

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Polyalphabetic Ciphers

- ❑ A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- ❑ polyalphabetic cipher 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.

Polyalphabetic Ciphers Encryption

❑ Assume

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

❑ Then We set these Rules:

Polyalphabetic Ciphers Encryption

□ Then We set Key as Rules:

- 1) Shift the first letter **three** position to the right
- 2) Shift the second letter **five** position to the right
- 3) Shift the third letter **seven** position to the right

□ Given Plaintext = security

Polyalphabetic Ciphers Encryption

□ Given Plaintext = security

1) Divide Plaintext to three words

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

2) P= sec uri ty

3) C= VJJ XWP WD

Polyalphabetic Ciphers Decryption

□ Then We set Key as Rules: (reverse)

- 1) Shift the first letter three position to the left
- 2) Shift the second letter five position to the left
- 3) Shift the third letter seven position to the left

□ Given Ciphertext = VJXWPWD

Polyalphabetic Ciphers Decryption

□ Given C= VJJXWPWD

1) Divide Plaintext to three words as your rules number

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

2) C= VJJ XWP WD

3) C= SEC URI TY

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Vigenère Cipher

- ❑ The Vigenère cipher, was invented by a Frenchman, Blaise de Vigenère in the 16th century.
- ❑ Vigenère cipher is a simple polyalphabetic cipher

Vigenère Cipher

$$\square C_i = (P_i + K) \bmod 26$$

$$\square P_i = (C_i - K) \bmod 26$$

□ Repeating key

Vigenère Cipher Encryption

□ K =deceptive

□ P =we are discovered save yourself

key: *deceptivedeceptivedeceptive*

plaintext: *wearediscoveredsaveyourself*

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

Vigenère Cipher Encryption

key: *deceptivedeceptivedeceptive*
plaintext: *wearediscoveredsaveyourself*

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenère Cipher Encryption

❑ Result

key:	<i>deceptivedeceptivedeceptive</i>
plaintext:	<i>wearediscoveredsaveyourself</i>
ciphertext:	ZIC <u>VTW</u> QNGRZG <u>VTW</u> AVZHCQYGLMGJ

Vigenère Cipher Encryption

- ❑ The strength of Vigenère Cipher is that there are multiple ciphertext letters for each plaintext letter

Vigenère Cipher Decryption

- ❑ decryption simply works in reverse
- ❑ $P_i = (C_i - K) \bmod 26$

ciphertext:	ZIC <u>VTW</u> QNGRZG <u>VTW</u> AVZHCQYGLMGJ
key:	<i>deceptivedeceptivedeceptive</i>
plaintext:	<i>wearediscoveredsaveyourself</i>

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Autokey Cipher

□ An autokey cipher (also known as the autoclave cipher) is a cipher which incorporates the message (the plaintext) into the key.

$$\square P = \{p_1, p_2, p_3, \dots, p_n\}$$

$$\square K = \{k_1, p_1, p_2, p_3, \dots, p_{n-1}\}$$

$$\square C = \{c_1, c_2, c_3, \dots, c_n\}$$

Autokey Cipher

$$\square C_i = (P_i + K_i) \bmod 26$$

$$\square P_i = (C_i - K_i) \bmod 26$$

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

Autokey Cipher Encryption

□ $K = m$

□ $P = \text{attack is today}$

Plaintext	a	t	t	a	c	k	i	s	t	o	d	a	y
P Value	0	19	19	0	2	10	8	18	19	14	3	0	24
Key	12	0	19	19	0	2	10	8	18	19	14	3	0
C Value	12	19	12	19	2	12	18	0	11	7	17	3	24
Ciphertext	m	t	m	t	c	m	s	a	l	h	r	d	y

Autokey Cipher Decryption

□ $K = m$

□ $C = mtmtcmsalhrdy$

Ciphertext	m	t	m	t	c	m	s	a	l	h	r	d	y
C Value	12	19	12	19	2	12	18	0	11	7	17	3	24
Key	12	0	19	19	0	2	10	8	18	19	14	3	0
P Value	0	19	19	0	2	10	8	18	19	14	3	0	24
Plaintext	a	t	t	a	c	k	i	s	t	o	d	a	y

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

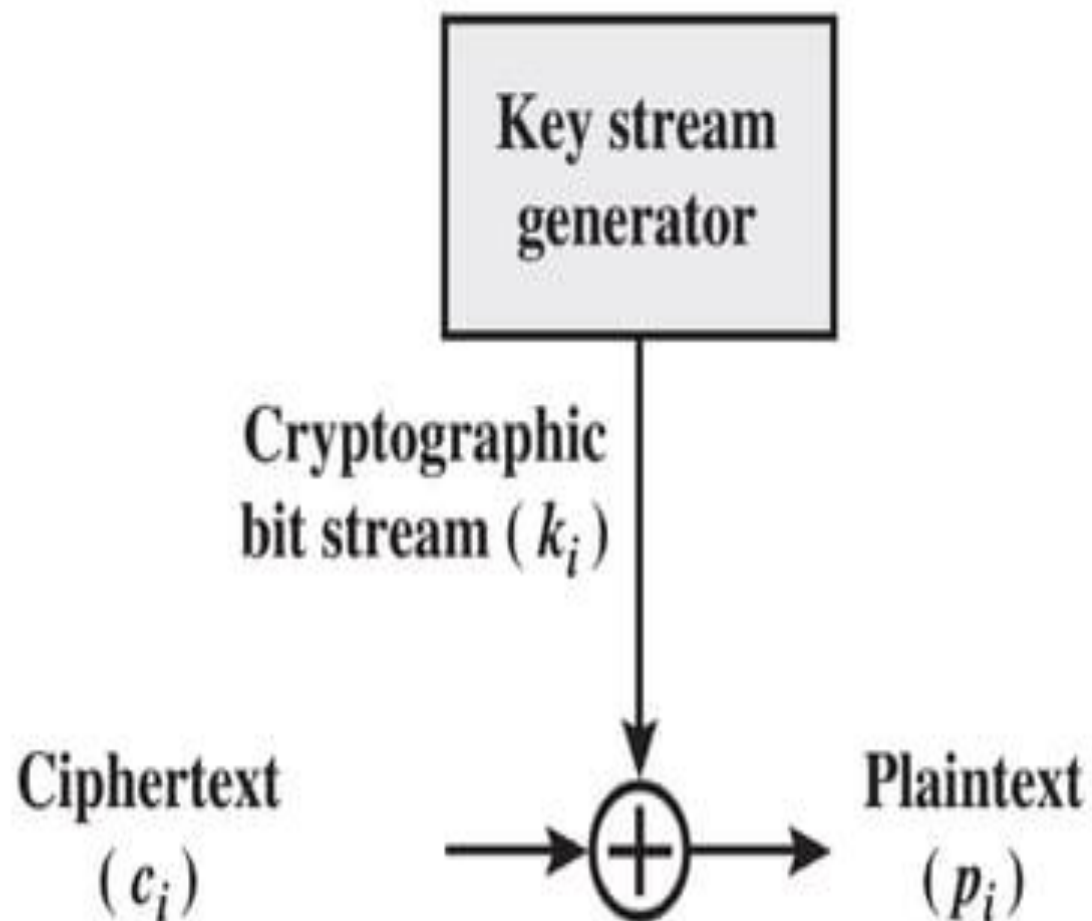
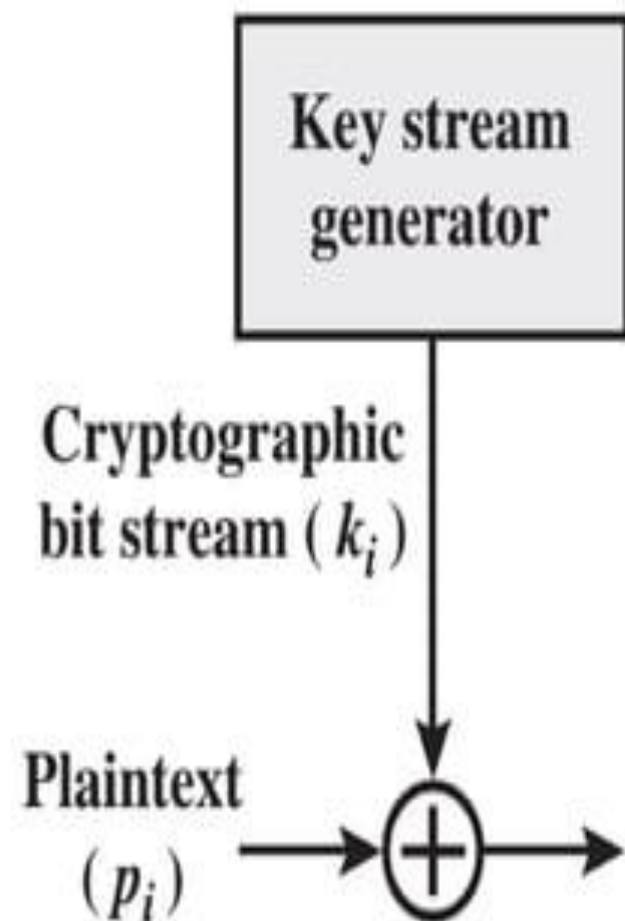
Rail Fence Cipher

Row Transposition Cipher

Vernam Cipher

- ❑ Vernam Cipher was introduced by an AT&T engineer named Gilbert Vernam in 1918.
- ❑ The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it.

Vernam Cipher



Vernam Cipher

❑ Encryption

$$\blacktriangleright C = P \text{ XOR } K$$

❑ Decryption

$$\blacktriangleright P = C \text{ XOR } K$$

Vernam Cipher Encryption

□ $P = 11100011101010101101$

□ $K = 1001010101$

□ $P = 11100011101010101101$

□ $K = 1001010101$ 1001010101

□ $C = 01110110110011111000$

Vernam Cipher Decryption

□ C=01110110110011111000

□ K=10010101011001010101

□ P=11100011101010101101

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Transposition Ciphers



The clear text message would be encoded using a key of 3.



Use a rail fence cipher and a key of 3.



The clear text message would appear as follows.

Transposition Techniques

□ Transposition Techniques performing some sort of permutation on the plaintext letters (reorder the position of letters in plaintext).

□ Types:

- Rail Fence Cipher
- Row Transposition Cipher

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Rail Fence Cipher Encryption

□ P= meet me after the toga party

□ K=2

$$1) p = \begin{bmatrix} m & e & m & a & t & r & h & t & g & p & r & y \\ e & t & e & f & e & t & e & o & a & a & t & \end{bmatrix}$$

2) C=mematrhtgpryetefeteoaat

Rail Fence Cipher Decryption

□ C=mematrhtgpryetefeteoaat

□ K=2

$$1) C = \begin{bmatrix} m & e & m & a & t & r & h & t & g & p & r & y \\ e & t & e & f & e & t & e & o & a & a & t \end{bmatrix} \downarrow$$

2) P= meetmeafterthetogaparty

Table of Contents

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Row Transposition Cipher Encryption

□ P= attack postponed until two am

□ K= 4312567

$$\square C = \begin{pmatrix} 4 & 3 & 1 & 2 & 5 & 6 & 7 \\ a & t & t & a & c & k & p \\ o & s & t & p & o & n & e \\ d & u & n & t & i & l & t \\ w & o & a & m & x & x & x \end{pmatrix} = \text{ttnaaptmtsuoaodwcoixknlxpetx}$$

Row Transposition Cipher Decryption

□ $C = \text{ttnaaptmtsuoao dwcoix knl xpetx} = \text{Len}(C) = 28$

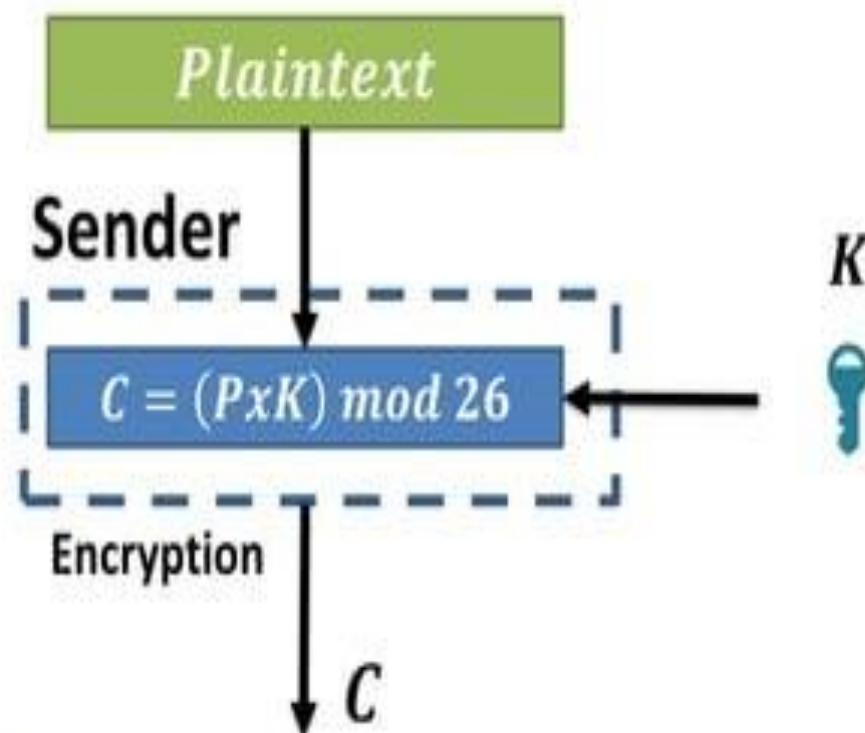
□ $K = 4312567$

□ Each Column have $28/7 = 4$ letter

□ $P = \begin{pmatrix} 4 & 3 & 1 & 2 & 5 & 6 & 7 \\ a & t & t & a & c & k & p \\ o & s & t & p & o & n & e \\ d & u & n & t & i & l & t \\ w & o & a & m & x & x & x \end{pmatrix} = \text{attackpostponeduntiltwoamxxx}$

Task 1

- As shown in Figure below, use *Multiplicative Cipher* to encrypt "enemy attack tonight" with key = 4.



Task2

- As shown in Figure below, use Affine Cipher to encrypt "enemy attack tonight" with key pair (4,3).

