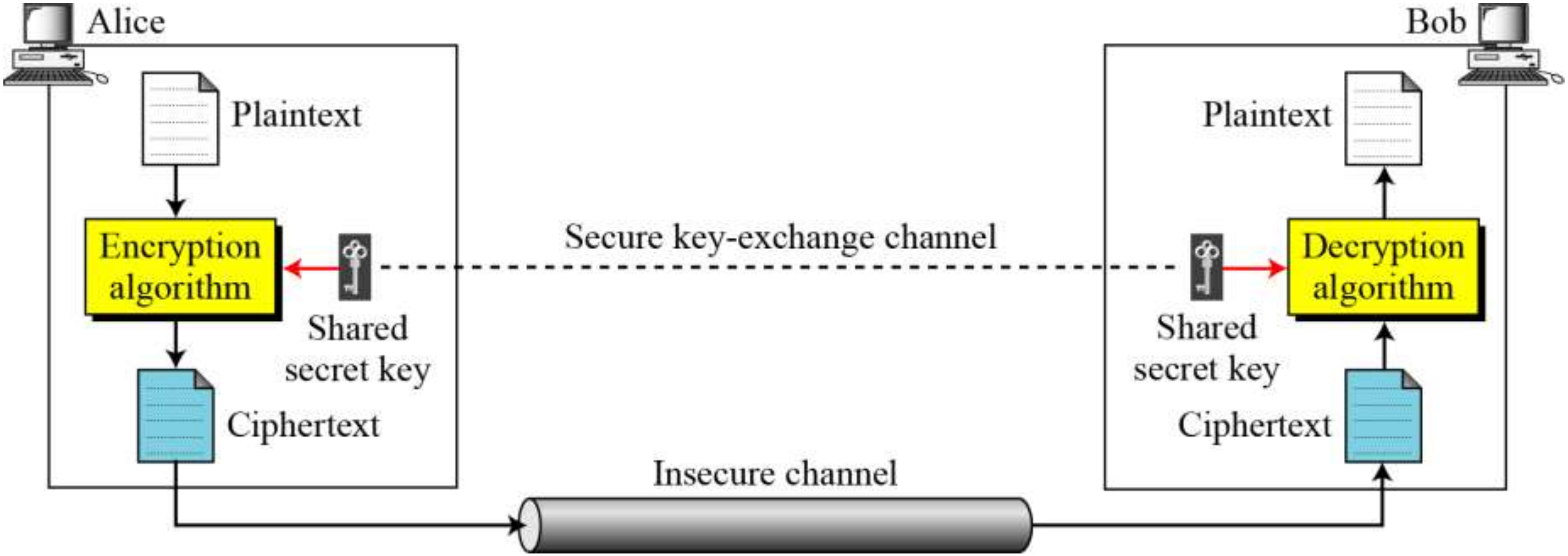
Traditional
Symmetric-Key Ciphers

Symmetric Key Cipher Model



Symmetric Key Cipher Model (Contd…)

If P is the plaintext, C is the cipher text, and K is the key, Then we represent the encryption done by Alice as:

$$\textbf{Alice: } C = E_k (P)$$

Similarly, for a given C , and shared key K, we represent the decryption done by Bob as:

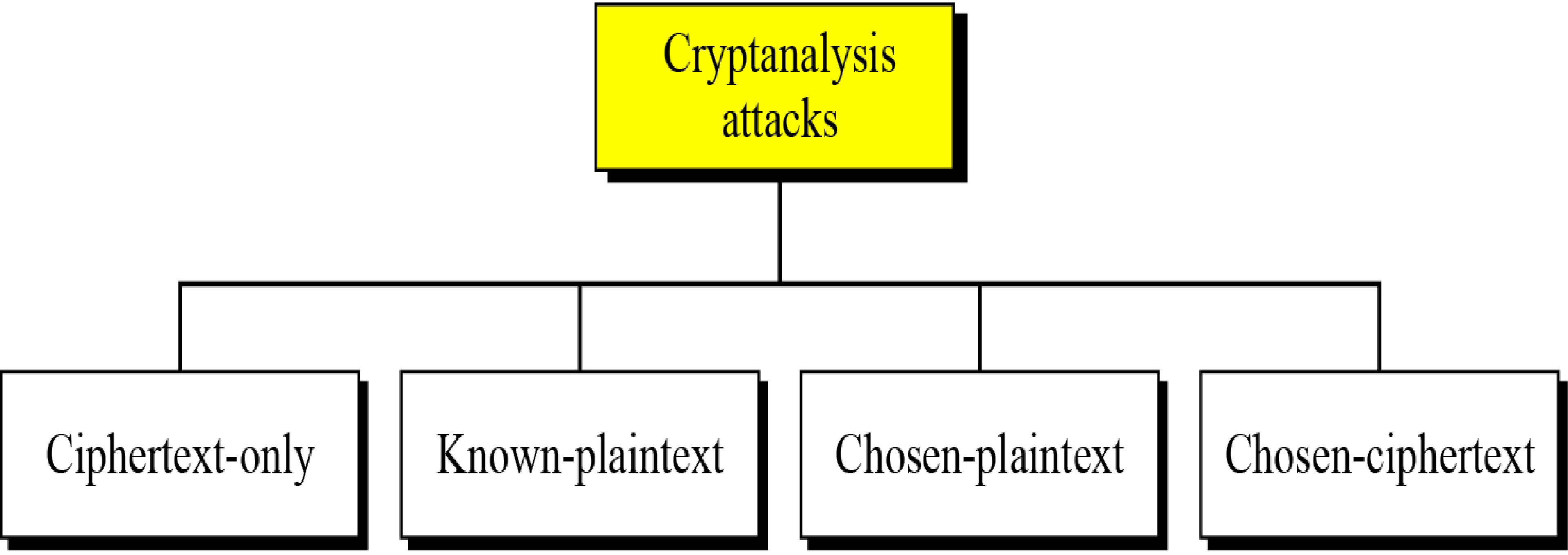
$$\textbf{Bob: } P_1 = D_k (C) = D_k (E_k(P)) = P$$

Kerckhoff's Principle

- Always assume that the adversary Eve, knows the encryption/decryption algorithm.
- So, the resistance of the cipher must be based only on the secrecy of the key.

Cryptography vs Cryptanalysis

As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking the codes.



Cryptanalysis

Cipher-text only attack (COA):

Here, the attacker is assumed to have access only to a set of ciphertexts. No knowledge of plain text.

Known plaintext attack (KPA):

Here, the attacker has a set of ciphertexts to which he knows the corresponding plaintext.

Chosen plaintext attack (CPA):

Here, the attacker can obtain the ciphertexts for arbitrary plaintexts he chooses.

Chosen ciphertext attack (CCA):

Here, the attacker can obtain the plaintexts corresponding to an arbitrary set of ciphertexts he chooses.

Type of Attack	Known to Cryptanalyst
Cipher text only	• Encryption algorithm • Cipher text to be decoded
Known plain text	• Encryption algorithm • Cipher text to be decoded • One or more plain text-cipher text pairs formed with the secret key
Chosen plain text	• Encryption algorithm • Cipher text to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Chosen cipher text	• Encryption algorithm • Cipher text to be decoded • The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key
Chosen text	• Encryption algorithm • Cipher text to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key • The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key

SUBSTITUTION CIPHERS

- It is an encryption technique which replaces/substitutes one symbol of the plain text with another symbol.
- There are 3 types of Substitution ciphers :
  - Additive cipher
  - Multiplicative cipher
  - Affine cipher
- Also we can classify this technique as:
  - Monoalphabetic Substitution cipher
  - Polyalphabetic Substitution cipher

Monoalphabetic vs Polyalphabetic

Note

- In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
- But in polyalphabetic substitution, that relationship is one-to-many.

Monoalphabetic vs Polyalphabetic Substitution

Example 1

The following shows a plaintext and its corresponding ciphertext. The cipher is monoalphabetic because both *l*’s are encrypted as *O*’s.

Plaintext: hello **Ciphertext:** KHOOR

Example 2

The following shows a plaintext and its corresponding ciphertext. The cipher is not monoalphabetic because each *l* is encrypted by a different character.

Plaintext: hello **Ciphertext:** ABNFZ

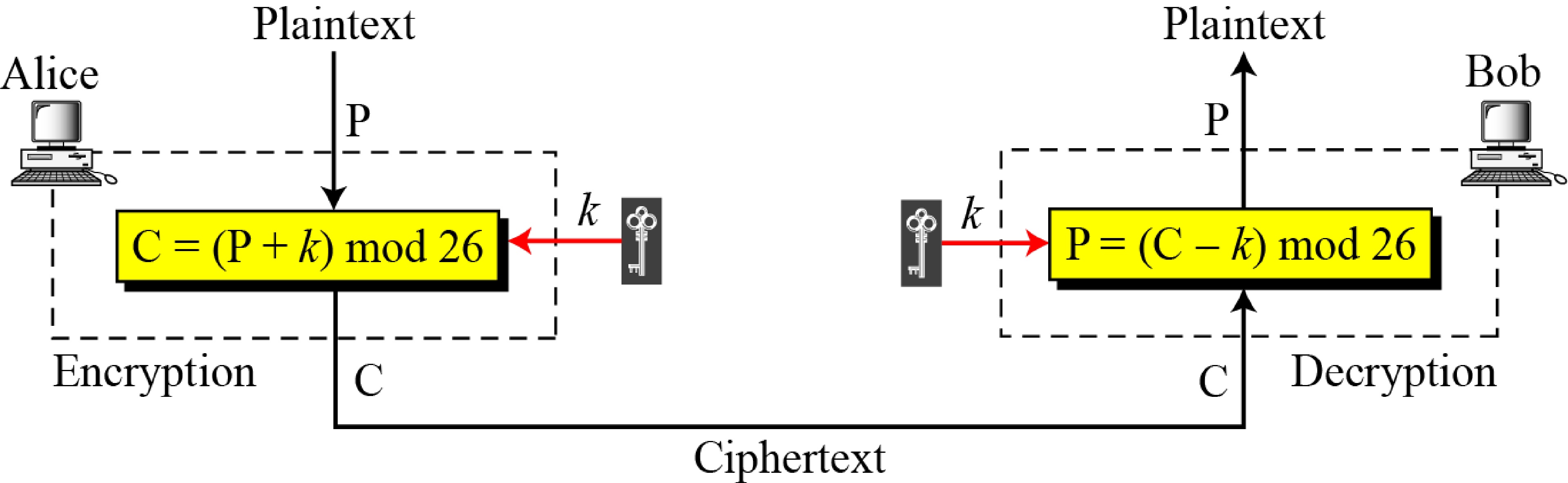
Additive Cipher

- The simplest substitution cipher is the additive cipher.
- This cipher is sometimes called a shift cipher or a Caesar cipher, but the term additive cipher better reveals its mathematical nature.

Table : ***Plaintext and cipher text in Z_{26}***

Plaintext →	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 →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Additive Cipher *(Contd…)*



Note

- When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.

Additive Cipher*(Contd…)*

Example

Use the additive cipher with key = 15 to encrypt the message "hello".

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Additive Cipher*(Contd…)*

Example

Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Solution

We apply the decryption algorithm to the plaintext character by character as follows:

Ciphertext: W $\rightarrow$ 22	Decryption: (22 – 15) mod 26	Plaintext: 07 $\rightarrow$ h
Ciphertext: T $\rightarrow$ 19	Decryption: (19 – 15) mod 26	Plaintext: 04 $\rightarrow$ e
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: D $\rightarrow$ 03	Decryption: (03 – 15) mod 26	Plaintext: 14 $\rightarrow$ o

Brute force attack or exhaustive key search

To try all possible keys of the domain to break the cipher.

Eve has intercepted the ciphertext "UVACLYFZLJBYL". Show how she can use a brute-force attack.

Solution

Eve tries keys from 1 to 7. And he got the result at K=7.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

Statistical attack

Based on the inherent properties of the language of plaintext

Table : *Frequency of occurrence of letters in English*

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Table : *digrams and trigrams*

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Statistical attack (*Contd…)*

Example

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

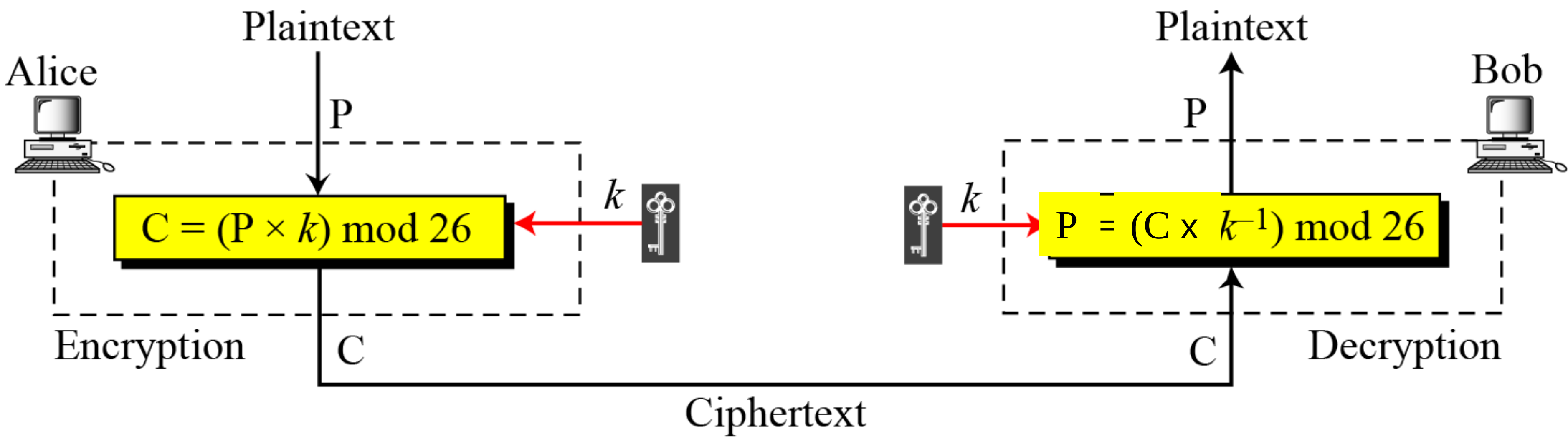
XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4.

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Multiplicative Ciphers



Note

- In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26}
- But, the key is an integer in Z_{26}*.

Multiplicative Ciphers*(Contd…)*

Example 1

What is the key domain for any multiplicative cipher?

Solution The key needs to be in Z_{26}*. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

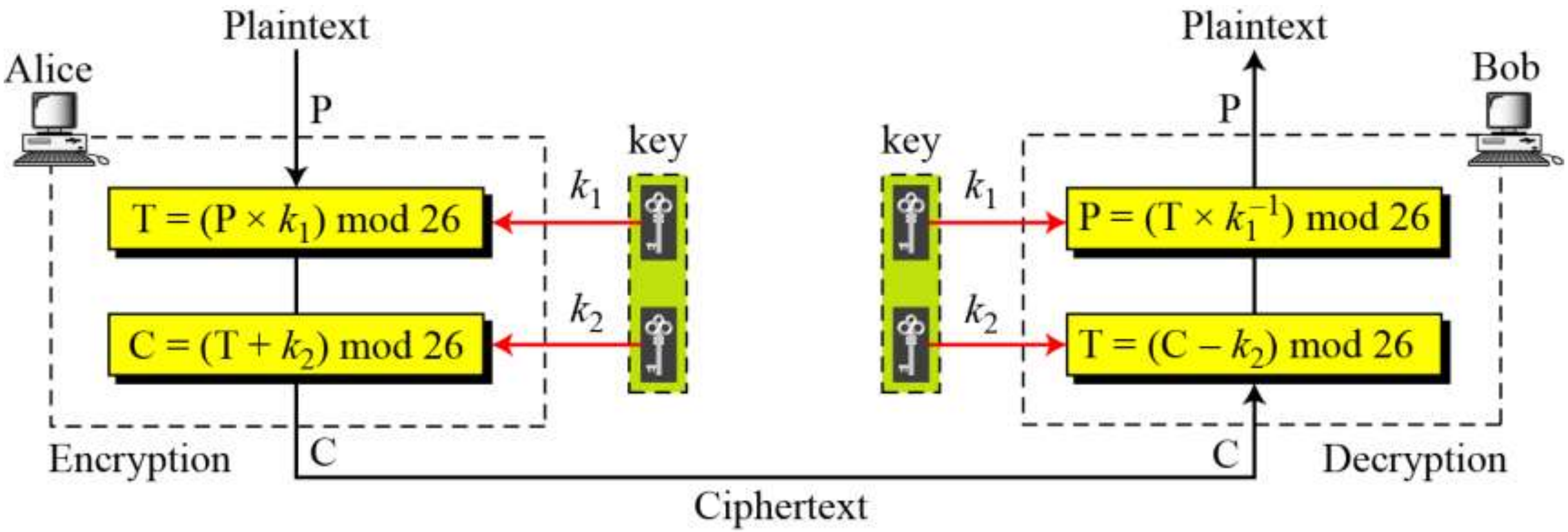
Example 2

Use a multiplicative cipher to encrypt the message "hello" with a key of 7.

Plaintext: h $\rightarrow$ 07	Encryption: (07×07) mod 26	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: (04×07) mod 26	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: (11×07) mod 26	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: (11×07) mod 26	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: (14×07) mod 26	ciphertext: 20 $\rightarrow$ U

Affine Ciphers

- It is a combination of additive and multiplicative ciphers with a pair of keys.



$$C = (P \times k_1 + k_2) \bmod 26 \qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

Affine Ciphers(Contd…)

Example

What is the key domain and its size in affine cipher ?

The affine cipher uses a pair of keys in which the first key is from Z_{26}* and the second is from Z_{26}. The size of the key domain is $26 \times 12 = 312$.

Example

Use affine cipher to encrypt the message "hello" with the key pair (7, 2).

P: h → 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 → W

Affine Ciphers(Contd…)

Example

Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in mod 26.

C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1})$ mod 26	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1})$ mod 26	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1})$ mod 26	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1})$ mod 26	P:11 $\rightarrow$ l
C: W $\rightarrow$ 22	Decryption: $((22 - 2) \times 7^{-1})$ mod 26	P:14 $\rightarrow$ o

Note

- 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 $k_2 = 0$.

Monoalphabetic Substitution Cipher

Is there any drawback of Affine cipher?

- Affine ciphers including additive and multiplicative ciphers have small key domains, hence very vulnerable to brute-force attack.

- A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character.
- Alice and Bob can agree on a table showing the mapping for each character.

Monoalphabetic Substitution Cipher(Contd…)

Figure : An example key for monoalphabetic substitution cipher

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

Cryptanalysis: ***What is the Size of the key space ?***

$26! = 4 \times 10^{26}$,hence extremely difficult to brute force attack,

But easy to statistical attack(?)

Playfair Cipher

- A multiple-letter encryption cipher developed by Charles Wheatstone, but named after his friend Baron Playfair who promoted it.
- The secret key in this cipher is made by a 5x5 matrix(I and J considered as one element).
- The encryption algo. takes a pair of letters (digrams) form the plain text and translates into ciphertext pair.
- If two letters in the pair is same, then insert a bogus letter.
- The cipher uses 3 rules for encryption:

Playfair Cipher(Contd…)

- If the two letters in a pair are located in the same row of the secret key, the corresponding encrypted character for each letter is the next letter to the right in the same row(with wrapping to the beginning)
- If the two letters in a pair are located in the same column of the secret key, the corresponding encrypted character for each letter is the letter beneath it in the same column(with wrapping to the beginning)
- If the two letters in a pair are not in the same row or column of the secret key, the corresponding encrypted character for each letter is a letter that is in its own row but in the same column as the other.

Playfair Cipher(Contd..)

Secret Key =

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

Example

Encrypt the plaintext “hello” using the key in above figure.

he $\rightarrow$ EC lx $\rightarrow$ QZ lo $\rightarrow$ BX

Plaintext: hello Ciphertext: ECQZBX

Cryptanalysis: Its key domain is 25!

- Hence difficult for brute force attack.
- Although it hides the single letter frequency, but digram frequency is available for the attacker.

Hill Cipher

Invented by Lester S. Hill.

Here the plaintext is divided into equal-sized(m) blocks. The key is a square matrix of size m x m , *where m is the block size*.

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

Note:

Encryption: ***C=PK***

Decryption: ***P=CK***$^{-1}$***,***
K is invertible.

The key matrix in the Hill cipher needs to have a multiplicative inverse.

Hill Cipher (Contd…)

If plain text $P = \{P_1, P_2, \ldots, P_m\}$ and
cipher text $\mathbf{C} = \{C_1, C_2, \ldots, C_m\}$ *then we have:*

$$
\begin{aligned}
C_1 &= P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1} \\
C_2 &= P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2} \\
&\cdots \\
C_m &= P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm}
\end{aligned}
$$

Cryptanalysis: Brute force attack is difficult as the key is a matrix of size mxm.

- And each entry in the matrix is chosen out of 26 values,
- Hence the size of the key domain is $26^{m \text{x} m}$.
- It also doesn't preserve the letter frequencies.

Assignment-1

(Submission deadline: 09.09.2023)

1. Show the process of encryption and decryption for the plaintext “play" by using the Hill cipher with the key $K=\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$
2. Find the multiplicative inverse of 15 in Z_{26} by using Extended Euclidean Algorithm (show all the steps involved in a table).

Polyalphabetic Substitution Ciphers

- A better method than Monoalphabetic substitution.
- Here, each occurrence of a character in plaintext may have a different substitute in cipher text.
- The relationship between a character in the plaintext to a character in the ciphertext is **one-to-many.**
- All the ciphers has some common techniques:
  - *A set of related monoalphabetic substitution rules is used*
  - *A key determines which particular rule is chosen for a given transformation*

Vigenere Cipher

- It is a polyalphabetic cipher designed by Blaise de Vigenere, French Mathematician (16th century)
- Here the key stream is a repetition of an initial secret key stream of length *m*
- Let the plaintext P = $p_0, p_1, p_2, \ldots, p_{n-1}$ and
- Key consisting of the sequence of letters K = $k_0, k_1, k_2, \ldots, k_{m-1}$, where $m < n$.
- Then the ciphertext letters C = $C_0, C_1, C_2, \ldots, C_{n-1}$ is calculated as follows:

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$

- Similarly, the plaintext can be calculated as

$$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

Vigenere Cipher (*Contd…*)

Example

Encrypt the message "She is listening" using the 6-character key "PASCAL".

The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed)

Plaintext →	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 →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Vigenere Cipher (*Contd…)*

Cryptanalysis: Can we say Vigenere cipher is secure ?

- The attacker has to know the Key length to attack.
- Once he knows the key length (say *m*), then he can apply frequency analysis of plaintext language to attack each of the *m* monoalphabetic ciphers.
- For example, with the keyword PASCAL, the letters in positions 1, 7, 13, and so on are all encrypted with the same letter of the Key.
- Key length can be predicted, *if there occurs two identical sequences of plaintext letters , as they will generate identical ciphertext sequences.*

Another *Example* *of* Vigenere Cipher

Plain Text (P): ***we are discovered save yourself***

Key (K) : ***deceptive***

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

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

Autokey Cipher

- The periodic nature of the keyword can be eliminated by using a non-repeating keyword that is as long as the message itself.
- So, Vigenere proposed an autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key.

$P = P_1P_2P_3 \ldots$ $\quad C = C_1C_2C_3\ldots$ $\quad k = (k_1, P_1, P_2, \ldots)$

Encryption: $C_i = (P_i + k_i) \bmod 26$ $\quad$ Decryption: $P_i = (C_i - k_i) \bmod 26$

Autokey Cipher (Contd…)

Example

Plain Text (P): ***we are discovered save yourself***

Key (K) : ***deceptive***

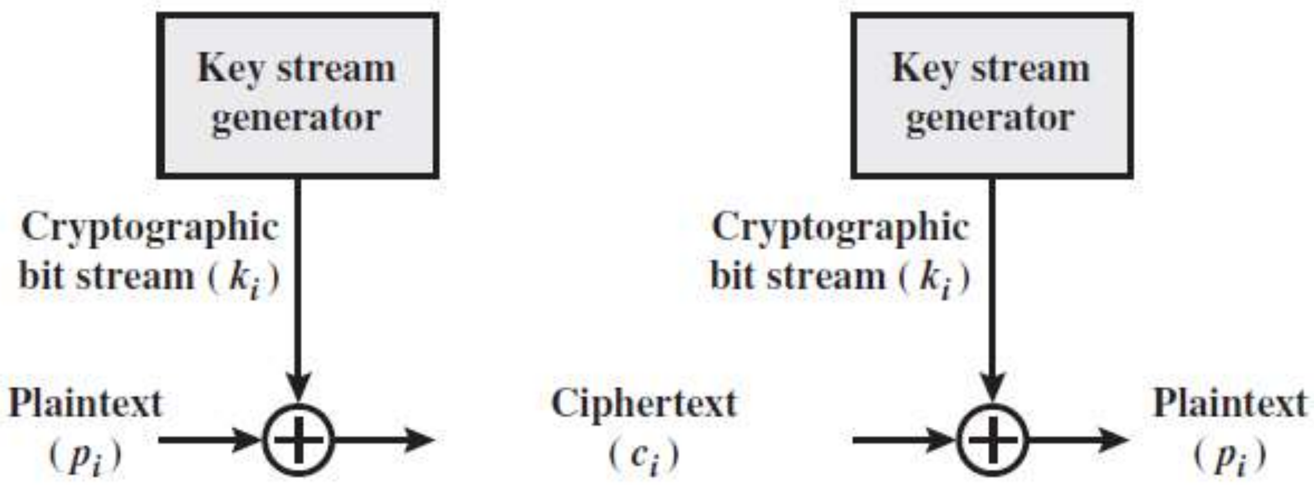
key:	*deceptivewearediscoveredsav*
plaintext:	wearediscoveredsaveyourself
ciphertext:	ZICVTWQNGKZEIIGASXSTSLVVWLA

***Cryptanalysis* :**

Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied.

Vernam Cipher

- Introduced by an AT&T engineer Gilbert Vernam in 1918.
- He proposed to choose a very long Key that has no statistical relationship to the plaintext.
- His system works on binary data (bits) rather than letters



Vernam Cipher (Contd…)

- So the Encryption process is given by:

$$c_i = p_i \oplus k_i$$

where p_i = ith binary digit of plaintext

k_i = ith binary digit of key

c_i = ith binary digit of ciphertext

$\oplus$ = exclusive-or (XOR) operation

- Because of the properties of the XOR, decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$

One-Time Pad

- It was an improvement over Vernam’s cipher.
- Vernam’s scheme, was using the key from a punched paper tape which was running in loop.
- So, a key was used again when the tape completed a cycle.
- Joseph Mauborgne (Army Signal Corp officer), proposed an improvement to the Vernam cipher
- He suggested to use a random key as long as the size of the message, so that the key need not be repeated.
- This is the only cryptosystem that exhibits **perfect secrecy**.

One-Time Pad (Contd…)

- The key is to be used to encrypt and decrypt a single message, and then it is discarded.
- Each new message requires a new key of the same length as the new message.
- Therefore, it is called one-time pad, and has been proved unbreakable.
- Drawbacks:
  - There is the practical problem of creating large number of random keys.
  - Difficulty in key distribution and protection

TRANSPOSITION CIPHERS

- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- Therefore, it only transposes or reorders the symbols.
- Two types: keyless or keyed (transposition cipher)

Keyless Transposition Cipher *(Rail Fence Cipher)*

- The plaintext is arranged in two lines as a zigzag pattern
- The ciphertext is created reading the first line and then the second line.
- After receiving the ciphertext, the receiver divides it into two lines from the middle and then read the characters in zigzag.

Example

- Let the plain text is: m e e t m e t o n i g h t
- Encryption:
  - Arrange it in zigzag pattern:
  - m e m t n g t
  - e t e o i h
  - Then read line by line.
- So the cipher text is: M E M T N G T E T E O I H
- Decryption:
  - Divide the cipher text into two parts from the middle:
  - M E M T N G T
  - E T E O I H
  - Then read in zig-zag style.

TRANSPOSITION CIPHERS (contd…)

Keyed Transposition Cipher:

- The drawback of keyless transposition is that, it has only two rows (fixed).
- So, the cryptanalysis will be very easy for the attacker.
    - only he has to know that rail fence has been used.

So, an improved method would be to use the **key**. It has the following three steps:

- First the plaintext is written into a table row by row.
- Then the permutation is done by using a Permutation Key (reordering the columns).
- Finally the new table is read column by column.

Example(Transposition Cipher)

Alice needs to send the message "Enemy attacks tonight" to Bob.

e n e m y   a t t a c   k s t o n   i g h t z

The key used for encryption and decryption is a permutation key, which shows how the characters are permuted assuming 5 columns

Encryption ↓

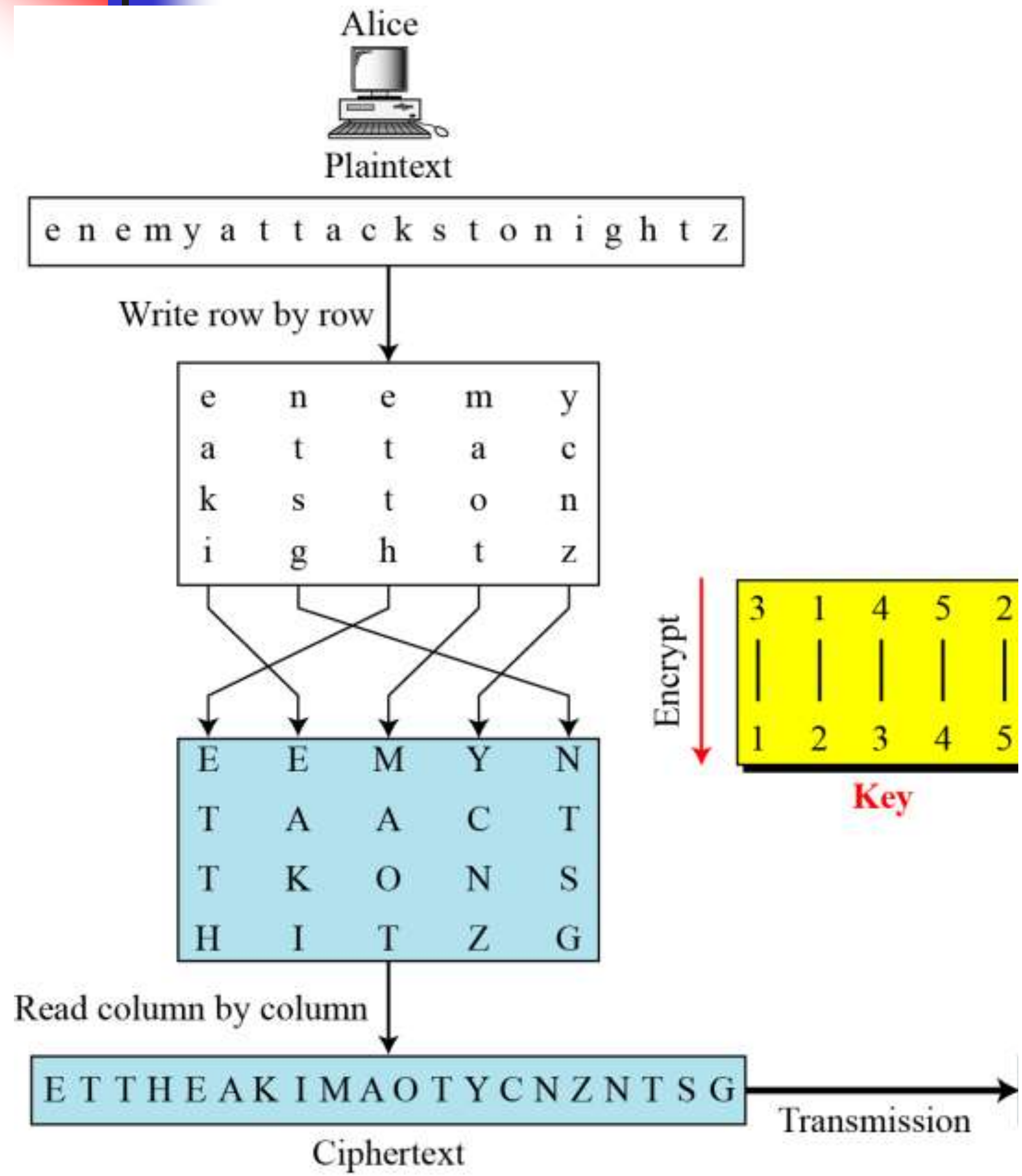
3	1	4	5	2
1	2	3	4	5

↑ Decryption

The permutation yields:

E E M Y N   T A A C T   T K O N S   H I T Z G

Example(with steps)



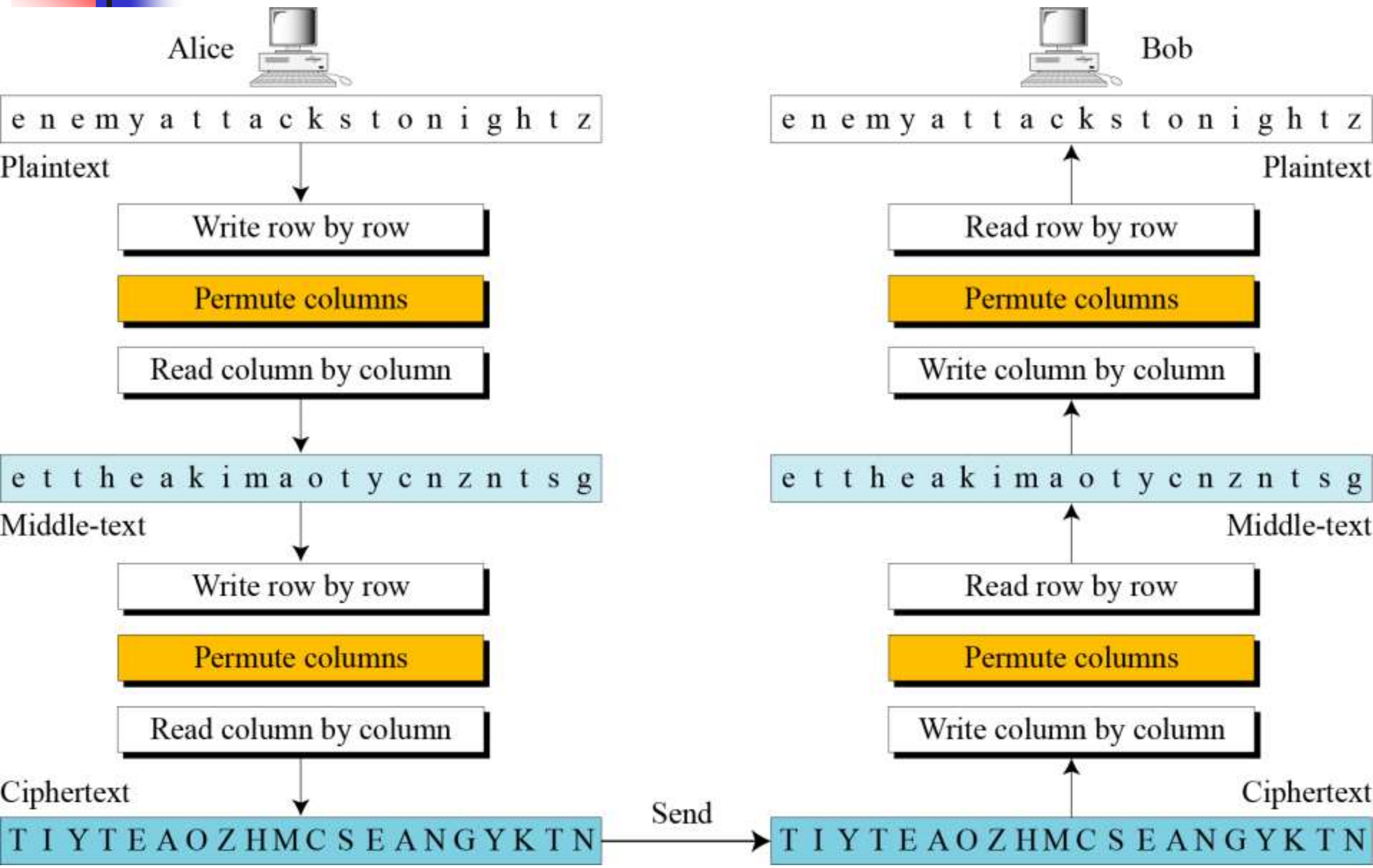
Expressing Permutation Table as Keys

- Encryption Key : Permutation key for encryption can be expressed as a sequence of column numbers of the plaintext with index values of those positions as column numbers in the ciphertext.
- Example: Let the encryption key is (3 1 4 5 2). First entry (3) means content of column 3 of plaintext becomes column 1 (1 is the index of that position) in ciphertext. Second entry (1) means column 1 in plaintext becomes column 2 in ciphertext and so on.
- Decryption Key : The decryption key for the above example will be (2 5 1 3 4). First entry(2) means content of column 2 in ciphertext would be column 1 (1 is the index of that position) in plaintext and so on.

Cryptanalysis of Transposition Cipher

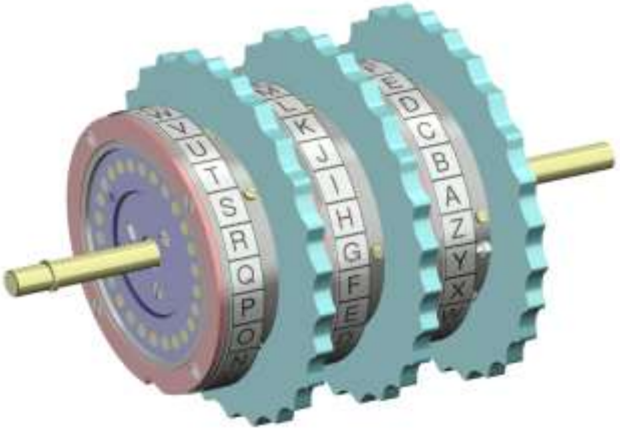
- Statistical attack is possible as it preserves the single letter frequency, but not the digrams & trigrams.
- Bruteforce attack although possible, but Key domain is huge
  i.e. $1!+2!+3!+\ldots+L!$, where, L is the length of the ciphertext.
- An attack called Pattern attack would be possible.
- It can be made more secure by using double transposition.

Double Transposition Ciphers



Rotor Cipher

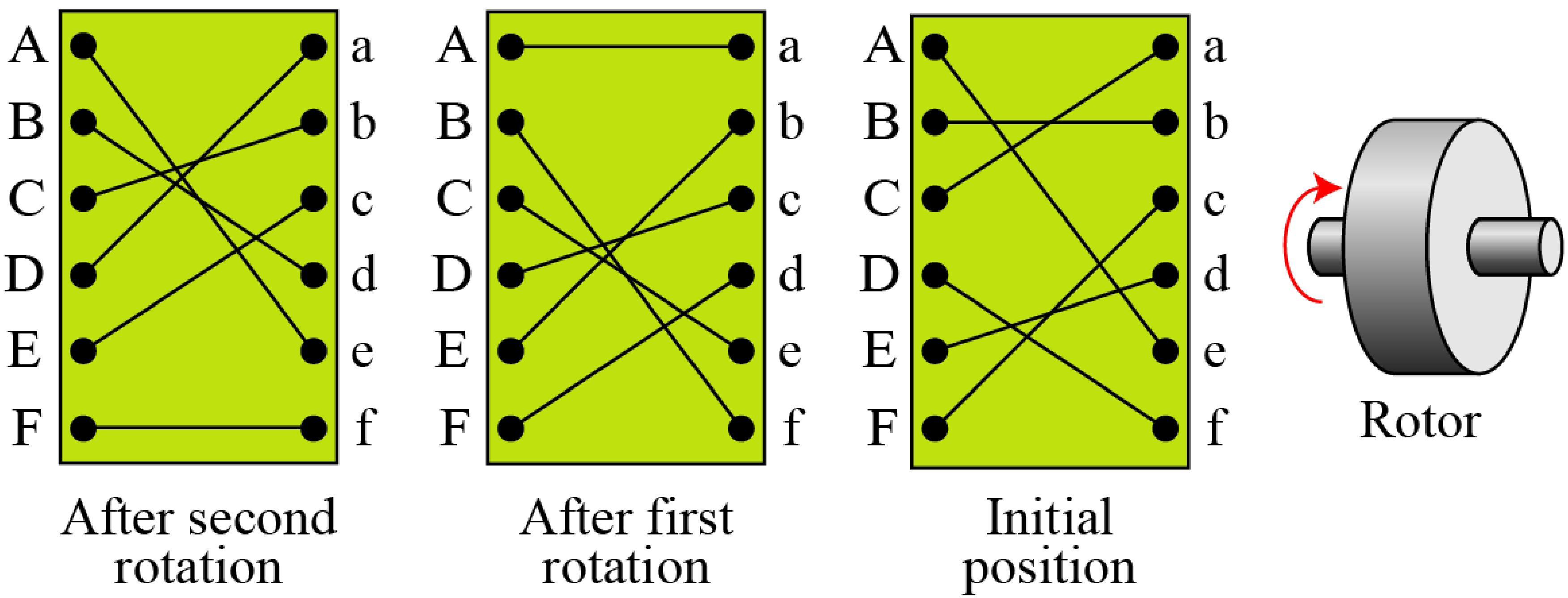
- It is based on the idea of multiple stages of monoalphabetic substitution.
- It is an electro-mechanical system having a set of independently rotating cylinders through which electrical pulses can flow.



- Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin.
- If we map each input and output pin with a letter of the alphabet, then a single cylinder defines a mono-alphabetic substitution.

Rotor Cipher

- But the mapping between plaintext and ciphertext characters changes after each rotation.
- Following is an example of rotations with 6 input and 6 output pins for simplicity.



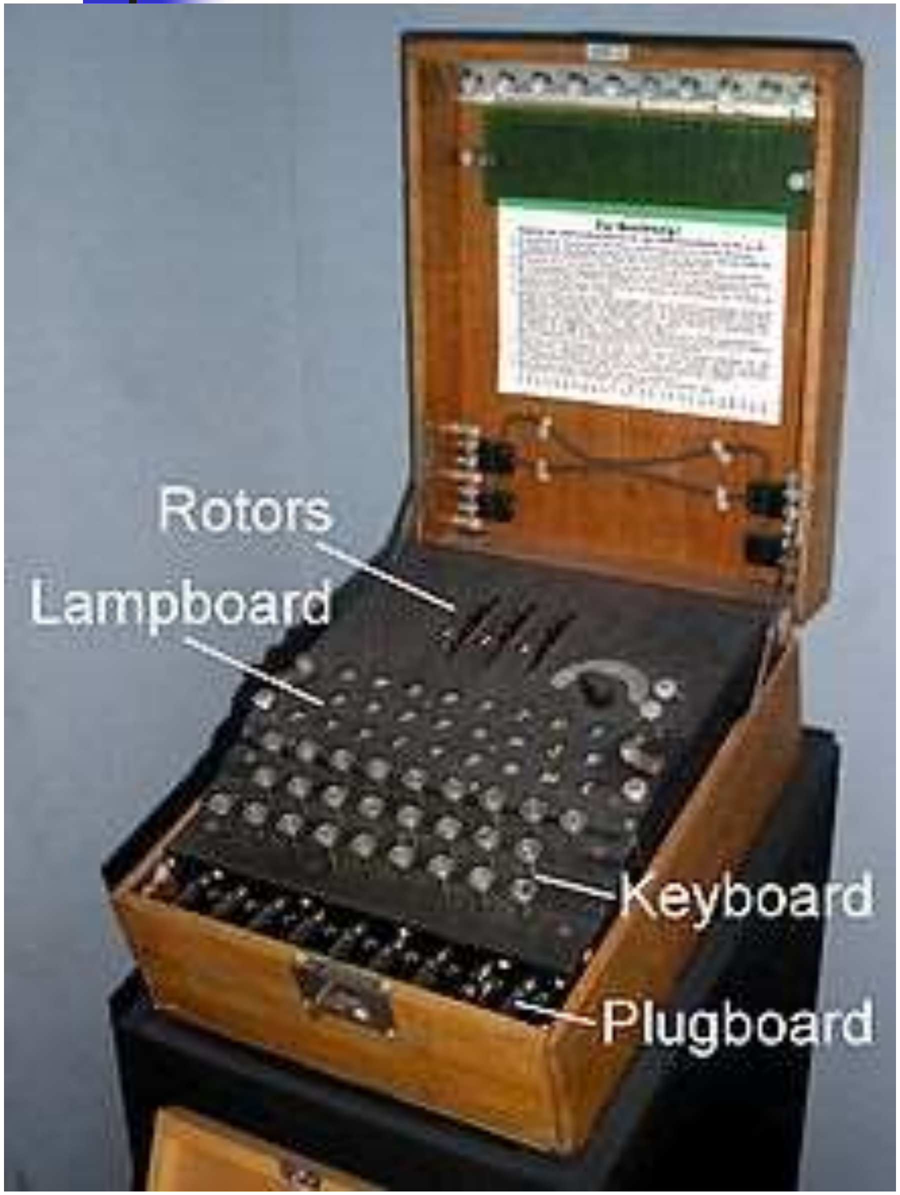
Rotor Cipher ***(Contd…)***

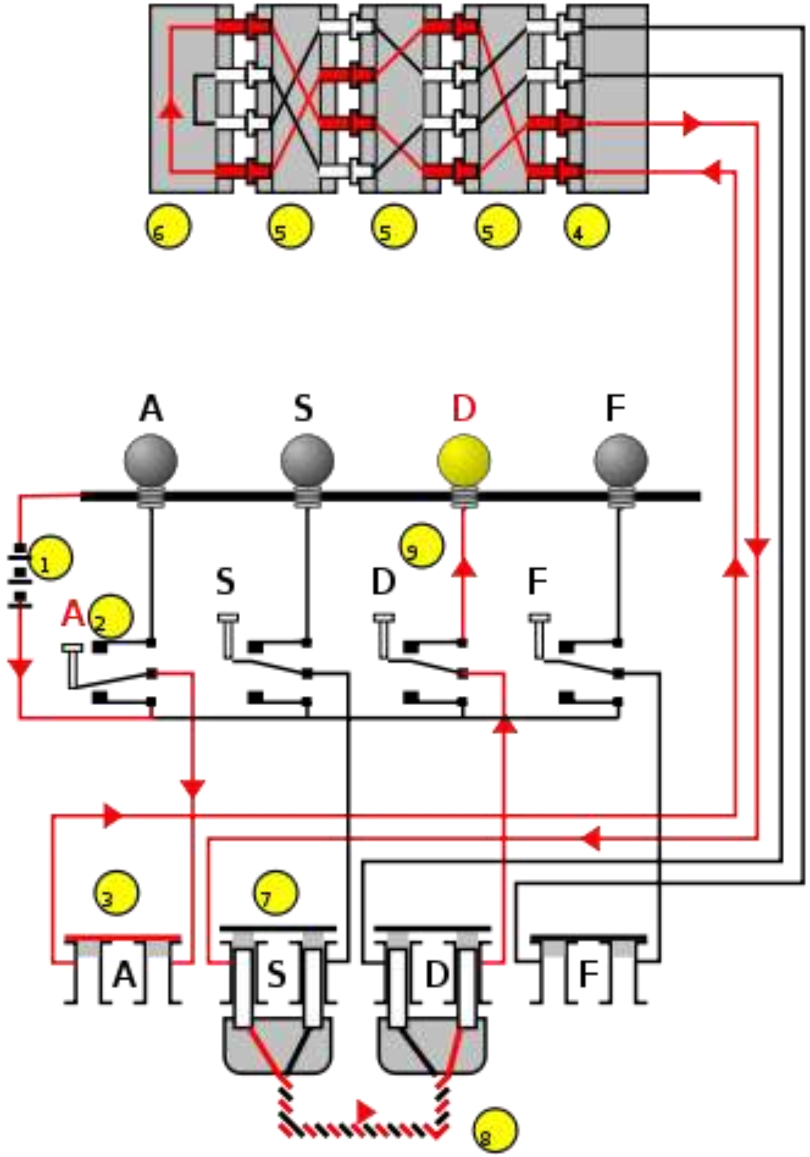
Cryptanalysis:

- If there is only one cylinder, then we have 26 different substitutions(keys).
- If you have two cylinders then we have 26*26 keys.
- If you have three cylinders then we have 26 * 26 * 26 = 17,576 different substitutions.
- So, by adding more cylinders the keys can be increased.
- Also it is much more resistive to statistical attack, when the no. of cylinders=**5** (11,881,376 substitutions)

Because of this, a modified version of Rotor cipher called Enigma Machine was extensively used by German Army during World War-II.

German Military's **Enigma Machine**





STREAM AND BLOCK CIPHERS

In a stream cipher, the encryption or decryption are done on one symbol(such as a character or bit) at a time.

- ***Additive Cipher***
- ***Monoalphabetic Substitution Cipher***
- ***Vigenere Cipher***

But, in a block cipher, a group of plaintext symbols of size m(m>1) are encrypted together creating a group of ciphertext of the same size.

Typically, a single key is used to encrypt the whole block.

- ***Playfair Cipher***
- ***Hill Cipher***