Secret key or Symmetric key cryptography

□ B- transposition (permutation) ciphers:

A transposition cipher reorders symbols.

- Single Columnar Transposition
- Double Columnar Transposition
- Rotor Machine
- Steganography

□ 2- modern systems

1- Block cipher

- DES Algorithm
- AES Algorithm

2- Stream cipher

Public key or Asymmetric key Cryptography And number theory

3. Public key or Asymmetric key Cryptography

    -RSA Algorithm

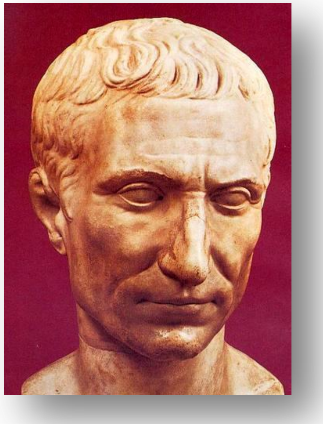
4.Number Theory

- GCD
- Inverse
- Exponential
- Route Transformation

Encryption Technique

- There are two basic building blocks of encryption techniques
  - Substitution
  - Transposition
- **Substitution encryption**
  - Is the classical encryption technique
  - In this method the letters of plain text are replaced by other letters or by numbers of symbol.
  - If plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Cont..



- **Caesar Cipher**
  - Is a known use of substitution cipher
  - Is the most simplest
  - Introduced by Julius Ceasar (Dictator, Roman Empire)
    - Example

plain: meet me after the toga party

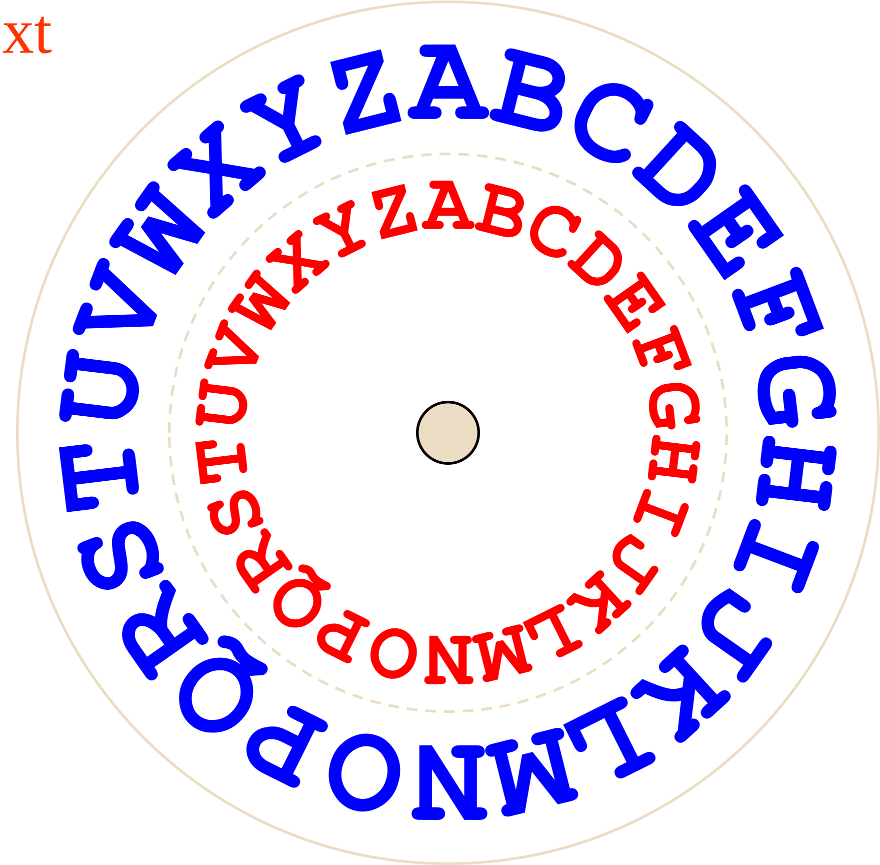
cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note: alphabet is wrapped around, so that the letter following Z is A

Caesar cipher Decoder Ring

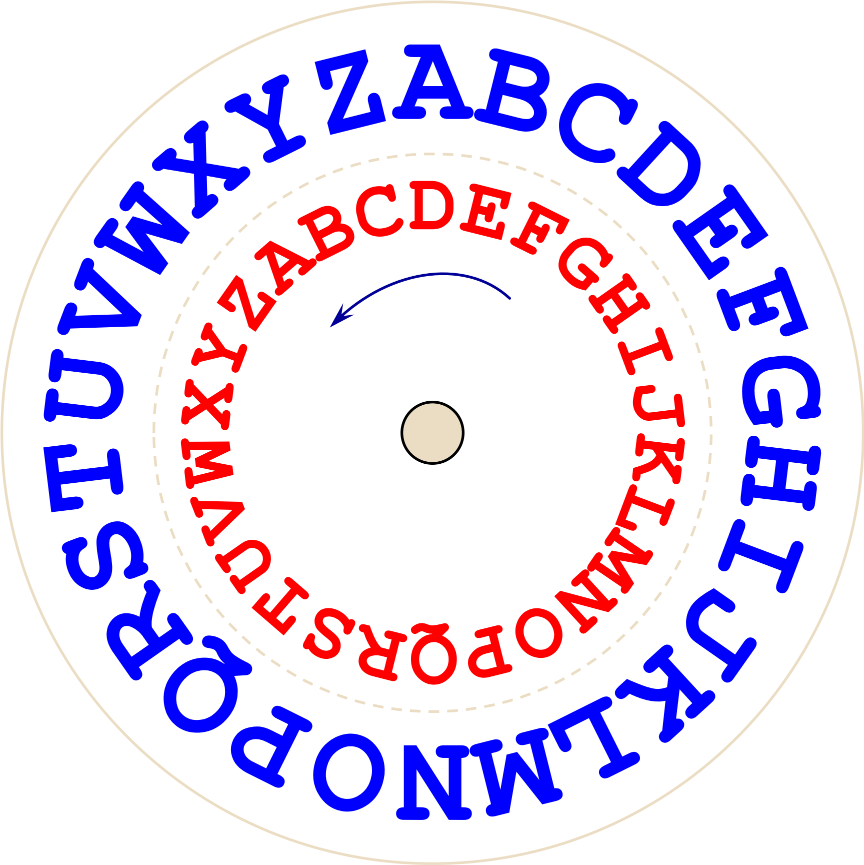
Outer: plaintext

Inner: ciphertext



The Caesar cipher

K=3



- Substitution

  plain: 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

  cipher: 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

- Let us assign number to each 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

- The Algorithm can be expressed as
  - For each plain letter ‘p’ substitute ciphertext letter ‘C’

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

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

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

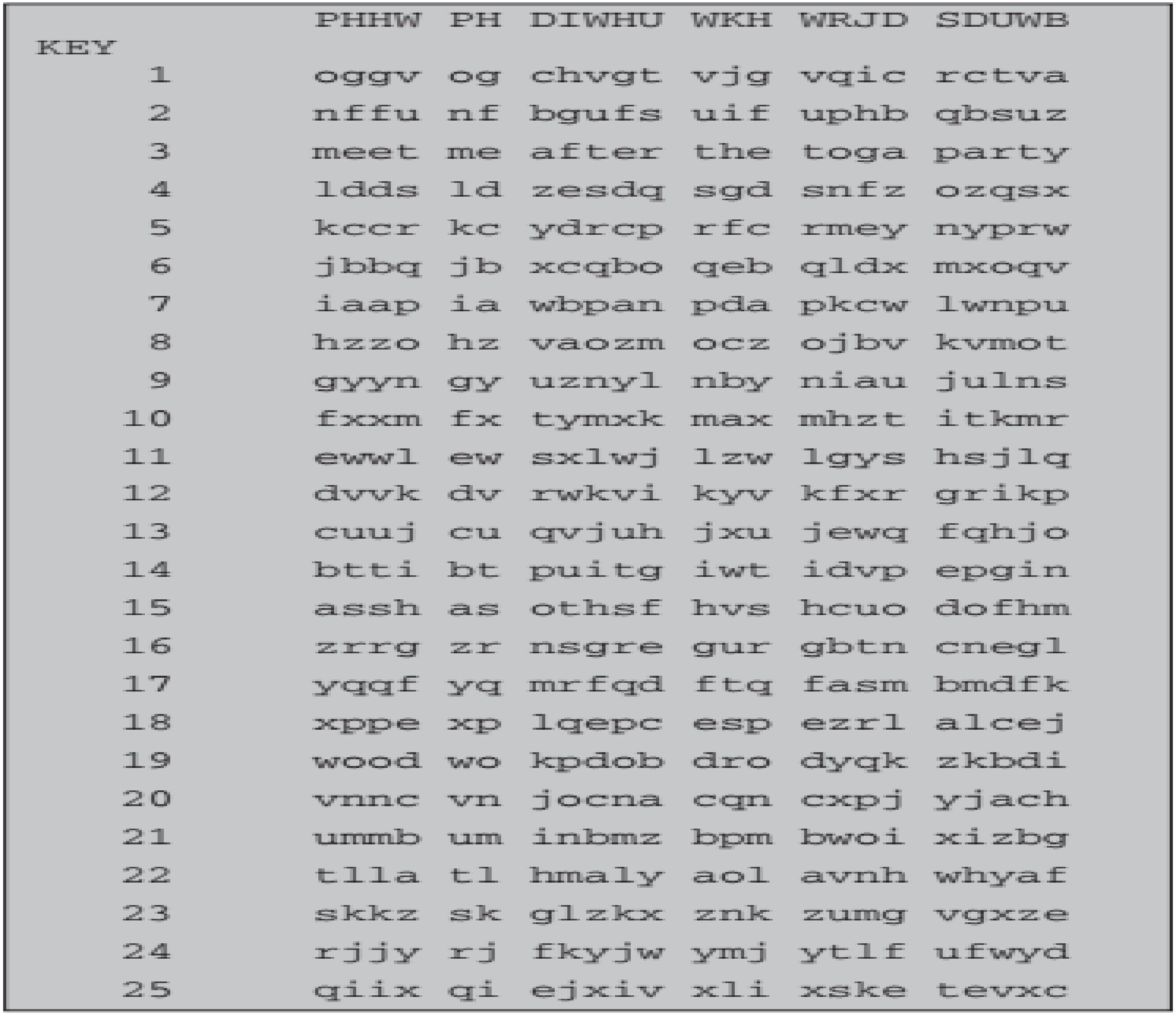
  - Where ‘k’ takes on a value in a range 1 to 25.

  - The Decryption algorithm is simply

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

- Example of Ceaser Cipher
  - Plain Text : hello how are u
  - Cipher text: khoor krz duh x

- Important
  - The encryption and decryption algorithms are known
  - There are only 25 keys to try
  - The language of the plain text is known and easily recognizable



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

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

Assignment

- Encrypt the message “ meet me tomorrow “ using a Ceasar cipher ,and the key is “how are you” .

Monoalphabetic Ciphers

□ Monoalphabetic Ciphers

- In this substitution cipher, each letter is replaced by another letter according to the cipher alphabet.
- Cipher Alphabet sequence for all 26 alphabets can be generated randomly.
- There are over 400,000,000,000,000,000,000,000,000 such rearrangements, which equivalent to (4 X 10^{26}) distinct cipher alphabets.
- Each cipher alphabet is known as a key.

Monoalphabetic Ciphers

- □ If an enemy could check one of these possible keys every second, it would take a long duration to check all of them and find the correct one.
- □ The simple brute force approach clearly will not work.

- Example
  - Encrypt the message “hello how are you” using Mono-alphabetic cipher .

Solution:-

Plain 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" }
Cipher Alphabet	{"Z", "Y", "X", "H", “I", "K" ,"D", "L", "O", "F", "G", "R", “E", "J", "V", "L", "N","M", "Q", "P", "S", "T", "U", "C", "B", "A" }

Note : key generation is random!

Plain text   : hello how are you – always in lower case.

Cipher Text : LIRRV LVU ZMI BVS – always in upper case.

Polyalphabetic Ciphers

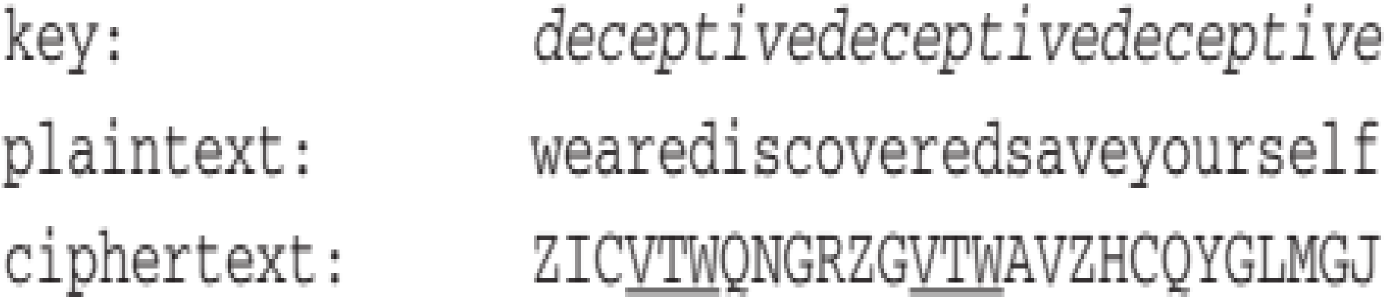
- Is the method to improve monoalphabetic cipher
- The general name of this approach is Polyalphabetic substitution cipher.
- Common feature
  - A set of related monoalphabetic substitution rules is used.
  - A key determines which particular rule is chosen for a given transformation.

VIGENERE CIPHER

- This cipher is given by **Blaise De Vigenere,** in sixteenth century, from the court of Henry III of France
- To aid in understanding the scheme and to aid in its use, a matrix known as the **Vigenre tableau** is constructed

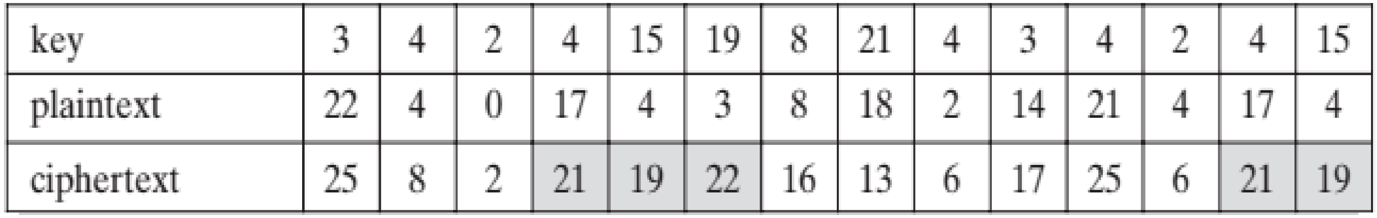
- Simplest polyalphabetic substitution cipher
- Effectively multiple Caesar ciphers (26 Caesar cipher)
- Key is multiple letters long K = k1 K2 ... kd
- ith letter specifies ith alphabet to use Fi(a)=a+ki mod n where n is the number of alphabet
- Use each alphabet in turn
- Repeat from start after d letters in message decryption simple works in reverse

- To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. For example, if the keyword is ***deceptive***, the message "***we are discovered save yourself***" is encrypted as:

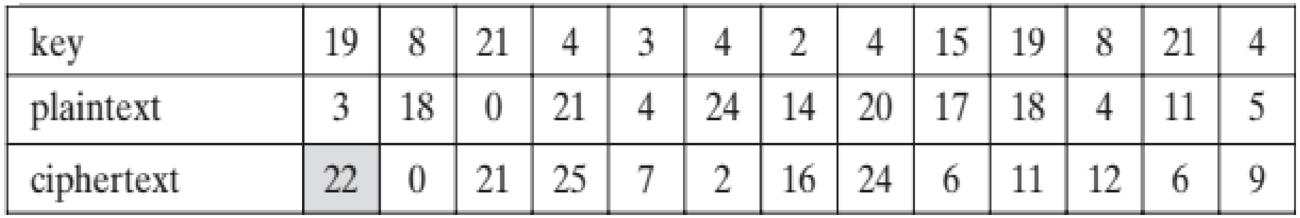


```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

- Expressed numerically, we have the following result.



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

PLAINTEXT LETTER

KEYWORD LETTER

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	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
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	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	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	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	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	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	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	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	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

- Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left.
- A normal alphabet for the plaintext runs across the top. The process of encryption is simple:
  - Given a key letter *x* and a plaintext letter y,
  - the ciphertext letter is at the intersection of the row labeled *x* and the column labeled y; in this case the ciphertext is V.
- Example
  - key: deceptivedeceptivedeceptive
  - plaintext: wearediscoveredsaveyourself
  - ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

- Decipherment
  - It is equally simple.
  - The key letter again identifies the row.
  - The position of the ciphertext letter in that row determines the column, and the plaintext letter is at the top of that column.
  - Example
    - Ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
    - Key : *deceptivedeceptivedeceptive*
    - *Plaintext :* wearediscoveredsaveyourself

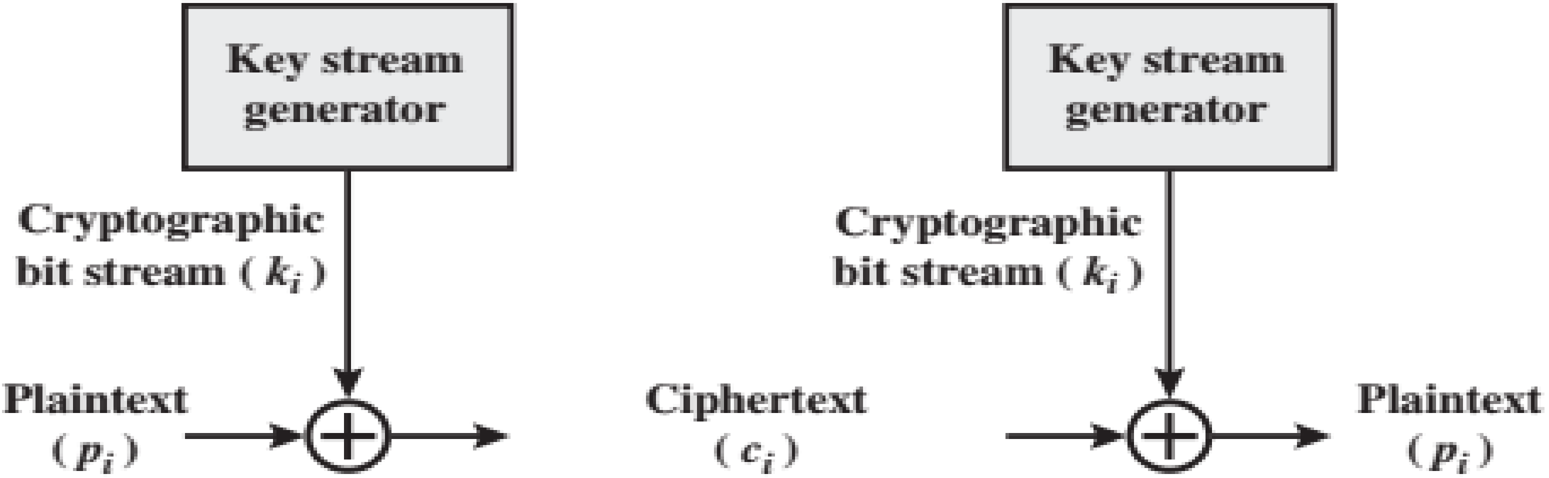
Assignment

- □ **Q:** How can we cryptanalyze the Viginer cipher?
- □ **Q:** Describe the ***Autokey system***, with example.

VERNAM CIPHER

- 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. The system works on binary data (bits) rather than letters. The system can be expressed succinctly as follows
- $ci=pi \oplus ki$
- where pi= ith binary digit of plaintext

- ki= ith binary digit of key
- ci= ith binary digit of ciphertext
- ⊕= exclusive-or (XOR) operation



- Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation:
- $pi = ci \oplus ki$

exclusive or Operator

a	b	$c = a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Example

- message =‘IF’
- then its ASCII code =(1001001 1000110)
- key = (1010110 0110001)
- *Encryption:*
  - 1001001 1000110 plaintext
  - 1010110 0110001 key
  - 0011111 1110110 ciphertext
- *Decryption:*
  - 0011111 1110110 ciphertext
  - 1010110 0110001 key
  - 1001001 1000110 plaintext

Playfair Cipher

- Best known as multiple-letter encryption cipher.
- It is based on the use of 5x5 matrix of letters constructed using a ‘keyword’
- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, then filling in the remainder of the matrix with the remaining letters of plain alphabet.

Charles Wheatstone

- The letters I and J count as one letter.
- Plaintext is encrypted two letters at a time, according to the following rules
- Example: keyword = ‘KEYWORD’

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

- Process
  1) Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that
     - **Secret message** would be treated as **se cr et me sx sa ge**.

  2)Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
     - For example, **cr** is encrypted as **RD**.

3) Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.

- For example, **ge** is encrypted as **ND**.

4) Otherwise, form a rectangle, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

- Thus, **se** becomes **NO** ,et becomes **KU, me becomes** NK, sa becomes PC and sx becomes QZ.

advantages and dis

- □ Key = welcome
- □ please meet me tomorrow

w e l c o

m a b d f

g h i/j k n

p q r s t

u v x y z

- □ pl ea se me et me to mo rr ow
- □ pl ea se me et me to mo rx ro wx
- □ rw ah qc aw oq aw zf fw xl tl lu

Transposition Technique

Transposition ciphers encrypt plaintext by moving small pieces of the massage around

- They are rarely used
- They differ form substitution ciphers in following way
    - In transposition cipher the letter of plaintext are shifted about to form cryptogram
    - This can be done in number of ways, and there are some system where whole words are transposed.

Rail fence cipher

- The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example, to encipher the message “meet me after the toga party” with a rail fence of depth = 2, we write the following:

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

- MEMATRHTGPRYETEFETEOAAT
- This sort of thing would be trivial t cryptanalyze.

Row Transposition cipher

- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example, plain text :“attack postponed until two am”
- Key: 4 3 1 2 5 6 7
- Plain text : 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
- Cipher text: TTNAAPTMTSUOAODWCOIXKNLYPETZ

- Thus, in this example, the key is 4312567. To encrypt, start with the column that is labeled 1, in this case column 3.Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7. A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is reencrypted using the same algorithm,

- Key: 4 3 1 2 5 6 7
- Input: t t n a a p t

  m t s u o a o

  d w c o i x k

  n l y p e t z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ