Cryptography

LECTURE-2

Mixed alphabet cipher

- the ciphertext alphabet is constructed by picking a keyword and writing it down, ignoring repeated letters. Follow it with the letters of the alphabet that have not yet been used.

Example

ENCRYPTION

Encrypt the plaintext” **computer**” using mixed alphabet with keyword “**information**”

Solution

Keyword: information

Remove duplicate: informat

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

Plaintext	computer
Ciphertext	FJGKUSRP

DECRYPTION

Decrypty the ciphertext” **FJGKUSRP**” using mixed alphabet with keyword “**information**”

Solution

Keyword: information

Remove duplicate: informat

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

Ciphertext	FJGKUSRP
Plaintext	computer

Greatest Common Divisor

The **Euclidean algorithm** is a way to find the *greatest common divisor* of two positive integers a and b.

Formal description of the Euclidean algorithm

- Input Two positive integers, a and b.
- Output The greatest common divisor of a and b.
- Internal computation
    1. If a<b, exchange a and b.
    2. Divide a by b and get the remainder, r. If r=0, report b as the GCD of a and b.
    3. Replace a by b and replace b by r. Return to the previous step.

Example

$60 \div 18 = 3$ r= 6 *(60 = 3 × 18 + 6)*

$18 \div 6 = 3$ r= 0 *(18 = 3 × 6 + 0)*

When remainder r = 0, the GCD is the divisor, b, in the last equation. GCD = 6

Relative Prime: *Two integers a and b are relatively prime if gcd(a,b) = 1*

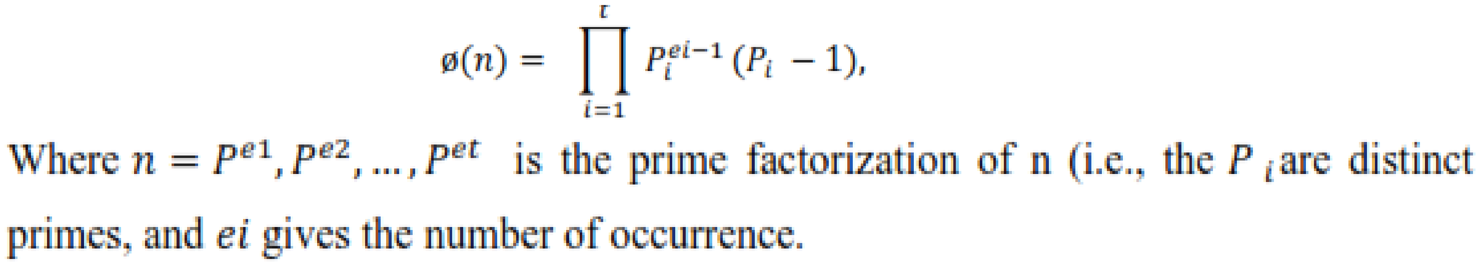
Example:

4 and 5 are relative prime

4 and 10 are not relative prime

Euler totient function ø(n): defined as the number of positive integers less than *n and* relatively prime to *n*

for arbitrary n, ø(n) is given by



$$ø(n) = \prod_{i=1}^{t} P_i^{ei-1}(P_i - 1),$$

Where $n = P^{e1}, P^{e2}, \ldots, P^{et}$ is the prime factorization of n (i.e., the P_i are distinct primes, and *ei* gives the number of occurrence.

Euler's generalization gives us an algorithm for solving an equation
$ax \; mod \; n = 1$, where gcd (a, n)=1
This solution is given by

$$x = a^{ø(n)-1} \; mod \; n$$

Examples

1. What is the Euler totient function for n=24

Solution

$\mathbf{24 = 2^3 \times 3}$

ø(24) =$\mathbf{2^2 \times (2-1) \times 3^0 \times (3-1) = 8}$

2. Find **ø(27)**

Solution

$\mathbf{27 = 3^3}$

ø(27) =$\mathbf{3^2 \times (3-1) = 18}$

3. Find ø(12) ?

Example

Find the inverse of 9 mod 26

Solution

gcd (9, 26)=1

$x = a^{\emptyset(n)-1}\ mod\ n$

$x = 9^{\emptyset(26)-1}\ mod\ 26$

$\emptyset(26)$ =?

$\mathbf{26 = 2 \times 13}$

$\emptyset(26) = 2^0 \times (\mathbf{2-1}) \times \mathbf{13^0} \times (\mathbf{13-1})$ =**12**

$x = 9^{\emptyset(26)-1}\ mod\ 26$

$x = 9^{12-1}\ mod\ 26$

X=3

Example

Let a=3 and n=7, find inverse of a mod n

Solution

gcd (3, 7)=1

$x = 3^{\emptyset(7)-1}\, mod\ 7$

$x = 3^{6-1}\, mod\ 7$

X=5

Multiplicative Cipher

In multiplicative cipher, each **plaintext** character is multiplied by ***K***

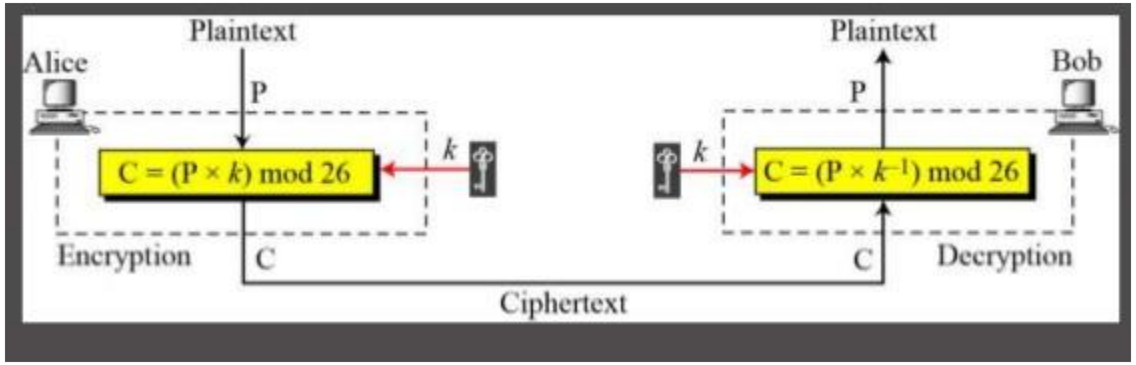
$C = E\ (P, K) = (P \times K) mod\ n$

and

$GCD\ (K, n)\ = 1$

For example 15 and 26 have no factors in common, so 15 is an acceptable value for *key* however 12 and 26 have factors in common (e.g. 2) so 12 cannot be used for a value of *key.*

$P = D\ (C, K)\ = C \times K^{-1}\ mod\ n$



What is the key domain for any multiplicative cipher?

only 12 possible keys: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have $GCD\ (K, 26) = 1$

Here are the possible multipliers and their inverses:

K	1	3	5	7	9	11	15	17	19	21	23	25
K^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Example

ENCRYPTION

We use a multiplicative cipher to encrypt the plaintext “**computer**” with a key of 9. The ciphertext is “SWEFYPKX”.

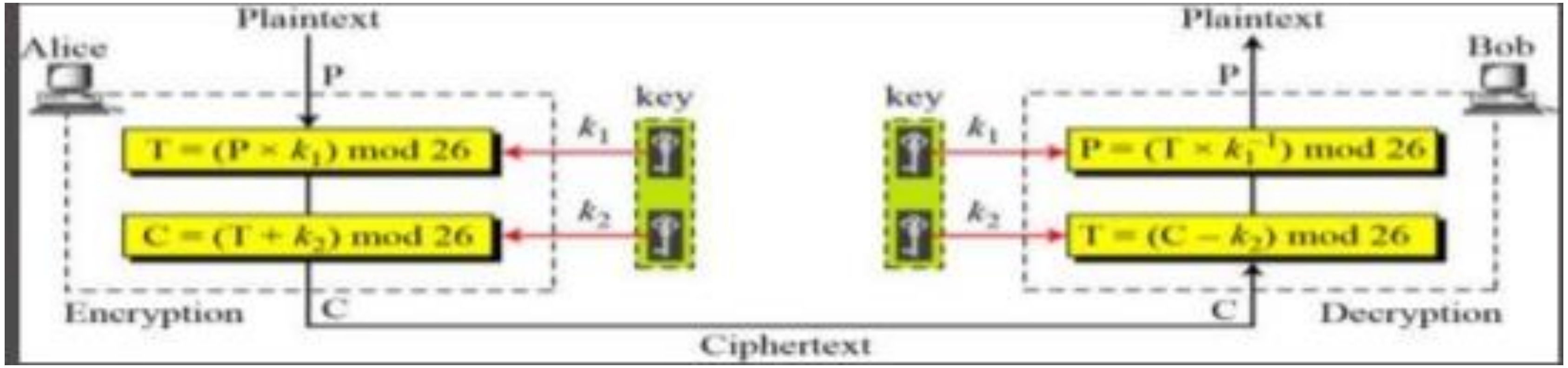
plaintext	c	o	m	p	u	t	e	r
value	2	14	12	15	20	19	4	17
Key(k=9)	9	9	9	9	9	9	9	9
Plaintext* 9	18	126	108	135	180	171	36	135
Mod 26	18	22	4	5	24	15	10	23
ciphertext	S	W	E	F	Y	P	K	X

DECRYPTION

We use a multiplicative cipher to decrypt the ciphertext “SWEFYPKX” with the inverse key of 9 which is k=3. The plaintext “computer”.

ciphertext	S	W	E	F	Y	P	K	X
value	18	22	4	5	24	15	10	23
$(K^{-1} = 3)$	3	3	3	3	3	3	3	3
Ciphertext * K^{-1}	45	66	12	15	72	45	30	69
Mod 26	2	14	12	15	20	19	4	17
plaintext	c	o	m	p	u	t	e	r

Affine Cipher



Affine cipher

$$C = E\ (P) = (PK_1 + K_2)\ mod\ n, \text{where GCD } (\mathrm{K}_1, \mathrm{n}) = 1$$

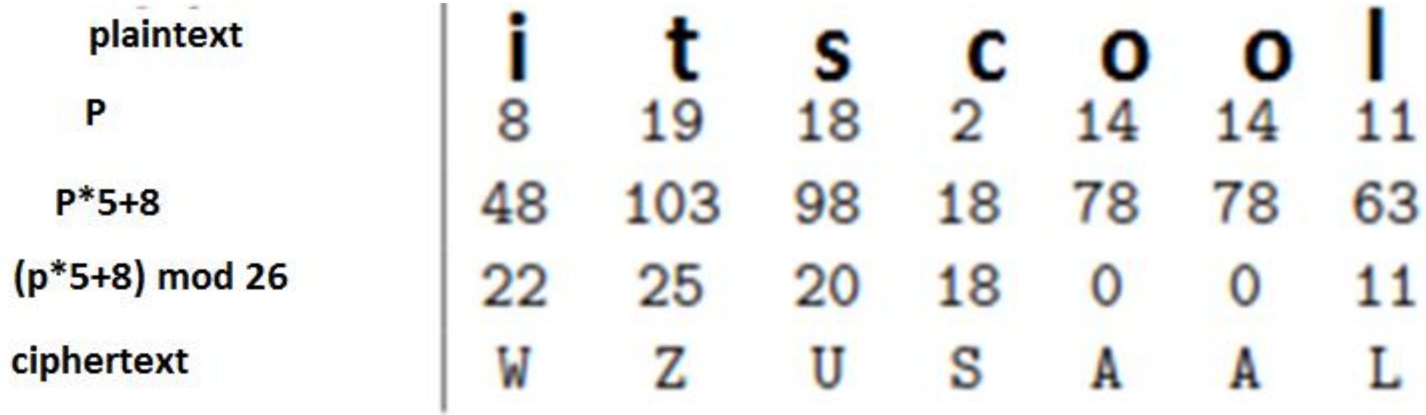
$$\mathrm{P} = D\ (\mathrm{C}) = ((C - K_2) \times K_1^{-1})\ mod\ n, \text{where GCD } (\mathrm{K}_1, \mathrm{n}) = 1$$

- 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 $k_2 = 0$.

Example

Encrypt the plaintext ”**its cool**” using affine cipher with k1=5 and k2=8

$$C = E\,(P) \;=\; (5 \times \mathrm{p} + 8)\; mod\; 26$$



plaintext	i	t	s	c	o	o	l
P	8	19	18	2	14	14	11
P*5+8	48	103	98	18	78	78	63
(p*5+8) mod 26	22	25	20	18	0	0	11
ciphertext	W	Z	U	S	A	A	L

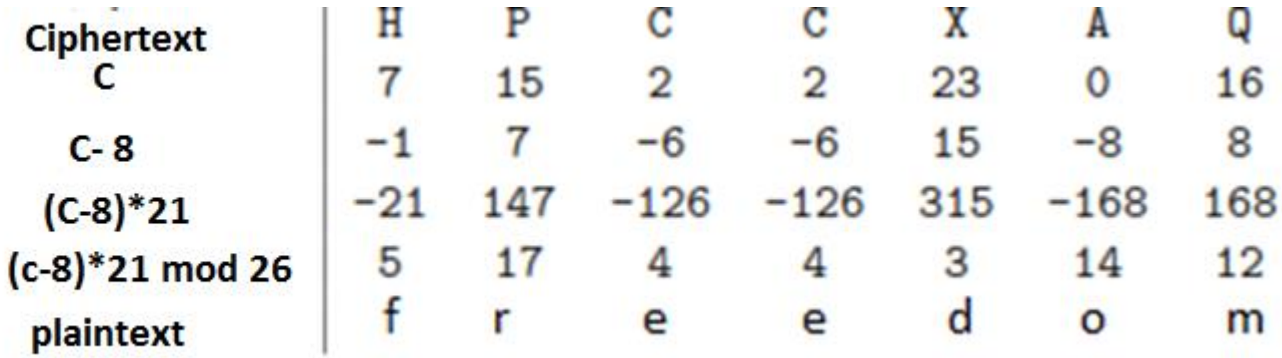
Example

Decrypt the ciphertext” **HPCCXAQ** ” using affine cipher with k1=5 and k2=8

Solution : we begin by finding the key inverse of k1, the key inverse of 5 is 21. Then apply

$$\mathrm{P} = D\ (\mathrm{C}) = \left((C - K_2) \times K_1^{-1}\right) mod\ 26,$$

$$\mathrm{P} = D\ (\mathrm{C})\ = ((C - 8) \times 21)\ mod\ 26$$



Ciphertext	H	P	C	C	X	A	Q
C	7	15	2	2	23	0	16
C- 8	-1	7	-6	-6	15	-8	8
(C-8)*21	-21	147	-126	-126	315	-168	168
(c-8)*21 mod 26	5	17	4	4	3	14	12
plaintext	f	r	e	e	d	o	m

Homophonic Cipher

Cipher involves replacing each letter with a variety of substitutes, the number of potential substitutes being proportional to the frequency of the letter.

A	12 29 25 43 71 80 89 95
B	05 92
C	19 37 36
D	23 41 61 66
E	16 30 47 59 72 83 90 60 69 88 99 00
F	17 49
G	02 31
H	04 45 55 63 76 82
I	15 34 56 97 77 86
J	03
K	11
L	24 38 48 64
M	65 46
N	26 42 53 70 73 98
O	10 44 50 94 78 85 91
P	06 39
Q	52
R	21 35 54 20 74 87
S	01 40 57 68 79 81
T	13 28 51 67 75 84 33 27 22
U	08 62 58
V	07
W	18 32
X	96
Y	09 93
Z	14

Plaintext:	computer
Ciphertext	19 10 65 06 58 13 16 21

Ciphertext	45 59 77 15 94
Plaintext	?

Polyalphabetic substitution cipher

- Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.

Vigenere Cipher

- The best known, and one of the simplest, polyalphabetic ciphers is the Vigenère cipher.
- In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter

$$c_i = (p_i + k_i)\ mod\ n$$
$$p_i = (c_i - k_i)\ mod\ n$$

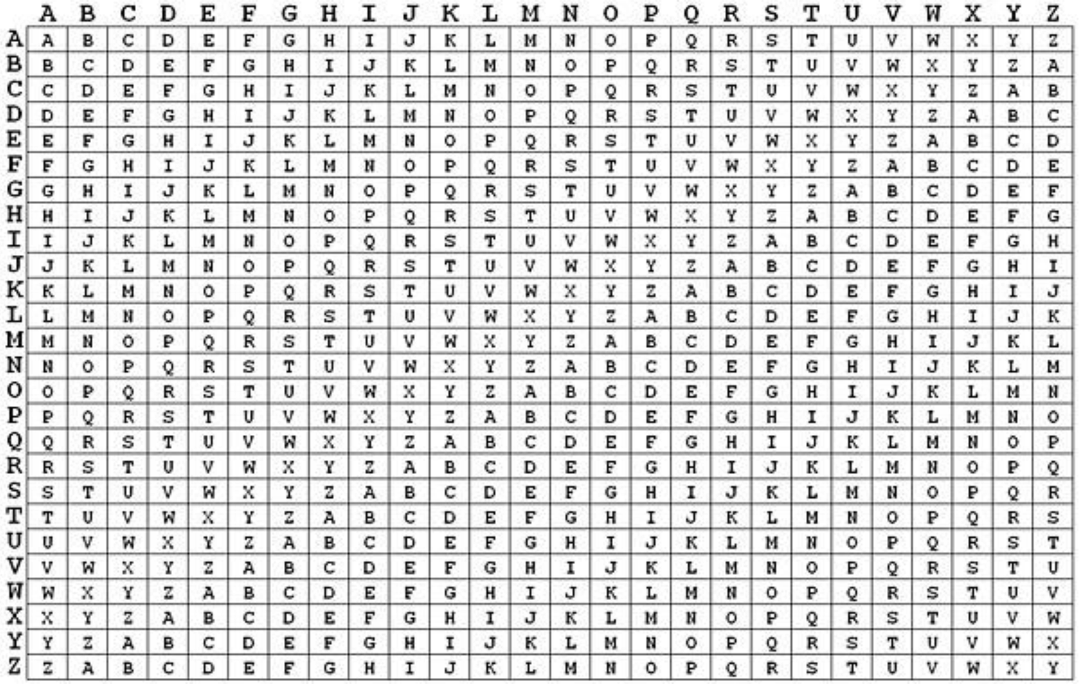
- key is needed that is as long as the message. Usually, the key is a repeating keyword.

Vigenère cipher

- ❑The Vigenère cipher uses a 26×26 table with **A** to **Z** as the row heading and column heading .

- ❑This table is usually referred to as the ***Vigenère Tableau***, ***Vigenère Table*** or ***Vigenère Square***.

- ❑The first row of this table has the 26 English letters. Starting with the second row, each row has the letters shifted to the left one position in a cyclic way.



	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

Example

The plaintext is "javatpoint", and the key is "best".

- the given key is repeated in a circular manner, as long as the length of the plain text does not equal to the new key.

j	a	v	a	t	p	o	i	n	t
b	e	s	t	b	e	s	t	b	e

Encryption

- The first letter of the plaintext is combined with the first letter of the key. The column of plain text “j" and row of key “b" intersects the alphabet of “k" in the vigenere table, so the first letter of ciphertext is “k".
- Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text “a" and row of key “e" intersects the alphabet of “e" in the vigenere table, so the second letter of ciphertext is “e".
- This process continues continuously until the plaintext is finished.

Ciphertext = kentutgbox

Decryption

Ciphertext = kentutgbox, key=best

k	e	n	t	u	t	g	b	o	x
b	e	s	t	b	e	s	t	b	e

- First, select the row of the key letter, find the ciphertext letter's position in that row, and then select the column label of the corresponding ciphertext as the plaintext.
- For example, in the row of the key is "b" and the ciphertext is "k" and this ciphertext letter appears in the column "j", that means the first plaintext letter is "j".
- Next, in the row of the key is "e" and the ciphertext is "e" and this ciphertext letter appears in the column "a", that means the second plaintext letter is "a".
- This process continues continuously until the ciphertext is finished.

Plaintext = javatpoint

Example

The plaintext is "javatpoint", and the key is "best".

Encryption: $c_i = (p_i + k_i) \bmod 26$

plaintext	j	a	v	a	t	p	o	i	n	t
Plaintext value (P)	09	00	21	00	19	15	14	08	13	19
Key	b	e	s	t	b	e	s	t	b	e
Key value (K)	01	04	18	19	01	04	18	19	01	04
Ciphertext value (E)	10	04	13	19	20	19	06	01	14	23
Ciphertext	k	e	n	t	u	t	g	b	o	x

DECRYPTION:

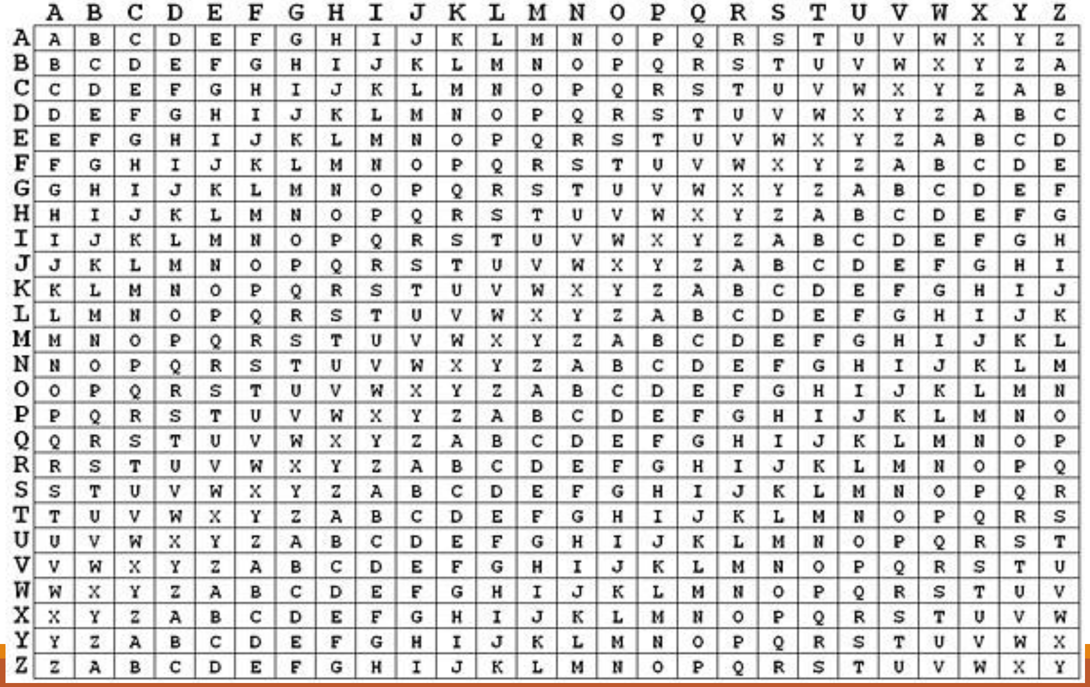
$p_i = (c_i - k_i) \bmod 26$

Ciphertext	k	e	n	t	u	t	g	b	o	x
Ciphertext value (E)	10	04	13	19	20	19	06	01	14	23
Key	b	e	s	t	b	e	s	t	b	e
Key value (K)	01	04	18	19	01	04	18	19	01	04
Plaintext value (P)	09	00	21	00	19	15	14	08	13	19
Plaintext	j	a	v	a	t	p	o	i	n	t

Example

Encrypt the plaintext “**now is the time for all good men**” using Vigenère cipher with keyword “**3 5 7 9 11**”

Repeated key	3	5	7	9	11	3	5	7	9	11	3	5	7	9	11	3	5	7	9	11	3	5	7	9	11
Plaintext	n	o	w	i	S	t	h	e	t	i	m	e	f	o	r	a	l	l	g	o	o	d	m	e	**n**
ciphertext	**q**	**t**	**d**	**r**	**d**	**w**	**m**	**l**	**c**	**t**	**p**	**k**	**m**	**x**	**c**	**d**	**q**	**s**	**p**	**z**	**r**	**i**	**t**	**n**	**y**



	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

Beaufort Cipher

$c_i = (k_i - p_i) \, mod \, n$

Question: Encrypt the plaintext "**now is the time for all good men**" using Beaufort cipher with key " computer"