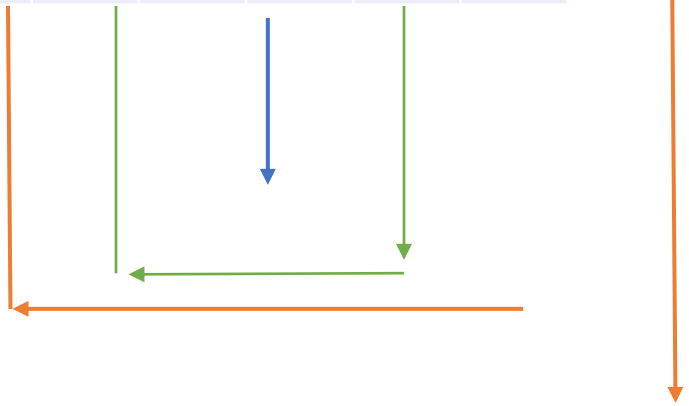
cipher text:emruoeweritsexxanobgnititrghtwmlloo

The Route Cipher Example

Key size =6

2. Plaintext: **the center of the city (ntyticehtthecefore)**

t	H	e	c	e	N
T	e	R	o	f	t
H	e	c	i	t	y



o	u	r	m	e
e	t	i	n	g
w	i	l	l	b
e	t	o	m	o
r	r	o	w	n
i	g	h	t	a
t	s	e	x	x

cipher text:egbonaxxestireweourmnlmwthgrtitiloo

cipher text:emruoeweritsexxanobgnititrghtwmlloo