Information Assurance Security (IT352)

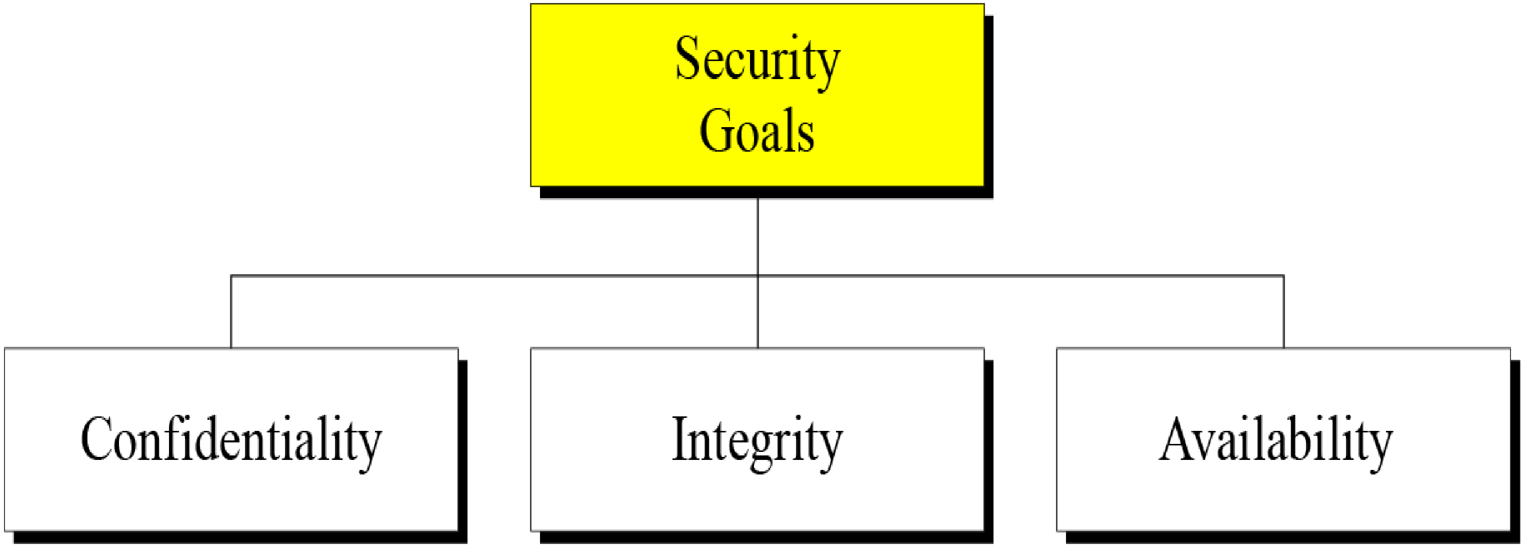
This material provides only overview of the topics covered in the class. Kindly refer text book to understand the concept in detail.

Note: Only this material is insufficient for mid-semester and end-semester examinations preparation.

Definition of Information Security

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

Security Goals



Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity

Information needs to be changed constantly. **Integrity** means that changes need to be done only by authorized entities and through authorized mechanisms.

Availability

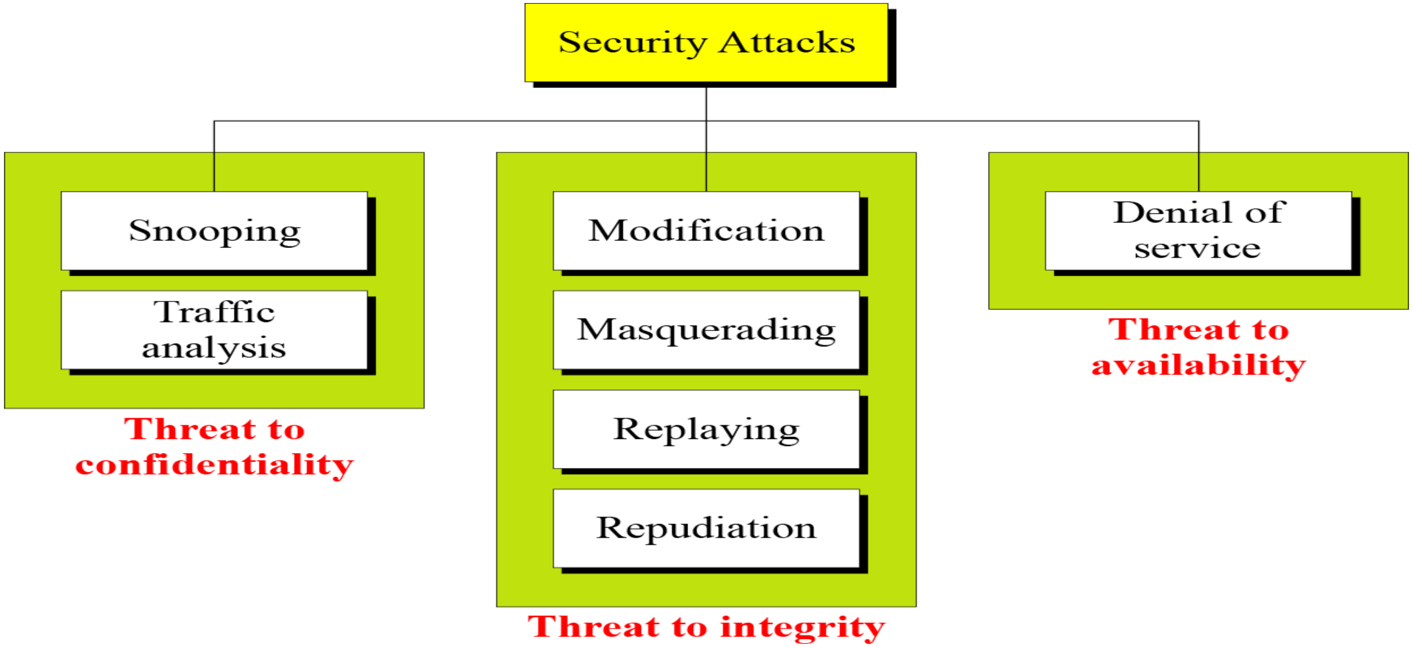
The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

Attacks Threatening Confidentiality
Attacks Threatening Integrity
Attacks Threatening Availability
Passive versus Active Attacks

Taxonomy of attacks with relation to security goals



Attacks Threatening Confidentiality

Snooping refers to unauthorized access to or interception of data.

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

Attacks Threatening Availability

Denial of Service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Attacks Threatening Integrity

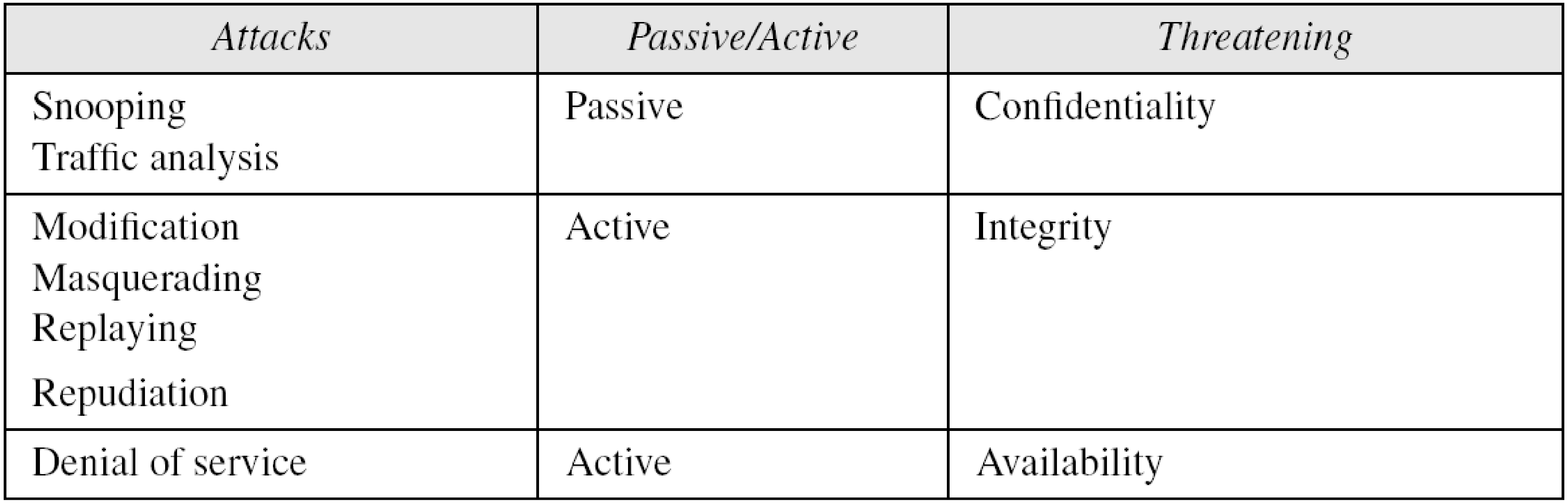
Modification means that the attacker intercepts the message and changes it.

Masquerading or **spoofing** happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Categorization of Passive and Active Attacks



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

SERVICES AND MECHANISMS

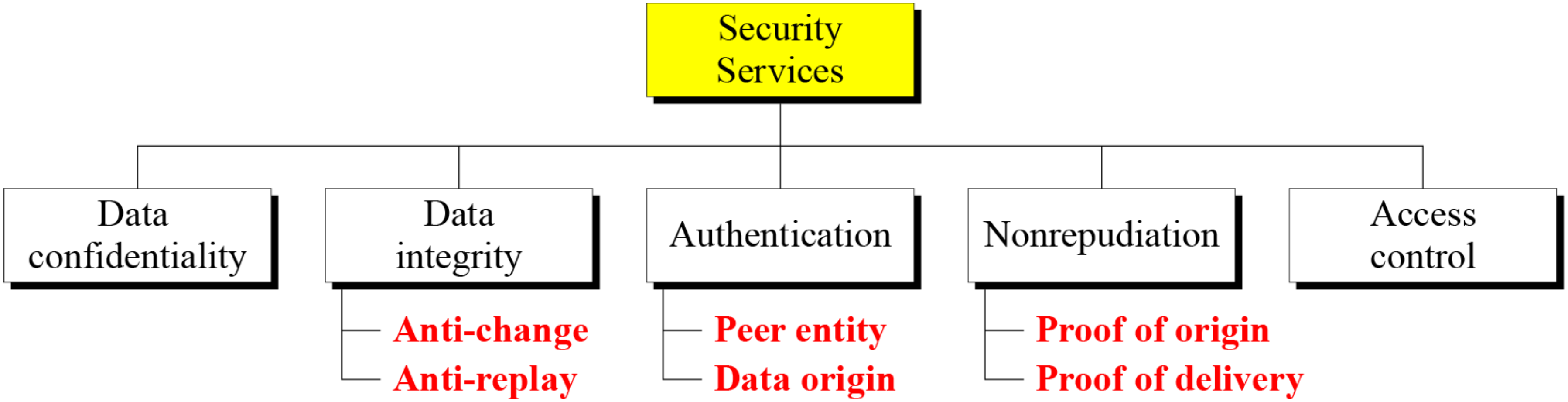
ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..

Security Services
Security Mechanism
Relation between Services and Mechanisms

Security Attack : Any action that compromises the security of information owned by an organization.

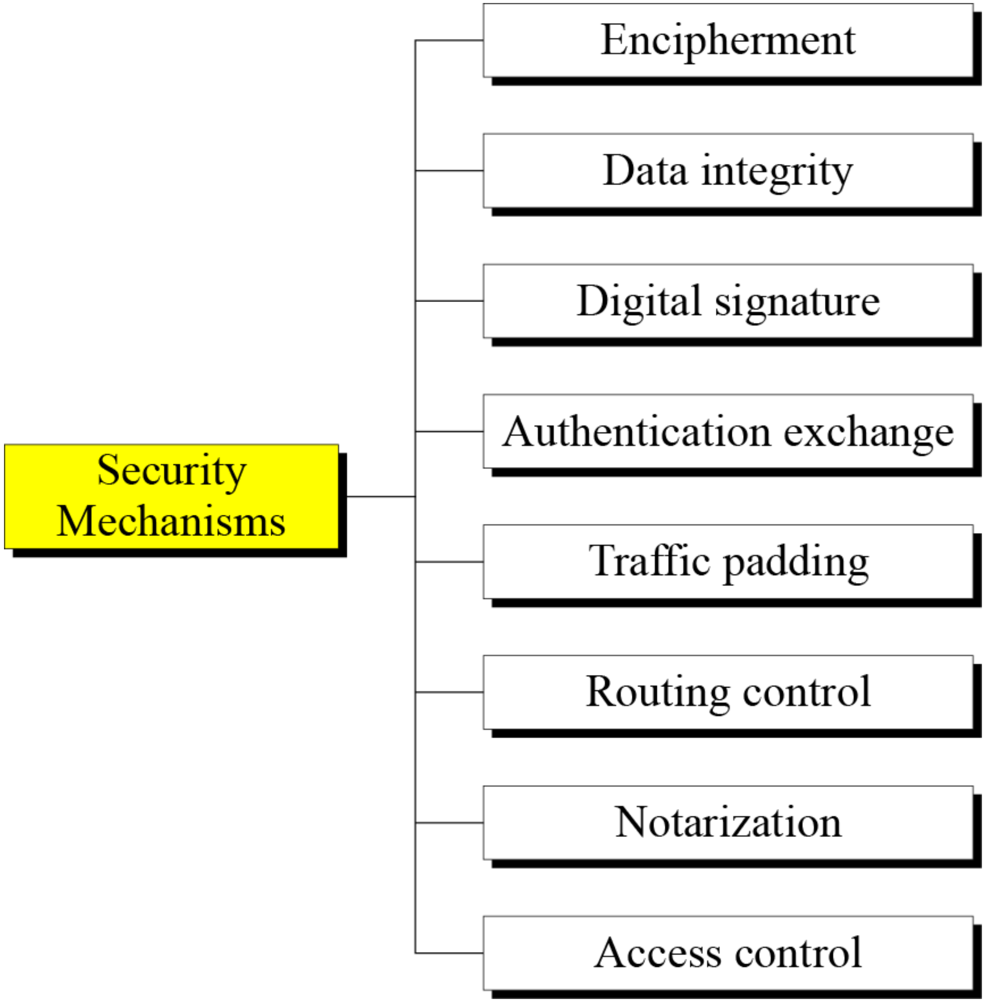
Security Services: A service that enhances the security of the data processing systems and the information transfers of an organization. The services are more intended to counter security attacks and they make use of one or more security mechanism to provide the service.

Security Services



Security Mechanisms

Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.

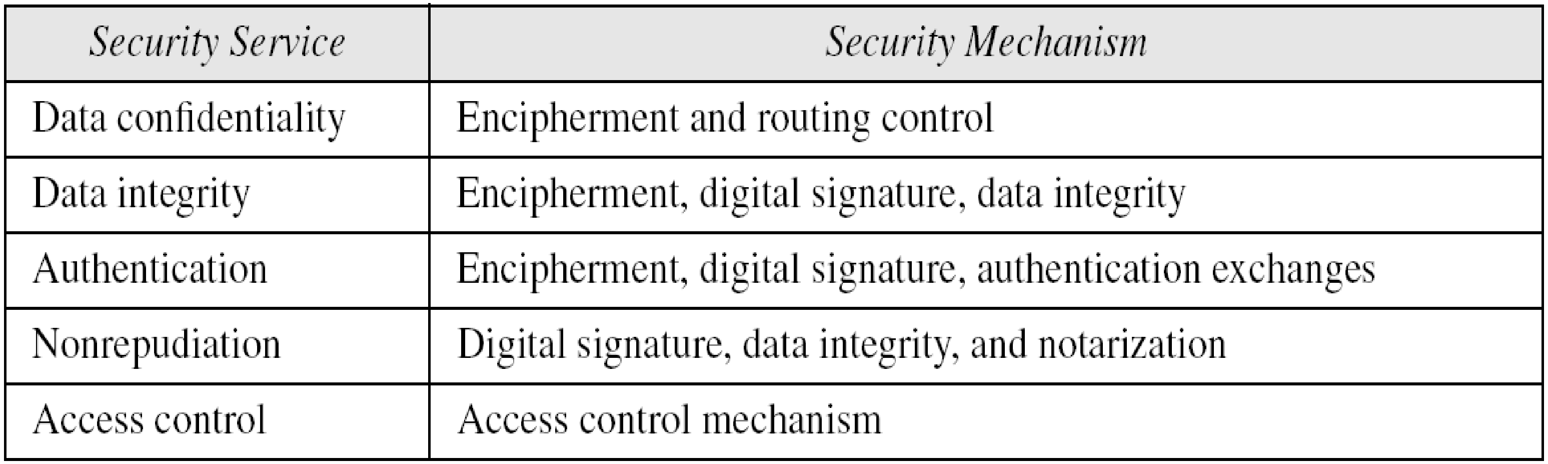


- **Notarization** means selecting a third party to control the communication between two entities. This can be done for example, to prevent repudiation.

Relation between Services and Mechanisms

Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

What is a Cryptosystem?

Plaintext: data to be ‘hidden’

Ciphertext: “not-meaningful” data

plaintext $\xrightarrow{\text{encryption}}$ ciphertext $\xrightarrow{\text{decryption}}$ ciphertext

Definition

A **cryptosystem** is a five-tuple (P, C, K, E, D), s. t.:

1. P is a finite set of possible plaintexts
2. C is a finite set of possible ciphertexts
3. K, the keyspace, is the set of possible keys
4. For each $k \in K$, there are
   - encryption rule e_k, $e_k: P \to C$,
   - decryption rule d_k, $d_k: C \to P$,
   - s.t. $d_k(e_k(x)) = x$

Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Two Requirements for Secure use of Symmetric Encryption

- **Strong Encryption Algorithm**

  The opponent should be unable to decrypt ciphertext or discover the key even if the opponent is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

$$Y = \mathrm{E}_K(X)$$

$$X = \mathrm{D}_K(Y)$$

- **Secret key known only to Sender / Receiver**

  Sender and Receiver must have obtained copies of the secrete key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm all communication using this key is readable.

Symmetric & Public Key Algorithms

Encryption and Decryption keys are known to both communicating parties (Alice and Bob).

They are usually related and it is easy to derive the decryption key once one knows the encryption key.

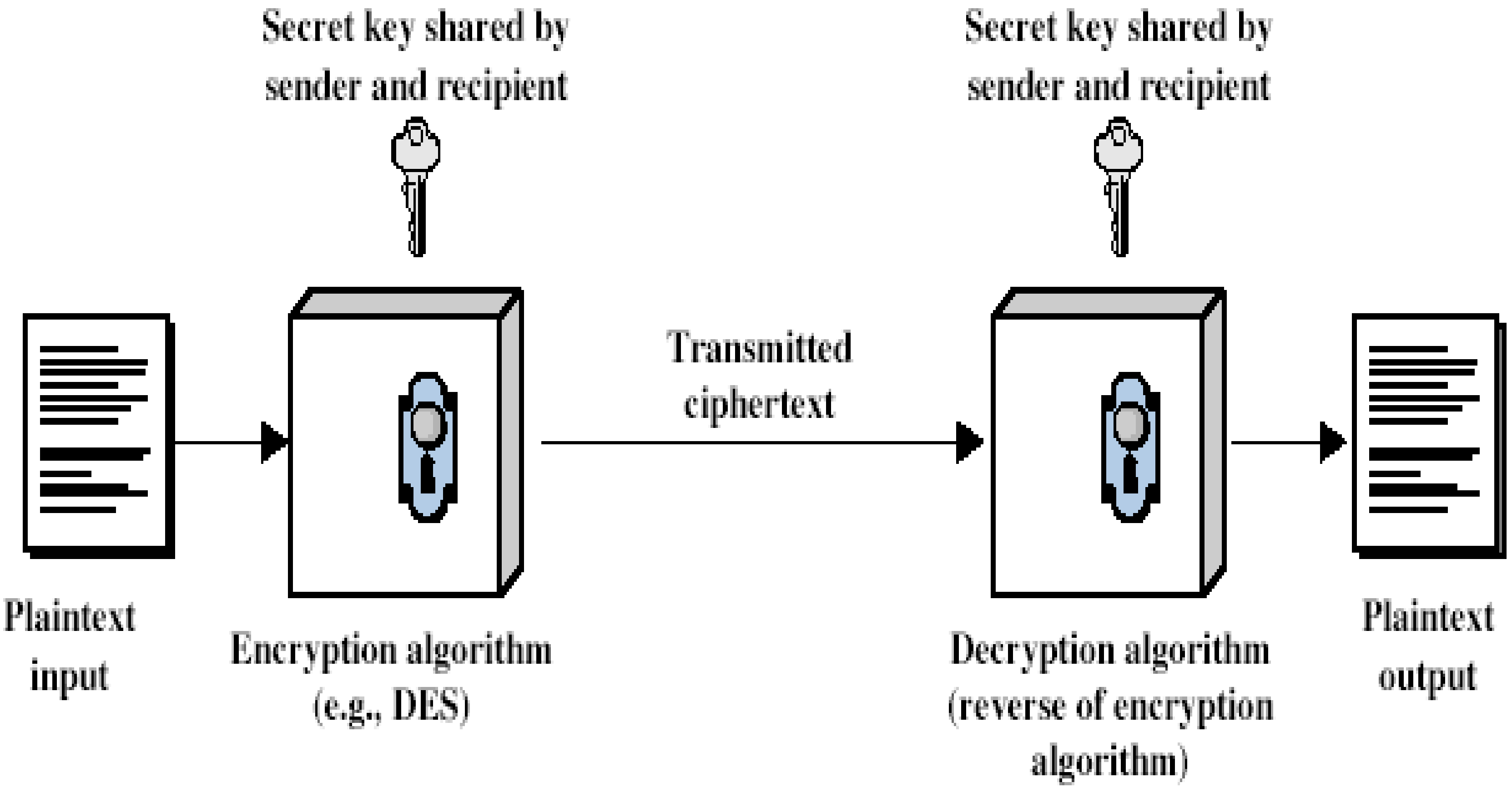
In most cases, they are identical. All of the classical (pre-1970) cryptosystems are symmetric. Examples : DES and AES (Rijndael)

A Secret should be shared (or agreed) between the communicating parties.

Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970’s

Symmetric Cipher Model


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Kerckhkoffs’s Principle

While assessing the strength of a cryptosystem, one should always assume that the enemy knows the cryptographic algorithm used.

The security of the system, therefore, should be based on

* the quality (strength) of the algorithm but not its obscurity
* the key space (or key length)

The Number of Keys Used

The Number of Keys Used

- If both sender and receiver use the same key, the system is referred to as symmetric key, single key, secret key or conventional encryption.

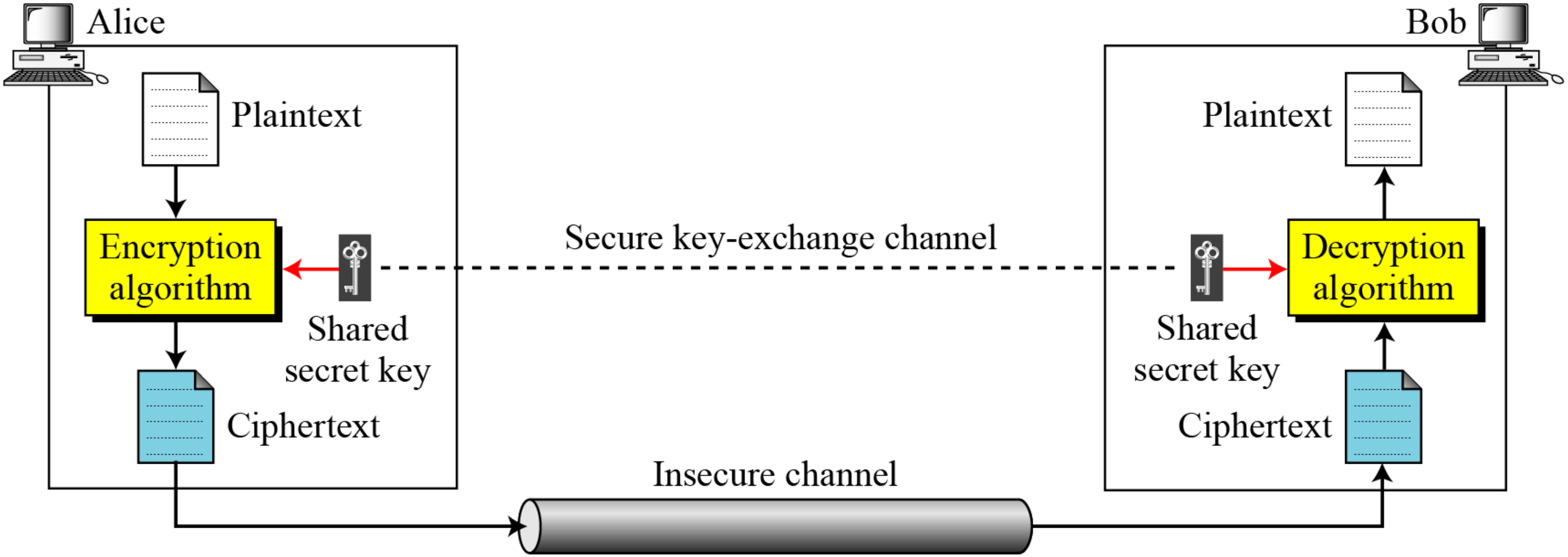
- If the sender and receiver is use different keys, the system is referred to asymmetric, two key or public key encryption.

The way in which the plain text is processed

- A block cipher processes the input one block of elements at a time, producing an output block for each input block.

- A stream cipher processes the input elements continuously producing output one element at a time as it goes along.

General idea of Symmetric-key Cipher



General idea of Symmetric-key Cipher Contd.

If P is the plaintext, C is the ciphertext, and K is the key,

$$\text{Encryption: } \mathrm{C} = \mathrm{E}_k(\mathrm{P}) \qquad\qquad \text{Decryption: } \mathrm{P} = \mathrm{D}_k(\mathrm{C})$$

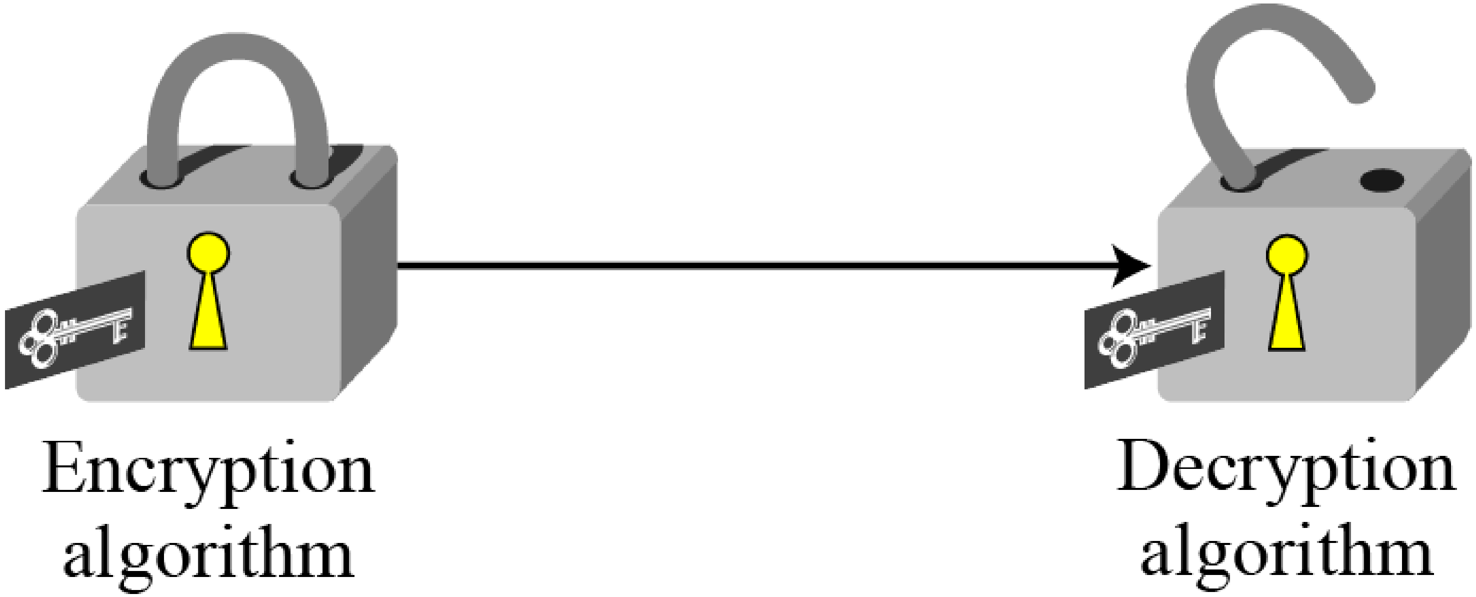
$$\text{In which, } \mathrm{D}_k(\mathrm{E}_k\,(x)) = \mathrm{E}_k(\mathrm{D}_k\,(x)) = x$$

We assume that Bob creates P_1; we prove that $\mathrm{P}_1 = \mathrm{P}$:

$$\textbf{Alice: } \mathrm{C} = \mathrm{E}_k\,(\mathrm{P})$$

$$\textbf{Bob: } \mathrm{P}_1 = \mathrm{D}_k\,(\mathrm{C}) = \mathrm{D}_k\,(\mathrm{E}_k(\mathrm{P})) = \mathrm{P}$$

Locking and Unlocking with the Same Key



Type of Operations used for Transforming Plain text to Cipher Text

All encryption algorithms are based on two general principles:

- substitution in which each element in the plain text (bit, letter, group of bits or letters) is mapped into another element, and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible).

- Most systems referred to as product systems, involve multiple stages of substitution and transposition.

SUBSTITUTION CIPHERS

A substitution cipher replaces one symbol with another. Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

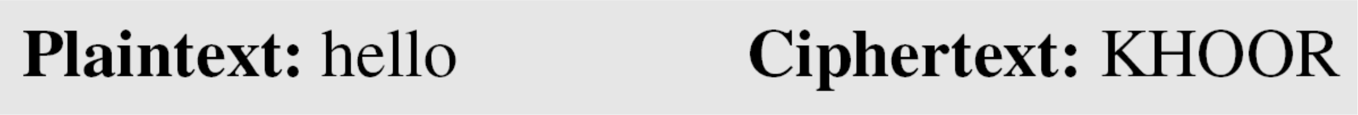
A Substitution Cipher Replaces one Symbol with Another.

Monoalphabetic Ciphers

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

Monoalphabetic Ciphers Contd.

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

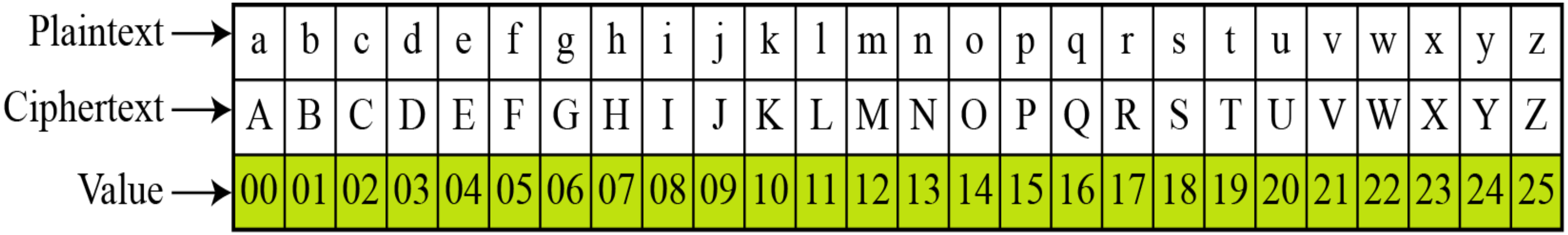


Plaintext: hello **Ciphertext:** KHOOR

Monoalphabetic Ciphers Additive Cipher Contd.

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

Plaintext and ciphertext in Z_{26}



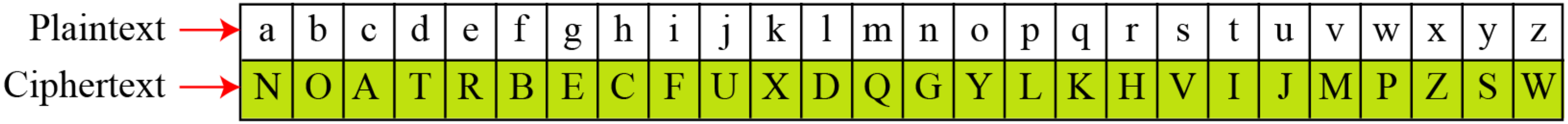
Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Monoalphabetic Substitution Cipher

Because additive, multiplicative, and affine ciphers have small key domains, they are 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.

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

Monoalphabetic Substitution Cipher Contd.

Example 3.13

We can use the key in Figure 3.12 to encrypt the message

this message is easy to encrypt but hard to find the key

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

Autokey Cipher

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

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

Example

Assume that Alice and Bob agreed to use an autokey cipher with initial key value $k_1 = 12$. Now Alice wants to send Bob the message “Attack is today”. Enciphering is done character by character.

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P’s Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C’s Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

Vigenere Cipher

$P = P_1P_2P_3 \ldots$ $C = C_1C_2C_3 \ldots$ $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$ Decryption: $P_i = C_i - k_i$

Example

We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.

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

Example

Let us see how we can encrypt the message “She is listening” using the 6-character keyword “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).

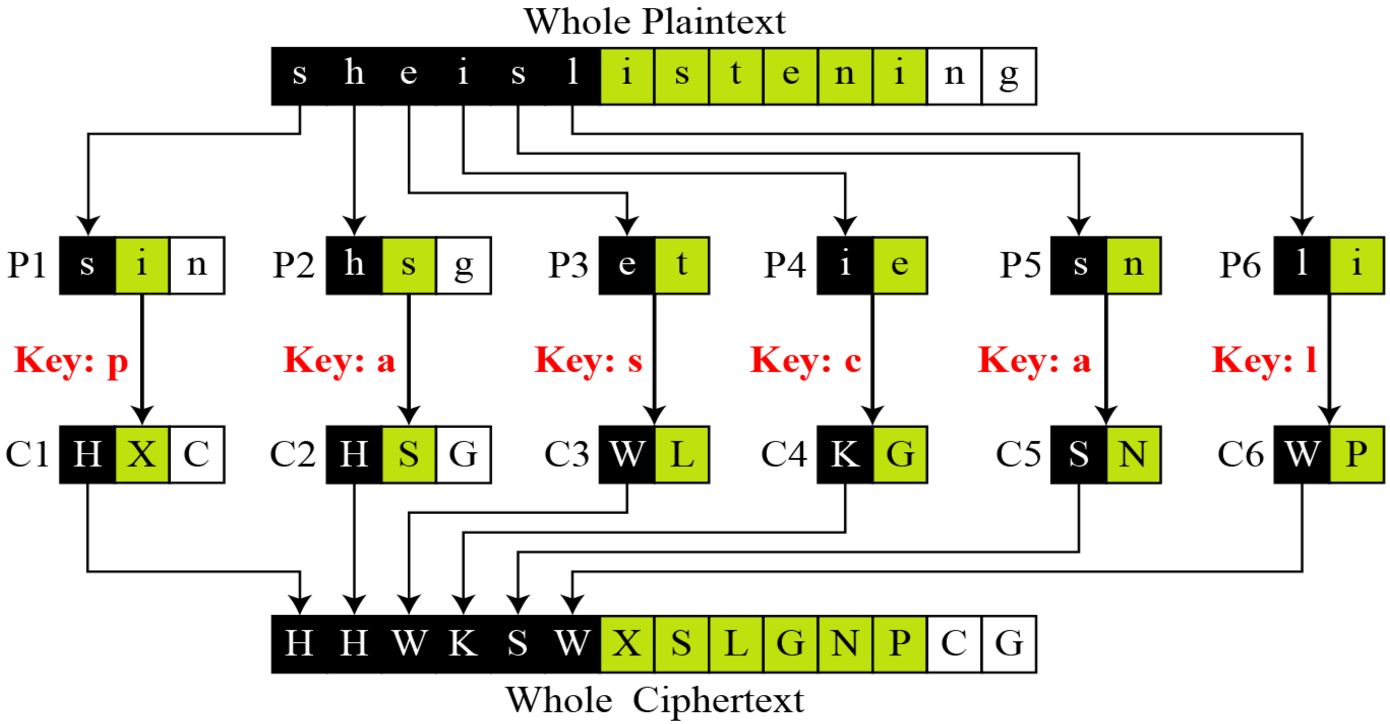
Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P’s values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C’s values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**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

Vigenere Cipher

Example

Vigenere cipher can be seen as combinations of m additive ciphers.

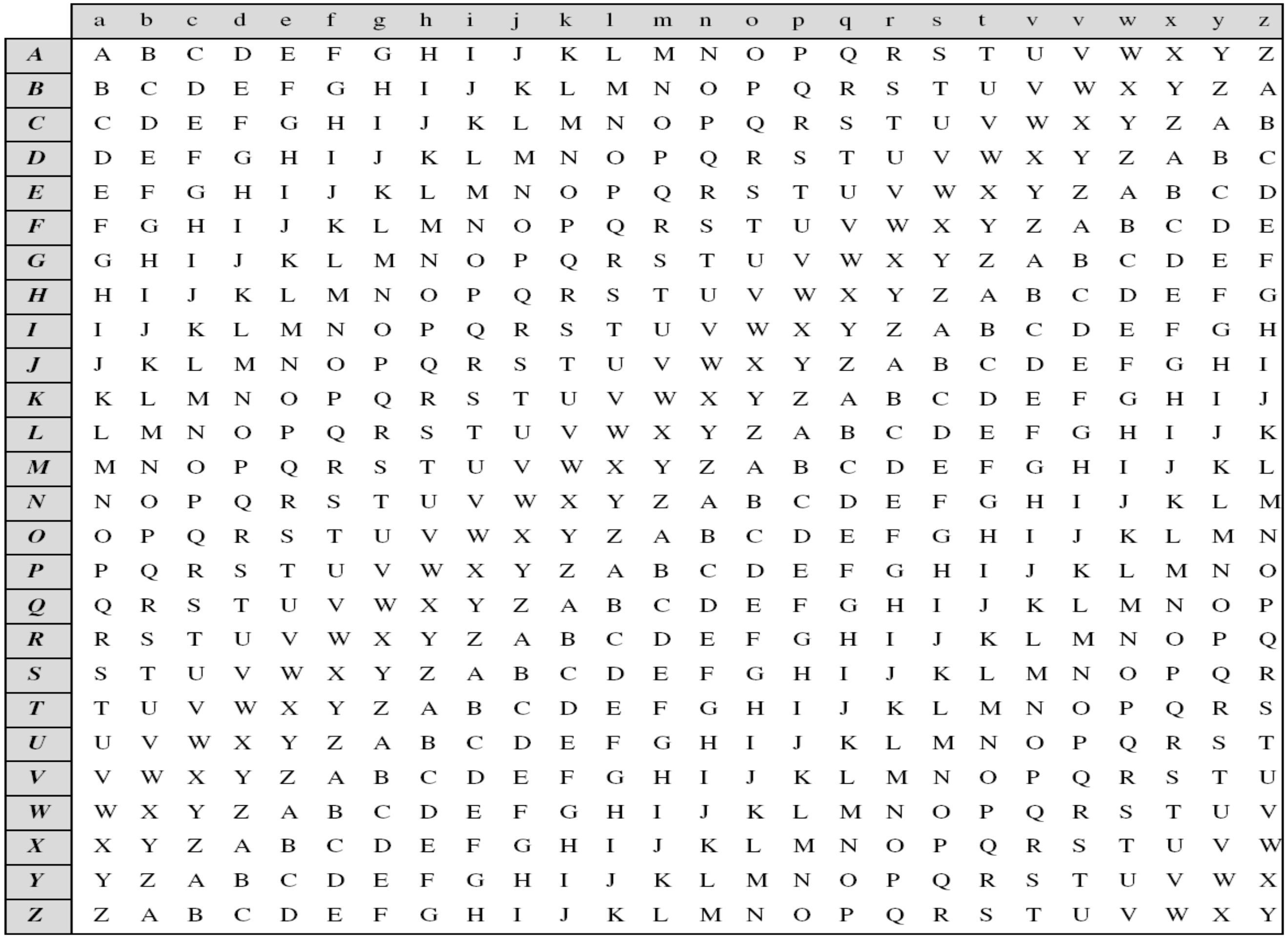
A Vigenere cipher as a combination of m additive ciphers



Vigenere Cipher Example

Using Example we can say that the additive cipher is a special case of Vigenere cipher in which m = 1.

A Vigenere Tableau



	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	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

Hill Cipher

- Hill Cipher developed by mathematician Lester Hill in 1929.

- The encryption algorithm takes m successive plaintext letters and substitutes for them m cipher text letters

- The substitution determined by m linear equation in which each character is assigned a numerical value (a=0, b=1,...,Z=25)

Hill Cipher Contd.

Key in the Hill cipher

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

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

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

Hill Cipher Contd.

1. Determinant of a matrix *A*, denoted by *det A* :
   -- if $A(a_{ij})$ is 2×2, then $det\ A = a_{11}a_{22} - a_{12}a_{21}$
   -- if $A(a_{ij})$ is 3×3, then $det\ A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$

2. Theorem: suppose $K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$ with $k_{ij} \in \mathcal{Z}_{26}$

Then *K* has an inverse **if and only if** *det K* is invertible in $\mathcal{Z}_{26}$

if and only if gcd(*det K*, 26)=1

Moreover,

$K^{-1} = (det\ K)^{-1} \begin{pmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{pmatrix}$ Where $det\ K = k_{11}k_{22} - k_{12}k_{21}$

Hill Cipher Contd.

- $C_1 = (K_{11}P_1+K_{12}P_2+K_{13}P_3) \bmod 26$
- $C_2 = (K_{21}P_1+K_{22}P_2+K_{23}P_3) \bmod 26$
- $C_3 = (K_{31}P_1+K_{32}P_2+K_{33}P_3) \bmod 26$
- $C=E(K,P)=KP \bmod 26$
- $P=D(K,C)=K^{-1}C\bmod 26=K^{-1}KP=P$

Hill Cipher (I)

A multiple-letter encryption method – encrypts m letters of plaintext at each step

- The encryption key K is a m x m matrix of coefficients
- To encrypt – multiply the matrix K by a vector of m plaintext letters to receive a vector of m ciphertext letters. (Arithmetic is modulo the size of the alphabet.)
- Example: m = 3

$$C1 = K_{11} P_1 + K_{12} P_2 + K_{13} P_3$$
$$C2 = K_{21} P_1 + K_{22} P_2 + K_{23} P_3$$
$$C3 = K_{31} P_1 + K_{32} P_2 + K_{33} P_3$$

Hill Cipher (II)

The encryption key K is a m x m matrix of coefficients

- The decryption key K^{-1} is the m x m matrix of coefficients that is the inverse of matrix K:

$$K K^{-1} = I$$

- To decrypt – multiply the matrix K^{-1} by the vector of m ciphertext letters to receive the vector of m plaintext letters. (Arithmetic is modulo the size of the alphabet.)

TRANSPOSITION CIPHERS

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.

A transposition cipher reorders symbols.

Keyless Transposition Ciphers
Keyed Transposition Ciphers
Combining Two Approaches

TRANSPOSITION CIPHERS

Transposition techniques differ from substitution technique in the way that they do not simply replace one alphabet with another: they also performs some permutation over the plain text alphabets.

Rail Fence Technique

The rail fence technique is an example of transposition cipher. It uses a simple algorithm as

1. Write down the plain text message as a sequence of diagonals.
2. Read the plain text written in step1 as a sequence of rows.

TRANSPOSITION CIPHERS Contd.

Simple Columnar Transposition Technique

Variation of the basic transposition technique such as Rail Fence Technique exist. Such a scheme is can call as Simple Columnar Transposition Technique.

1. Write the plain text message row by row in a rectangle of predefined size.

2. Read the message column-by-column. However, it need not be in the order of Column 1, Column 2, It can be random order such as 2, 3 ect.

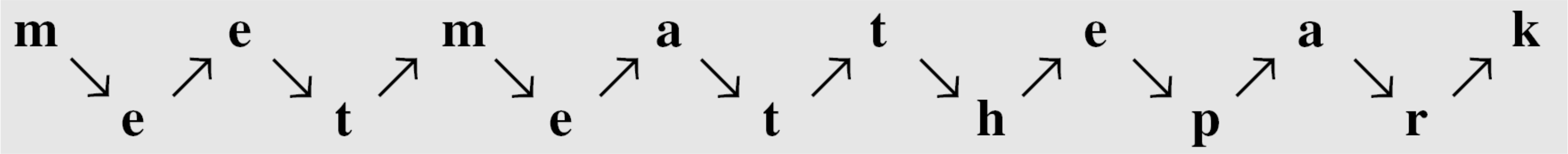
3. The message thus obtained is the cipher text message.

Keyless Transposition Ciphers

Simple transposition ciphers, which were used in the past, are keyless.

Example

A good example of a keyless cipher using the first method is the rail fence cipher. The ciphertext is created reading the pattern row by row. For example, to send the message **“meet me at the park”** to Bob, Alice writes



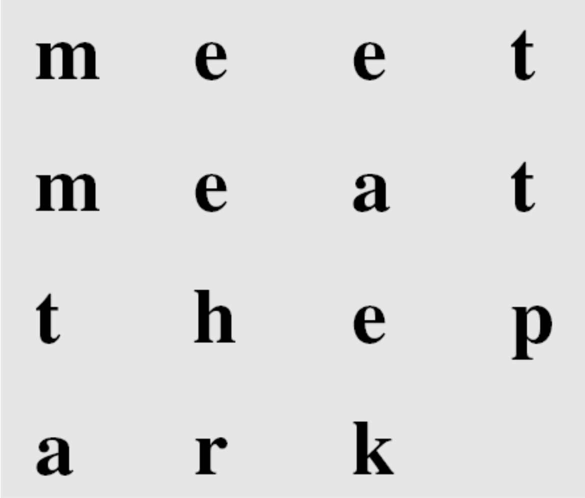
m ↘ e ↗ e ↘ t ↗ m ↘ e ↗ a ↘ t ↗ t ↘ h ↗ e ↘ p ↗ a ↘ r ↗ k

She then creates the ciphertext “MEMATEAKETETHPR”.

Keyless Transposition Ciphers

Example

Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

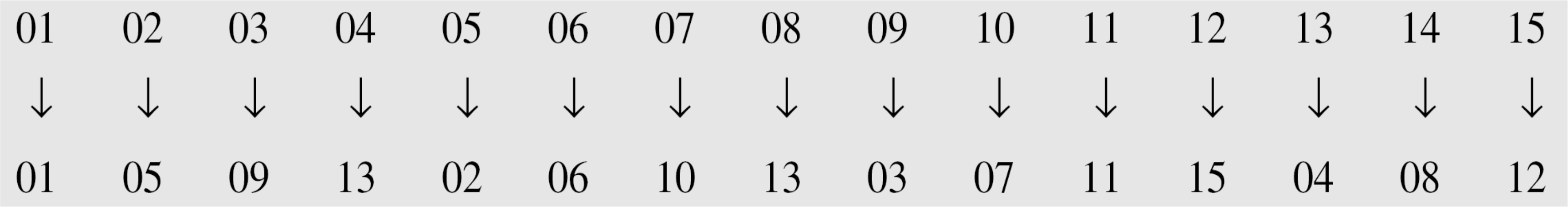


m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

She then creates the ciphertext “MMTAEEHREAEKTTP”.

Example

The cipher in previous example is actually a transposition cipher. The following shows the permutation of each character in the plaintext into the ciphertext based on the positions.



01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
01	05	09	13	02	06	10	13	03	07	11	15	04	08	12

The second character in the plaintext has moved to the fifth position in the ciphertext; the third character has moved to the ninth position; and so on. Although the characters are permuted, there is a pattern in the permutation: (01, 05, 09, 13), (02, 06, 10, 13), (03, 07, 11, 15), and (08, 12). In each section, the difference between the two adjacent numbers is 4.

Keyed Transposition Ciphers

The keyless ciphers permute the characters by using writing plaintext in one way and reading it in another way.

The permutation is done on the whole plaintext to create the whole ciphertext.

Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

Keyed Transposition Ciphers

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 character are permuted.

Encryption ↓

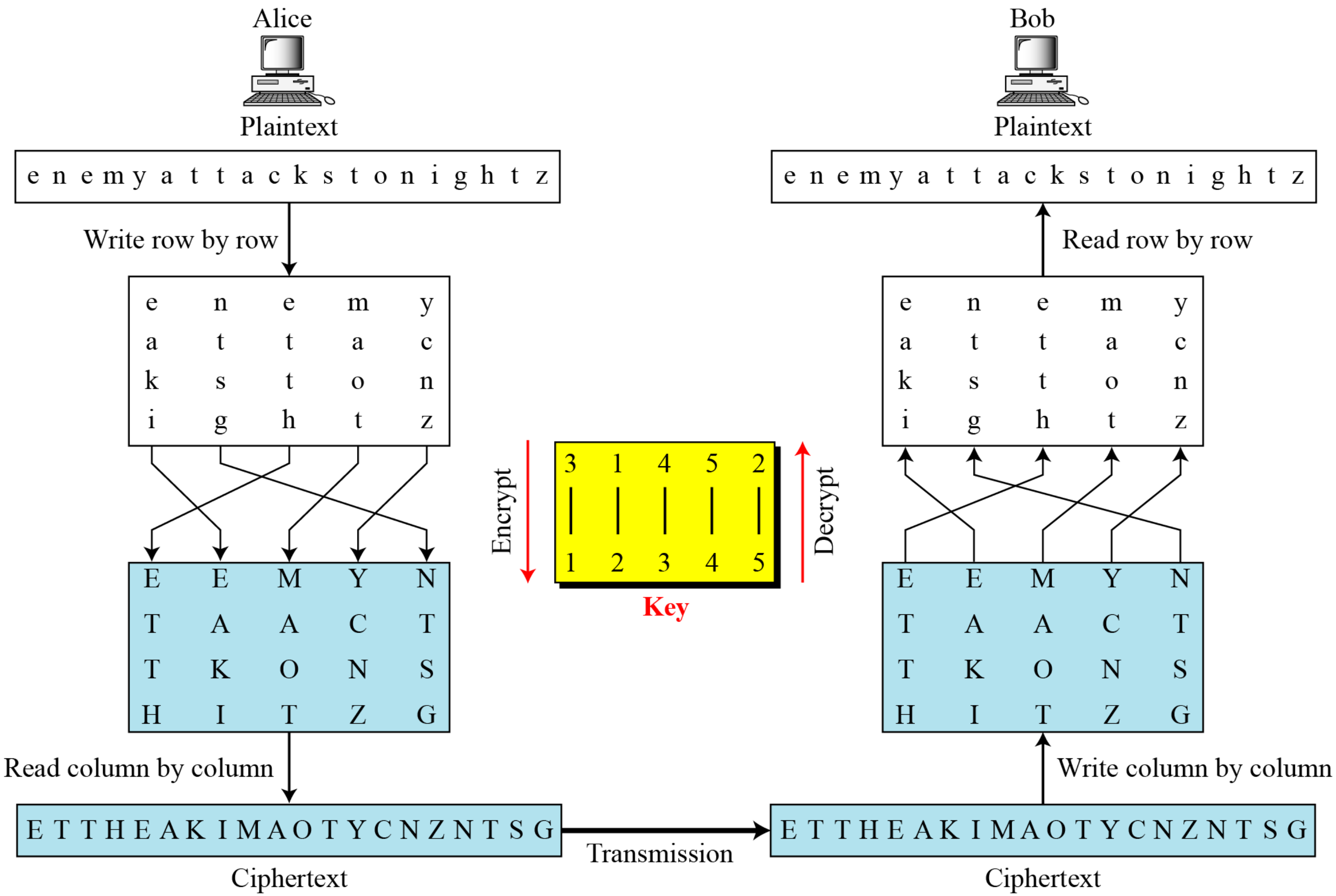
3	1	4	5	2
1	2	3	4	5

↑ Decryption

The permutation yields

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

Combining Two Approaches



Alice

Plaintext

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

Write row by row

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

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

Read column by column

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

Ciphertext

Transmission

Encrypt

3	1	4	5	2
1	2	3	4	5

Key

Decrypt

Bob

Plaintext

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

Read row by row

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

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

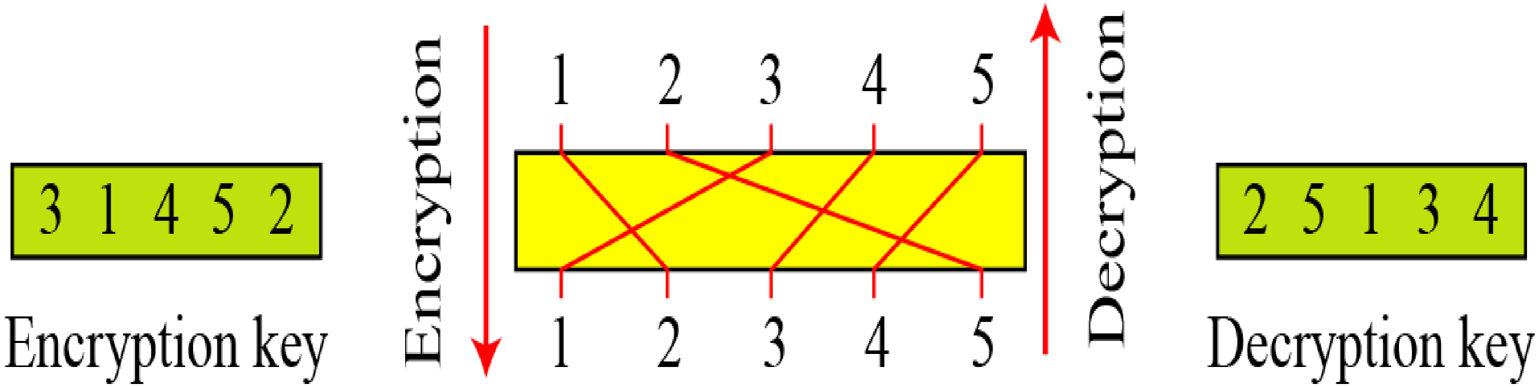
Write column by column

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

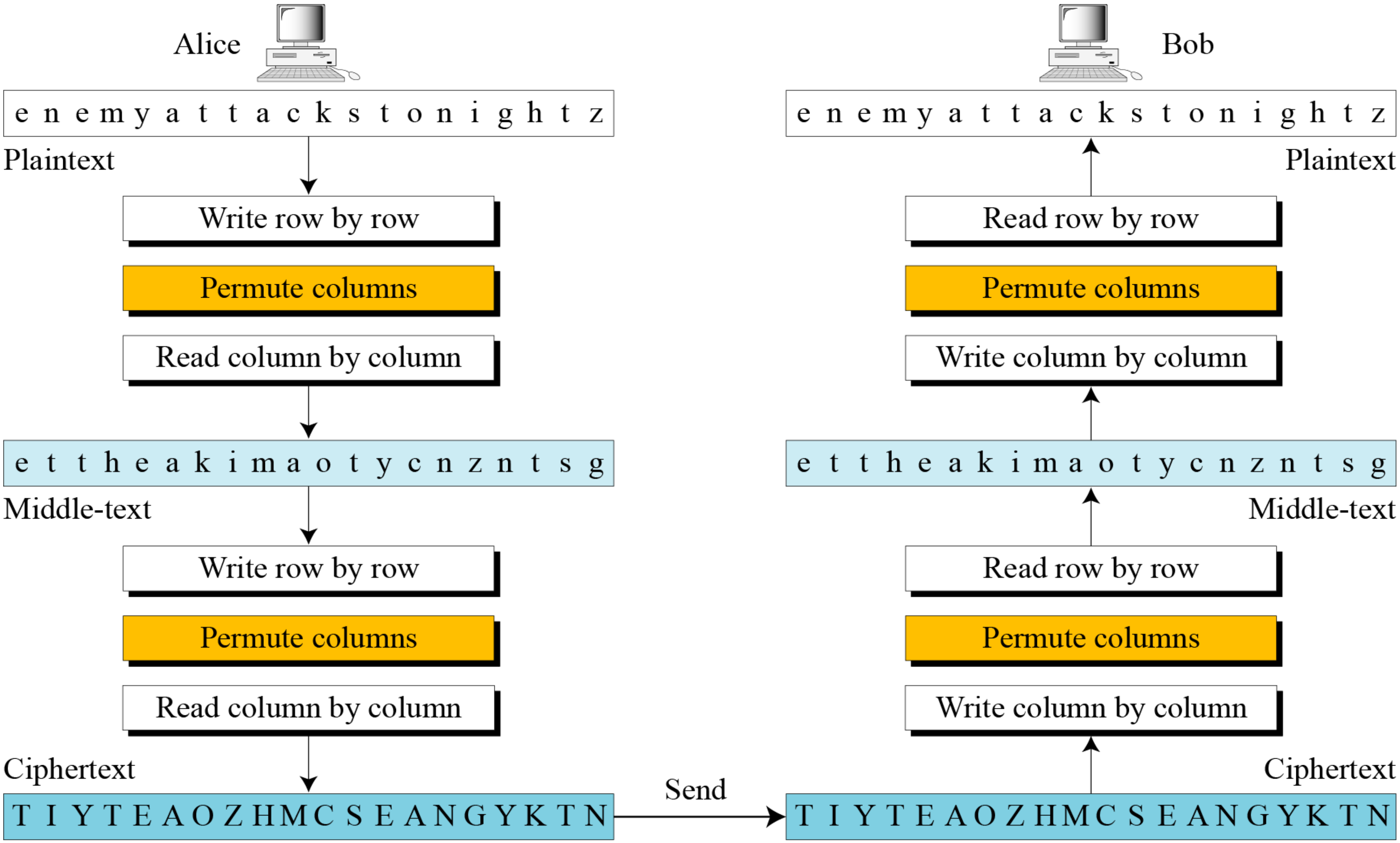
Ciphertext

In previous example, a single key was used in two directions for the column exchange: downward for encryption, upward for decryption. It is customary to create two keys.

Encryption/Decryption keys in Transpositional Ciphers



Double Transposition Ciphers



Alice

enemyattackstonightz

Plaintext

Write row by row

Permute columns

Read column by column

ettheakimaotycnzntsg

Middle-text

Write row by row

Permute columns

Read column by column

Ciphertext

TIYTEAOZHMCSEANGYKTN

Send

Bob

enemyattackstonightz

Plaintext

Read row by row

Permute columns

Write column by column

ettheakimaotycnzntsg

Middle-text

Read row by row

Permute columns

Write column by column

Ciphertext

TIYTEAOZHMCSEANGYKTN

There are Two Requirements for Secure use of Conventional Encryption

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Cryptanalysis and Brute-Force Attack

Objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Attack Methods

1. **Ciphertext only:** Alice has only a copy of ciphertext

2. **Known Plaintext:** Eve has a copy of ciphertext and the corresponding plaintext and tries the deduce the key.

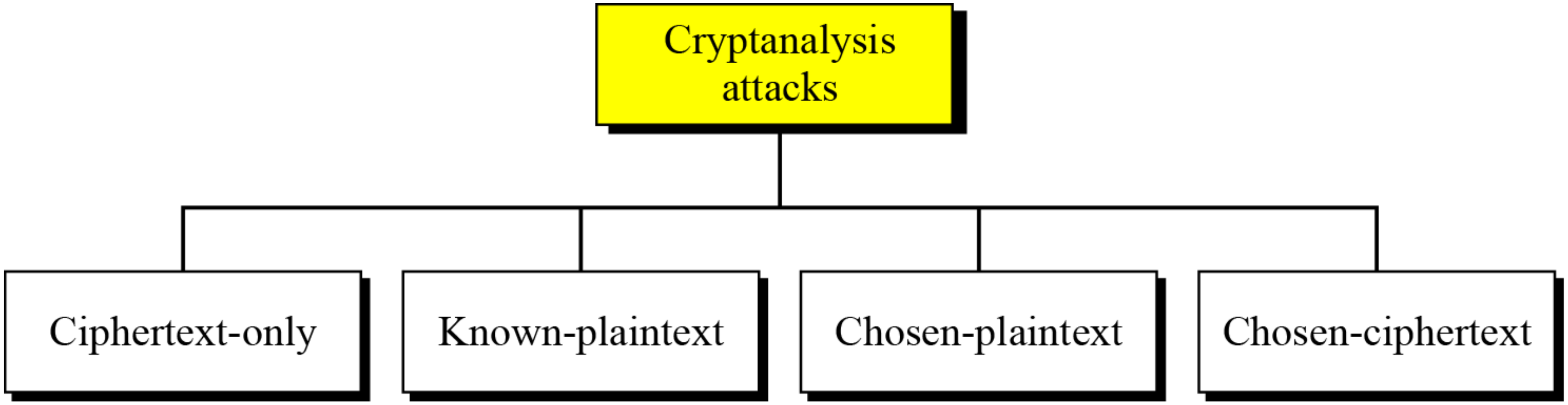
3. **Chosen Plaintext:** Eve has a copy of ciphertext corresponding to a copy of plaintext selected by Alice who believes it is useful to deduce the key.

4. **Chosen Ciphertext:** Eve has a copy plaintext corresponding to a copy of ciphertext selected by Alice who believes it is useful to deduce the key.

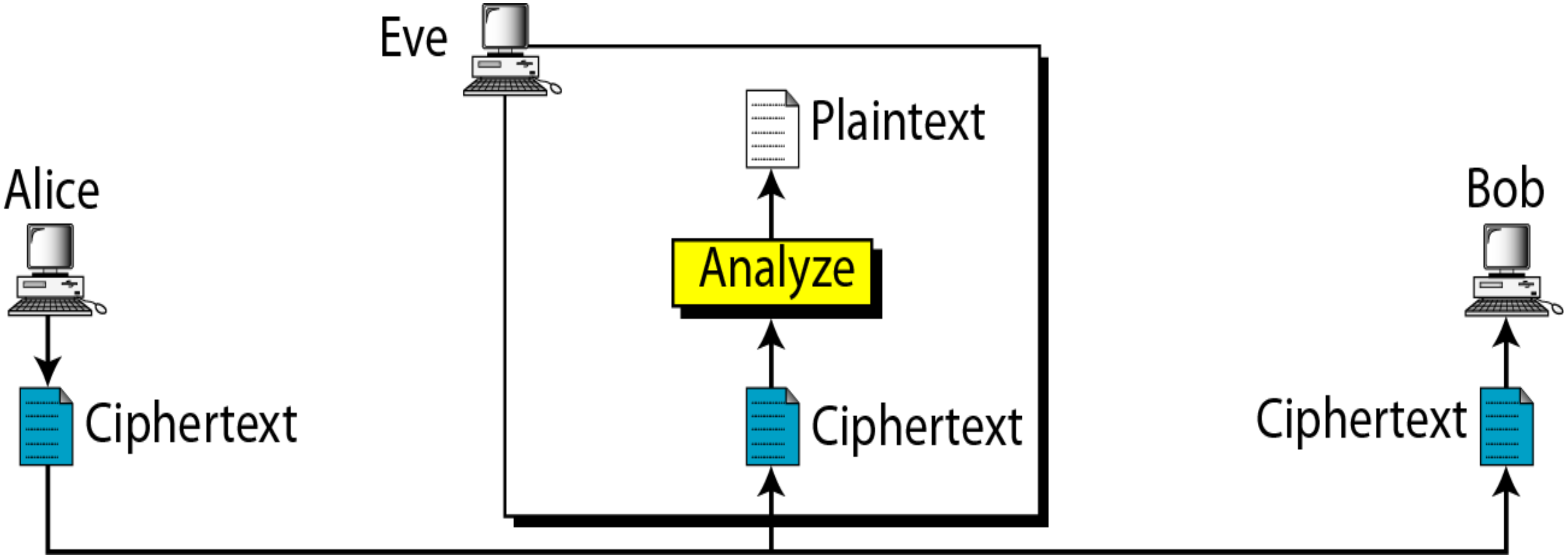
Cryptanalysis

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

Cryptanalysis attacks

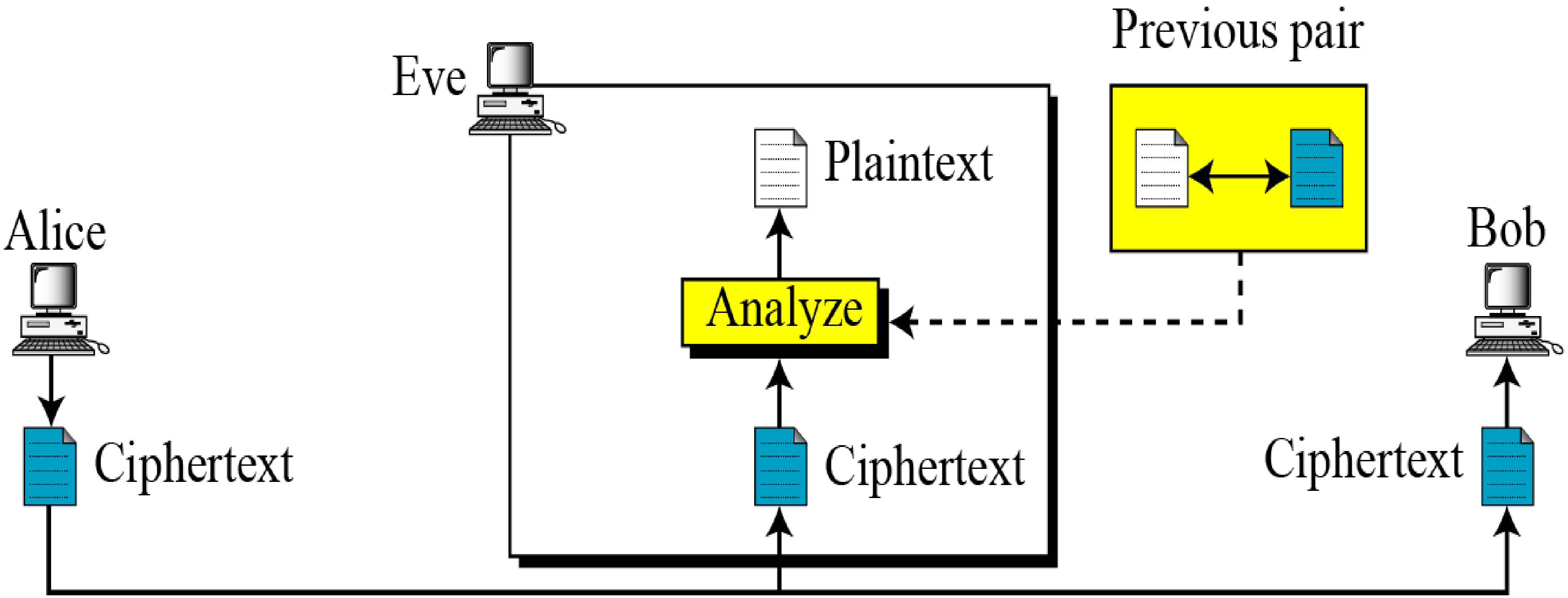


Ciphertext-Only Attack



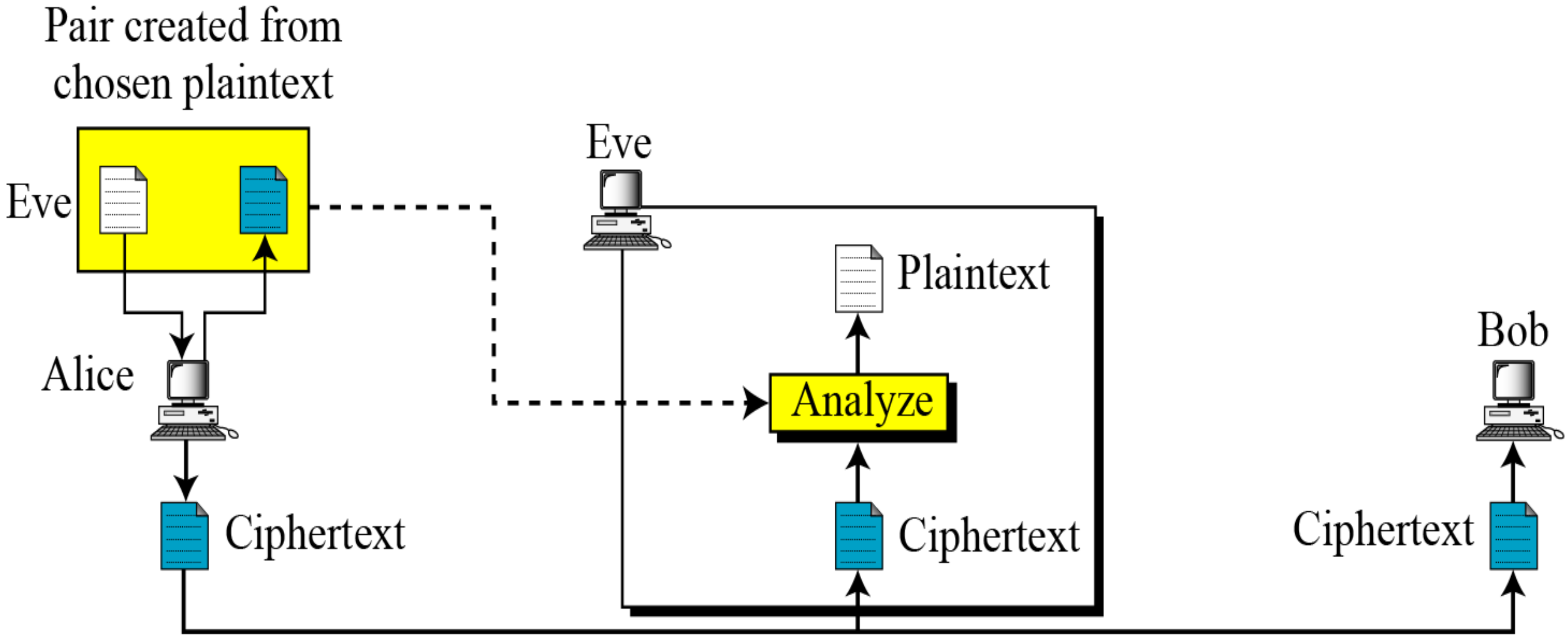
Note: Refer/Read Text Book to get the description

Known-Plaintext Attack



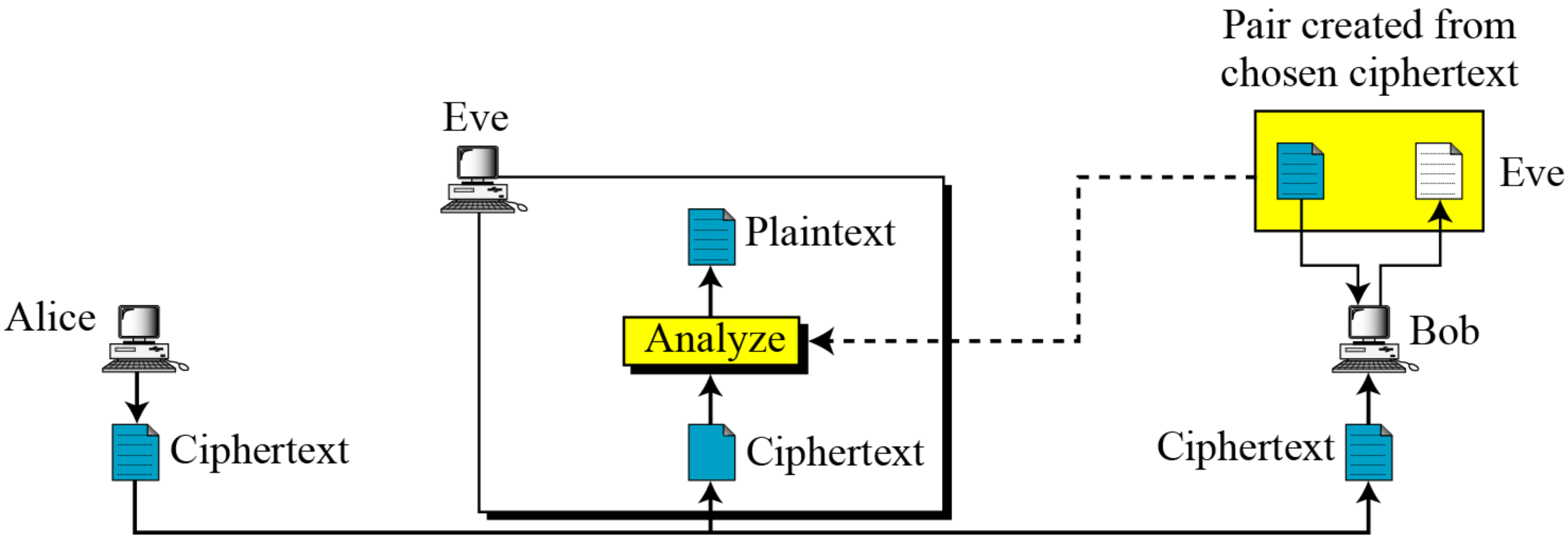
Note: Refer/Read Text Book to get the description

Chosen-Plaintext Attack



Note: Refer/Read Text Book to get the description

Chosen-Ciphertext Attack



Note: Refer/Read Text Book to get the description