INFORMATION SECURITY [3 0 0 3]

ICT 3172:

Outline

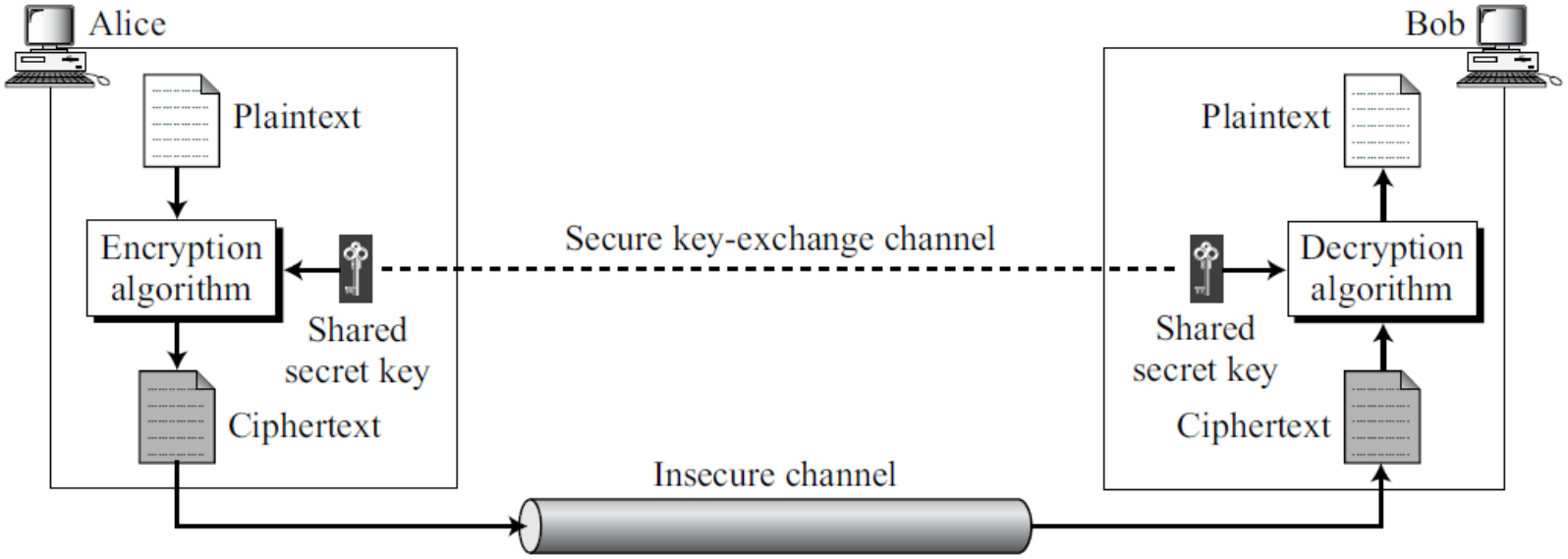
General idea behind symmetric-key ciphers.

Traditional symmetric-key ciphers: Not used today, study them for several reasons.

- simpler than modern ciphers and easier to understand.
- Give the basic foundation of cryptography and encipherment: To better understand modern ciphers.
- Provide the rationale for using modern ciphers, because the traditional ciphers can be easily attacked using a computer. Ciphers that were secure in earlier eras are no longer secure in this computer age.
- DES
- AES

3.1 INTRODUCTION

The general idea behind a symmetric-key cipher.



An entity, Alice, can send a message to another entity, Bob, over an insecure channel with the assumption that an adversary, Eve, cannot understand the contents of the message by simply eavesdropping over the channel.

- Plaintext: Original message from Alice to Bob.
- Ciphertext: The message that is sent through the channel.
- Encryption algorithm and a shared secret key: To create the ciphertext from the plaintext..
- Decryption algorithm and the shared secret key: To create the plaintext from ciphertext.
- We refer to encryption and decryption algorithms as ciphers.
- A key is a set of values (numbers) that the cipher operates on.

Encryption and decryption algorithms are inverses of each other.

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

Encryption algorithm $E_k(x)$ creates the ciphertext from the plaintext;

Decryption algorithm $D_k(x)$ creates the plaintext from the ciphertext.

$E_k(x)$ and $D_k(x)$ are inverses of each other: they cancel the effect of each other if they are applied one after the other on the same input.

Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

According to Kerckhoff's principle, it is better to make the encryption and decryption public but keep the shared key secret.

This means that Alice and Bob need another channel, a secured one, to exchange the secret key.

- Alice and Bob can meet once and exchange the key personally. Secured channel here is the face-to-face exchange of the key.
- Trust a third party to give them the same key.
- Create a temporary secret key using another kind of cipher-asymmetric-key ciphers- (discussed later).

Assumption: There is an established secret key between Alice and Bob.

Another element in symmetric-key encipherment is the number of keys.

Alice needs another secret key to communicate with another person, say David.

If there are **m** people in a group who need to communicate with each other, how many keys are needed?

Another element in symmetric-key encipherment is the number of keys.

Alice needs another secret key to communicate with another person, say David.

If there are m people in a group who need to communicate with each other, how many keys are needed?

$(m \times (m - 1))/2$

Kerckhoff's Principle

Based on Kerckhoff's principle, one should always assume that the adversary, Eve, knows the encryption/decryption algorithm.

Resistance of the cipher to attack must be based only on the secrecy of the key.

Guessing the key should be so difficult that there is no need to hide the encryption/decryption algorithm.

Cryptanalysis

Cryptography: The science and art of creating secret codes.
cryptanalysis : The science and art of breaking those codes.

- In addition to studying cryptography techniques, we also need to study cryptanalysis techniques.
- Not to break the codes, but to learn how vulnerable our cryptosystem is.
- The study of cryptanalysis helps us create better secret codes.

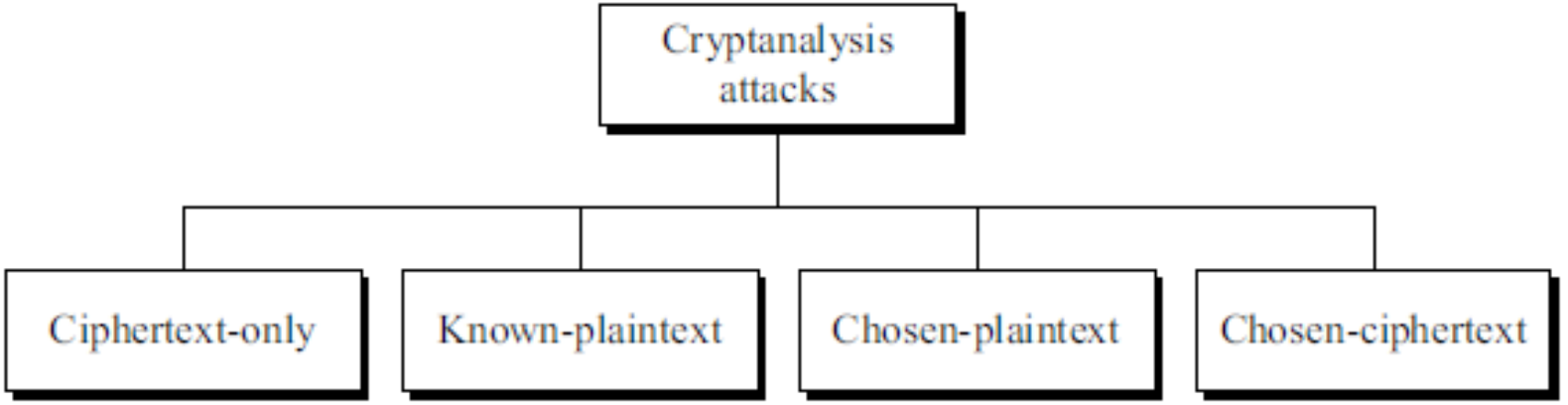
Relationship between Cryptography and Cryptanalysis

Interdependence: Cryptography and cryptanalysis are two sides of the same coin. While cryptography focuses on creating secure communication methods, cryptanalysis tests these methods for weaknesses.

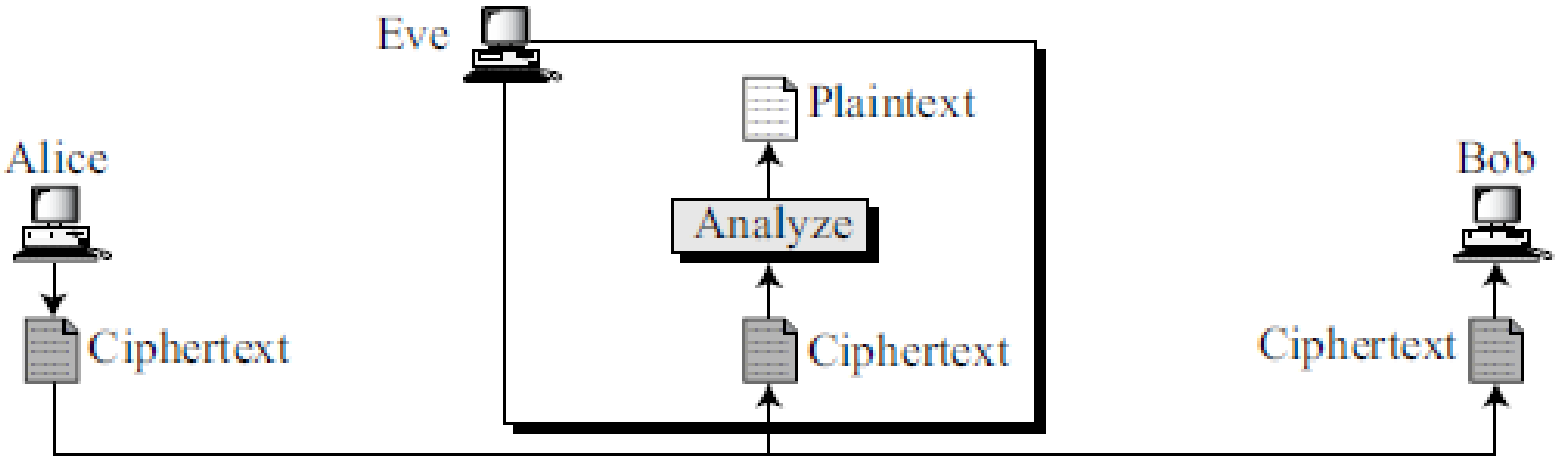
Advancement: The evolution of cryptographic techniques often goes hand-in-hand with advances in cryptanalysis. When a cryptographic method is found to be vulnerable, it prompts the development of stronger algorithms.

Security Assurance: The effectiveness of cryptographic systems is often validated through rigorous cryptanalysis. By attempting to break these systems, cryptanalysts help ensure that they are robust against potential attacks.

4 common types of cryptanalysis attacks.



Ciphertext-Only Attack



Eve has access to only some ciphertext.
She tries to find the corresponding key and the plaintext.
Assumption : Eve knows the algorithm and can intercept the ciphertext.

Various methods can be used in ciphertext-only attack. Some are:

- ✓ Brute-Force Attack
- ✓ Statistical Attack
- ✓ Pattern Attack

Brute-Force Attack

In the brute-force method or exhaustive-key-search method, Eve tries to use all possible keys.

Assumption : Eve knows the algorithm and knows the key domain (the list of all possible keys).

Was a difficult task in the past; it is easier today using a computer.

To prevent this type of attack, the number of possible keys must be very large.

Statistical Attack

The cryptanalyst can benefit from some inherent characteristics of the plaintext language to launch a statistical attack.

Example :

- ✓ Letter E is the most frequently used letter in English text.
- ✓ Cryptanalyst finds the mostly-used character in the ciphertext and assumes that the corresponding plaintext character is E.

To prevent this type of attack, the cipher should hide the characteristics of the language.

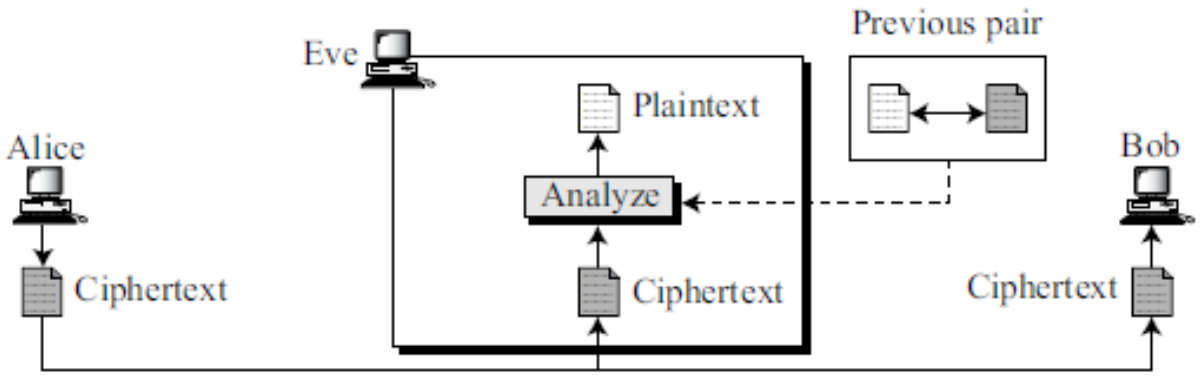
Pattern Attack

A cryptanalyst may use a pattern attack to break the cipher.

It is important to use ciphers that make the ciphertext look as random as possible.

Known-Plaintext Attack

Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext that she wants to break.



Known-Plaintext Attack (contd)

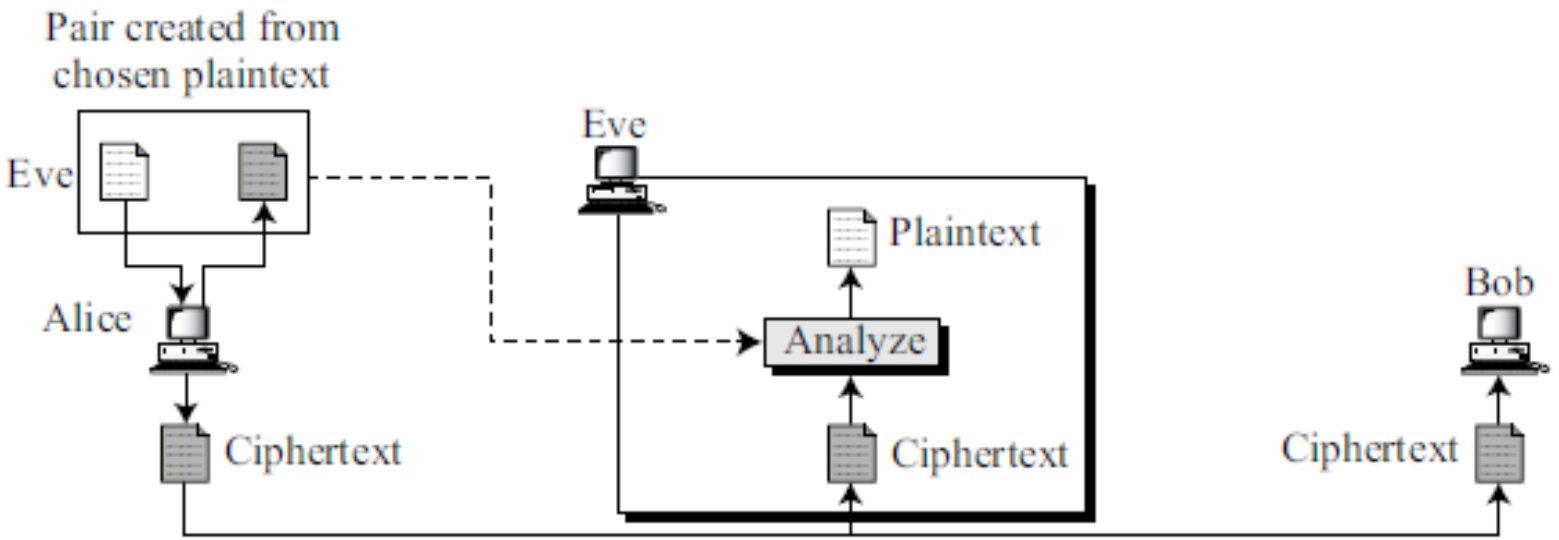
The plaintext/ciphertext pairs have been collected earlier.

For example, Alice has sent a secret message to Bob, but she has later made the contents of the message public.

Eve has kept both the ciphertext and the plaintext to use them to break the next secret message from Alice to Bob, assuming that Alice has not changed her key.

It is less likely to happen because Alice may have changed her key or may have not disclosed the contents of any previous messages.

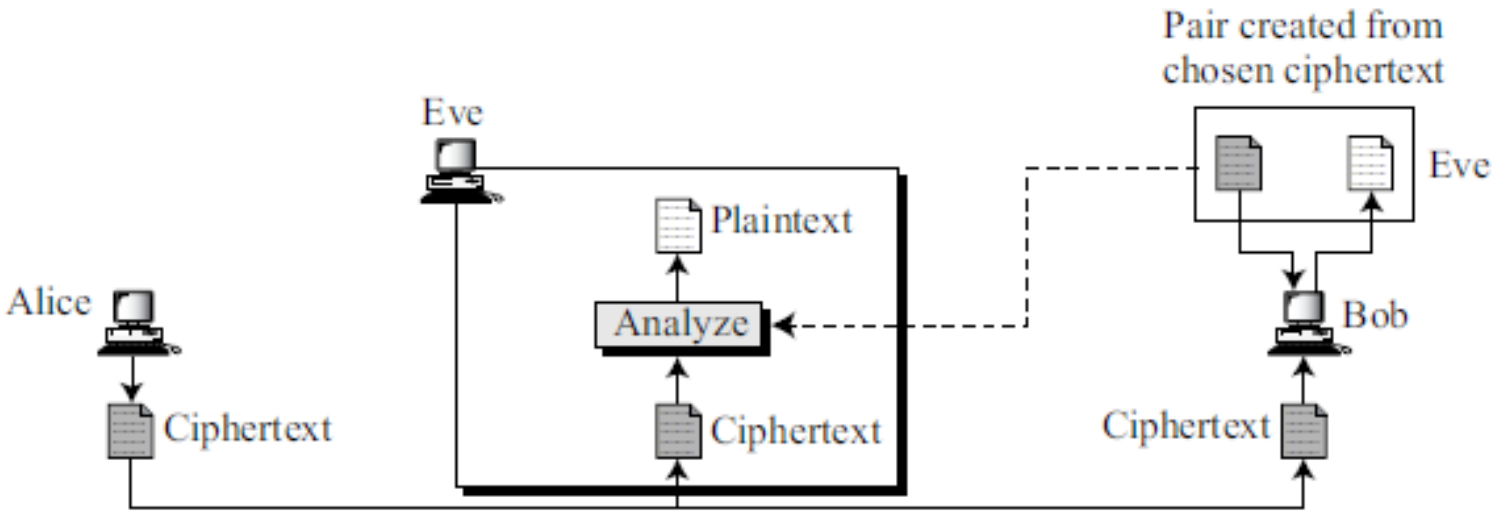
Chosen-Plaintext Attack



Chosen-plaintext attack is similar to the known-plaintext attack, but the plaintext/ ciphertext pairs have been chosen by the attacker herself.

This can happen, if Eve has access to Alice's computer.

Chosen-Ciphertext Attack



The chosen-ciphertext attack is similar to the chosen-plaintext attack, except that Eve chooses some ciphertext and decrypts it to form a ciphertext/plaintext pair.
This can happen if Eve has access to Bob's computer.

Categories of Traditional Ciphers

Two broad categories: substitution ciphers and transposition ciphers.

substitution cipher: Replace one symbol in the ciphertext with another symbol;

transposition cipher: Reorder the position of symbols in the plaintext.

3.2 SUBSTITUTION CIPHERS

A substitution cipher replaces one symbol with another.

For example, we can replace letter A with letter D, and letter T with letter Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6.

Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

Monoalphabetic Ciphers

Character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text.

Relationship between letters in the plaintext and the ciphertext is one-to-one.

Example : The cipher is probably monoalphabetic.

Plaintext: hello **Ciphertext:** KHOOR

Example : The cipher is not monoalphabetic.

Plaintext: hello **Ciphertext:** ABNZF

Additive Cipher (shift cipher or Caesar cipher)

Simplest monoalphabetic cipher is the additive cipher.

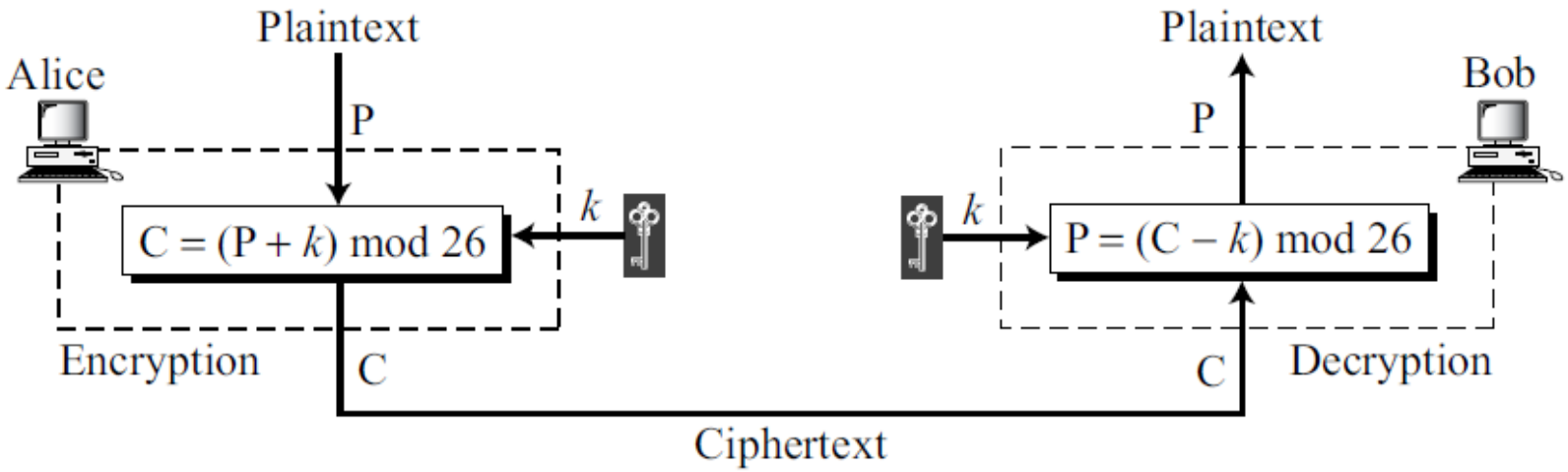
Assume: plaintext consists of lowercase letters (a to z), and ciphertext consists of uppercase letters (A to Z).

To apply mathematical operations on the plaintext and ciphertext, assign numerical values to each letter.

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

Representation of plaintext and ciphertext characters in Z_{26}

Additive Cipher (contd)



Additive Cipher (contd)

Example : Use the additive cipher with key = 15 to encrypt the message “hello”.

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

The result is “WTAAD”.

The cipher is monoalphabetic.

Additive Cipher (contd)

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

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

The result is "hello".

The operation is in modulo 26, which means that a negative result needs to be mapped to Z_{26} (for example −15 becomes 11).

Additive ciphers are sometimes referred to as shift ciphers or Caesar cipher.

Caesar Cipher

Julius Caesar used an additive cipher to communicate with his officers.

Caesar used a key of 3 for his communications.

Cryptanalysis

Additive ciphers are vulnerable to ciphertext-only attacks using exhaustive key searches (brute-force attacks).

- Key domain of the additive cipher is very small; there are only 26 keys.
- One of the keys, zero, is useless. This leaves only 25 possible keys.
- Eve can easily launch a brute force attack on the ciphertext.

Example : Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Show how she can use a brute-force attack to break the cipher.

Example : Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Show how she can use a brute-force attack to break the cipher.

Solution : Eve tries keys from 1 to 7. With a key of 7, the plaintext is “not very secure”, which makes sense

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

Additive ciphers are also subject to statistical attacks.

- This is especially true if the adversary has a long ciphertext.
- Adversary can use the frequency of occurrence of characters for a particular language.

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 : frequency for an English text of 100 characters

Sometimes it is difficult to analyze a ciphertext based only on information about the frequency of a single letter;

we may need to know the occurrence of specific letter combinations.

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

Table : Most common 2-letter groups (digrams) and 3-letter groups (trigrams) for the English text .

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.
- Most common character is I with 14 occurrences. Character I in the ciphertext probably corresponds to the character e in plaintext.
- This means key = 4. Eve deciphers the text to get

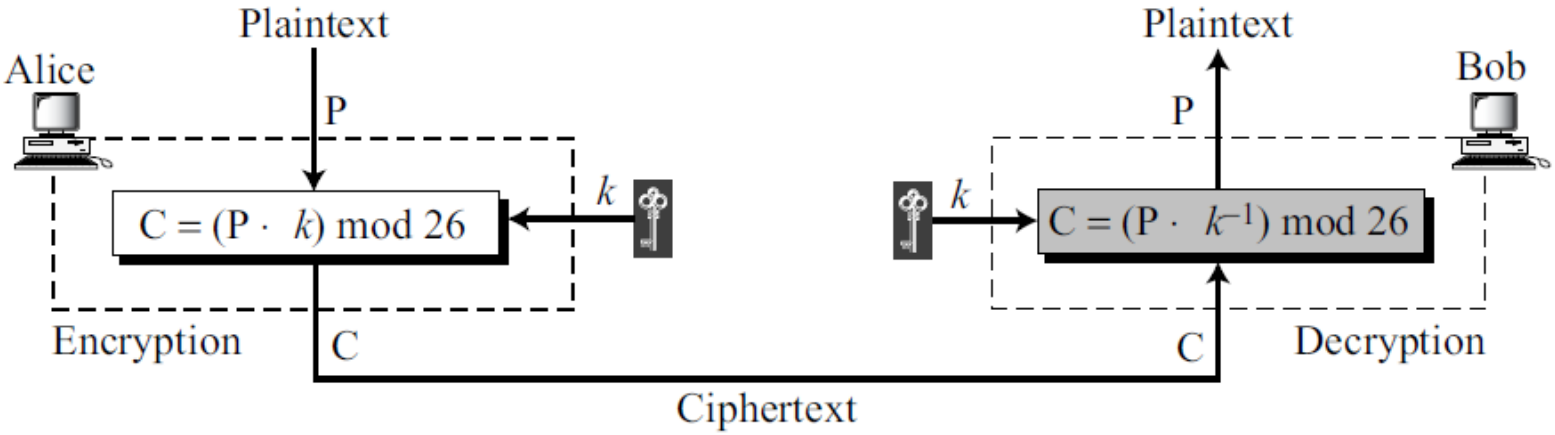
the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Multiplicative Ciphers

Encryption algorithm specifies multiplication of the plaintext by the key and the decryption algorithm specifies division of the ciphertext by the key.

Since operations are in Z_{26}, decryption here means multiplying by the multiplicative inverse of the key.

The key needs to belong to the set Z_{26}^* to guarantee that encryption and decryption are inverses of each other.



In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26}

the key is an integer in Z_{26}^*

Example : 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.

gcd(n,26)=1

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

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

Example 3.8 : We use a multiplicative cipher to encrypt the message “hello” with a key of 7. The ciphertext is “XCZZU”.

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

Affine Cipher

Combination of the additive and multiplicative ciphers with a pair of keys. The first key is used with the multiplicative cipher; the second key is used with the additive cipher.

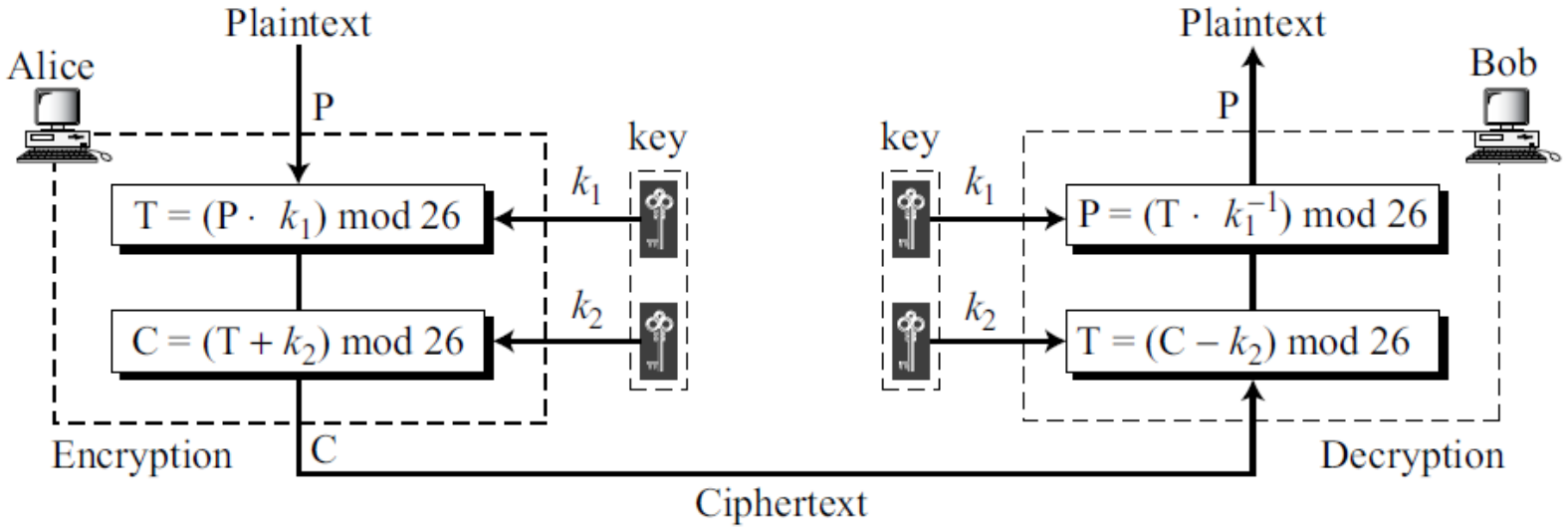
The affine cipher is actually two ciphers, applied one after another.

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

Whenever we use a combination of ciphers we should be sure that each one has an inverse at the other side of the line and that they are used in reverse order in the encryption and decryption.

If addition is the last operation in encryption, then subtraction should be the first in decryption.

Affine Cipher (contd)



In the affine cipher, the relationship between the plaintext P and the ciphertext C is

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

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

Affine Cipher (contd)

Example : 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 × 12 = 312.

Affine Cipher (contd)

Example : Use an affine cipher to encrypt the message “hello” with the key pair (7, 2).

Solution : We use 7 for the multiplicative key and 2 for the additive key. We get “ZEBBW”.

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

Affine Cipher (contd)

Example : Use the affine cipher to decrypt the message “ZEBBW” with the key pair (7, 2) in modulus 26.

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

Affine Cipher (contd)

Example 3.12

The additive cipher is a special case of an affine cipher in which k1 = 1.

The multiplicative cipher is a special case of affine cipher in which k2 = 0.

Cryptanalysis of Affine Cipher

Using chosen-plaintext attack.

Assume that Eve intercepts the following ciphertext:

PWUFFOGWCHFDWIWEJOUUNJORSMDWRHVCMWJUPVCCG

Eve also very briefly obtains access to Alice's computer and has only enough time to type a two-letter plaintext: "et".
She then tries to encrypt the short plaintext using two different algorithms, because she is not sure which one is the affine cipher.

Algorithm 1:	Plaintext: et	ciphertext: → WC
Algorithm 2:	Plaintext: et	ciphertext: → WF

Cryptanalysis of Affine Cipher

Using chosen-plaintext attack.

Algorithm 1:	Plaintext: et	ciphertext: → WC
Algorithm 2:	Plaintext: et	ciphertext: → WF

e → W	04 → 22
t → C	19 → 02

e → W	04 → 22	$(04 \times k_1 + k_2) \equiv 22 \pmod{26}$
t → C	19 → 02	$(19 \times k_1 + k_2) \equiv 02 \pmod{26}$

$$\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 16 \\ 10 \end{bmatrix} \longrightarrow k_1 = 16 \quad k_2 = 10$$

To find the key, Eve uses the following strategy:

a. Eve knows that if the first algorithm is affine, she can construct the following two equations based on the first data set.

e → W	04 → 22	$(04 \times k_1 + k_2) \equiv 22 \pmod{26}$
t → C	19 → 02	$(19 \times k_1 + k_2) \equiv 02 \pmod{26}$

These two congruence equations can be solved and the values of k1 and k2 can be found.

However, this answer is not acceptable because k1 = 16 cannot be the first part of the key. Its value, 16, does not have a multiplicative inverse in Z_{26}^*.

$$\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 16 \\ 10 \end{bmatrix} \longrightarrow k_1 = 16 \quad k_2 = 10$$

b. Eve now tries the result of the second set of data.

e → W	04 → 22	$(04 \times k_1 + k_2) \equiv 22 \pmod{26}$
t → F	19 → 05	$(19 \times k_1 + k_2) \equiv 05 \pmod{26}$

Square matrix and its inverse are the same.
Now she has k1 = 11 and k2 = 4.
This pair is acceptable because k1 has a multiplicative inverse in Z_{26}^*.

She tries the pair of keys (19, 22), which are the inverse of the pair (11, 4), to decipher the message.

The plaintext is

best time of the year is spring when flowers bloom

Monoalphabetic Substitution Cipher

Additive, multiplicative, and affine ciphers have small key domains, they are very vulnerable to brute-force attack.

- After Alice and Bob agreed to a single key, that key is used to encrypt each letter in the plaintext or decrypt each letter in the ciphertext.
- In other words, the key is independent from the letters being transferred.

Monoalphabetic Substitution Cipher (contd)

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.

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)

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

ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

Mapping table

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

The size of the key space is 26! (almost 4×10^{26}).

Brute-force attack is difficult

The monoalphabetic ciphers do not change the frequency of characters in the ciphertext, which makes the ciphers vulnerable to statistical attack.

Polyalphabetic Ciphers

Each occurrence of a character may have a different substitute.

Relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

Advantage of hiding the letter frequency of the underlying language.

Polyalphabetic Ciphers (contd)

Here each ciphertext character dependent on both the corresponding plaintext character and the position of the plaintext character in the message.

key stream $k = (k_1, k_2, k_3, \ldots)$

k_i is used to encipher the i^{th} character in the plaintext to create the i^{th} character in the ciphertext.

Autokey Cipher

simple polyalphabetic cipher called the autokey cipher.

In this cipher, the key is a stream of subkeys, in which each subkey is used to encrypt the corresponding character in the plaintext.

- First subkey is a predetermined value secretly agreed upon by Alice and Bob.
- Second subkey is the value of the first plaintext character (between 0 and 25).
- Third subkey is the value of the second plaintext. And so on.

Autokey Cipher

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

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

Autokey implies that the subkeys are automatically created from the plaintext cipher characters during the encryption process.

Example : Assume that Alice and Bob agreed to use an autokey cipher with initial key value $k_1 = 12$.

message "Attack is today" and K1=12

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**

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

Cryptanalysis

- Hides the single-letter frequency statistics of the plaintext.
- It is still as vulnerable to the brute-force attack as the additive cipher.
- The first subkey can be only one of the 25 values (1 to 25).
- Need polyalphabetic ciphers that not only hide the characteristics of the language but also have large key domains.

Playfair Cipher

Playfair cipher used by the British army during World War I.

Secret key in this cipher is made of 25 alphabet letters arranged in a 5× 5 matrix (letters I and J are considered the same when encrypting).

Different arrangements of the letters in the matrix can create many different secret keys.

Here dropped the letters in the matrix diagonally starting from the top right-hand corner.

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

An example of a secret key in the Playfair cipher

Playfair Cipher (contd)

Before encryption:

- ✓ if the two letters in a pair are the same, a bogus letter is inserted to separate them.
- ✓ After inserting bogus letters, if the number of characters in the plaintext is odd, one extra bogus character is added at the end to make the number of characters even.

Playfair Cipher (contd)

The cipher uses three rules for encryption:

If the two letters in a pair

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

Playfair Cipher (contd)

- The key is a stream of subkeys in which the subkeys are created two at a time.
- Encryption algorithm takes a pair of characters from the plaintext and creates a pair of subkeys by following the above-mentioned rules.
- The key stream depends on the position of the character in the plaintext.

$$P = P_1P_2P_3 \ldots \qquad C = C_1C_2C_3 \ldots \qquad k = [(k_1, k_2), (k_3, k_4), \ldots]$$

$$\text{Encryption: } C_i = k_i \qquad \text{Decryption: } P_i = k_i$$

Playfair Cipher (contd)

Example : Encrypt the plaintext "hello" using the key in Figure 3.13.

- When we group the letters in two-character pairs, we get "he, ll, o".
- We need to insert an x between the two l's (els), giving "he, lx, lo".
- We have

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

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

The cipher is actually a polyalphabetic cipher

Figure 3.13

Cryptanalysis of a Playfair Cipher

Brute-force attack on a Playfair cipher is very difficult.

The size of the key domain is 25! (factorial 25).

In addition, the encipherment hides the single-letter frequency of the characters.

Vigenere Cipher

Key stream is a repetition of an initial secret key stream of length m, where we have $1 \leq m \leq 26$.

The cipher can be described as follows

$$P = P_1 P_2 P_3 \ldots \qquad C = C_1 C_2 C_3 \ldots \qquad K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$$

$$\text{Encryption: } C_i = P_i + k_i \qquad \text{Decryption: } P_i = C_i - k_i$$

where $(k_1, k_2, \ldots, k_m)$ is the initial secret key agreed to by Alice and Bob.

Vigenere Cipher

The Vigenere key stream does not depend on the plaintext characters; it depends only on the position of the character in the plaintext.

Vigenere Cipher

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

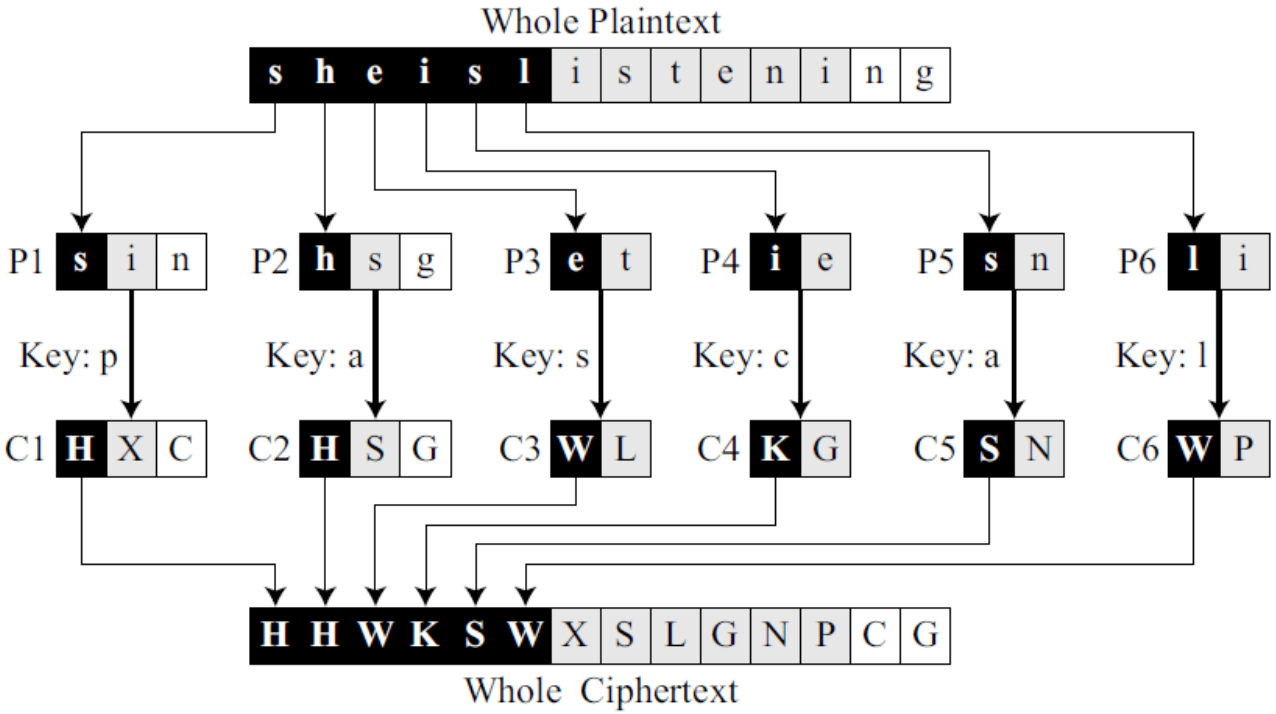
The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

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**

Example 3.17

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

There are m pieces of the plaintext, each encrypted with a different key, to make m pieces of ciphertext.



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

Vigenere Tableau

Another way to look at Vigenere ciphers is through what is called a Vigenere tableau shown in Table 3.3.

	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

A Vigenere tableau

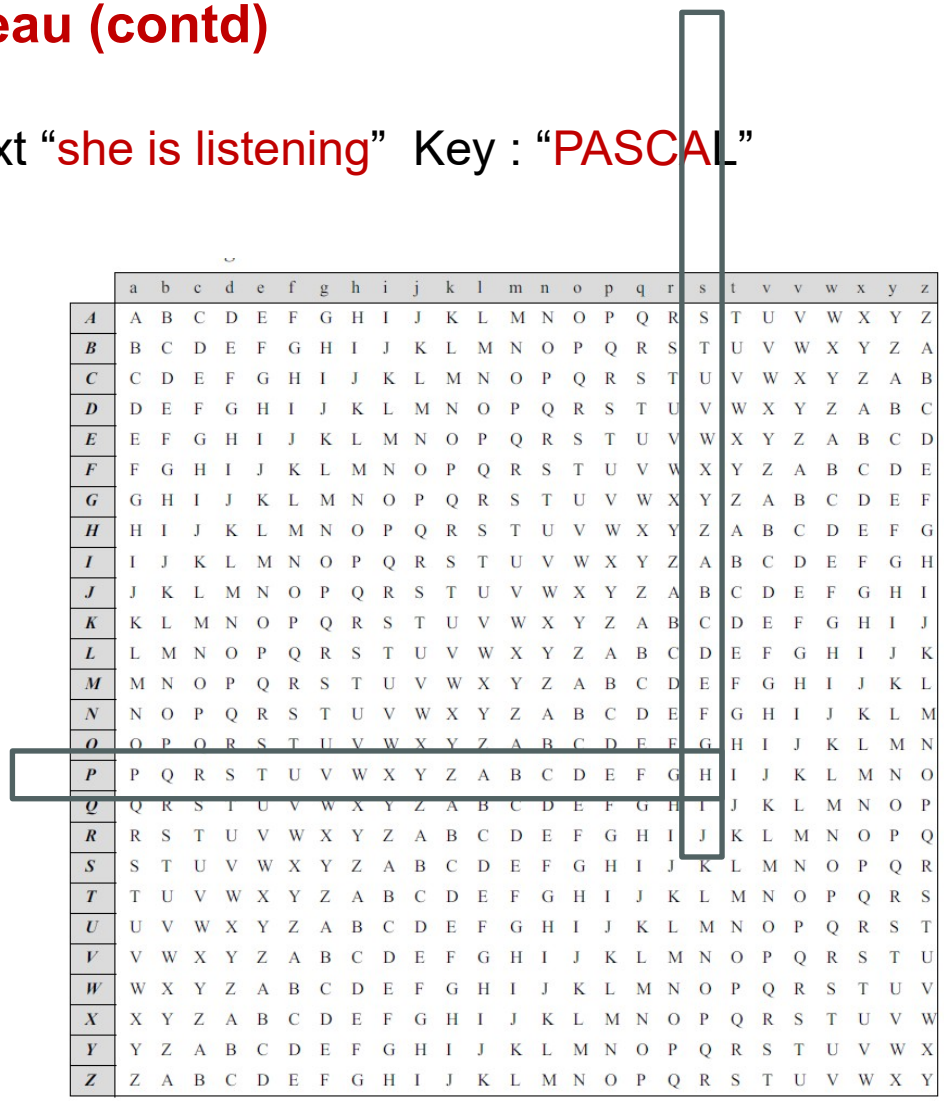
First row shows the plaintext character to be encrypted.

First column contains the characters to be used by the key.

Rest of the tableau shows the ciphertext characters.

Vigenere Tableau (contd)

Example: plaintext “she is listening” Key : “PASCAL”



	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

Find “s” in the first row, “P” in the first column, the cross section is the ciphertext character “H”.
Find “h” in the first row and “A” in the second column, the cross section is the ciphertext character “H”.

Hill cipher

Here the plaintext is divided into equal-size blocks.

Blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block.

Hill cipher belongs to a category of ciphers called block ciphers.

Other ciphers studied so far belong to the category called stream ciphers.

Hill Cipher

★ Review few terminologies from linear algebra.

★ Concepts to be known:

- Matrix arithmetic modulo 26.
- Square matrix.
- Determinant.
- Multiplicative inverse.

This can be expressed as

$C = E(K,P) = P \times K \bmod 26$

$P = D(K,C) = C\ K^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26$

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

Encryption

$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$

$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$

$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$

Question: Encrypt "pay more money" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution:

p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

Key = 3 x 3 matrix.

PT = pay mor emo ney

Question: Encrypt "pay more money" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Plaintext : pay more money

Ciphertext : RRLMWBKASPDH

Hill cipher

In a Hill cipher, the key is a square matrix of size m × m in which m is the size of the block.

If we call the key matrix K, each element of the matrix is $k_{i,j}$ as shown in Figure 3.15.

Figure 3.15 *Key in the Hill cipher*

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

Hill cipher (contd)

Let us show how one block of the ciphertext is encrypted.

Let m characters in the plaintext block P1, P2, …, Pm.

The corresponding characters in the ciphertext block are C1, C2, …, Cm.

Then

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

Hill cipher (contd)

Each ciphertext character such as C1 depends on all plaintext characters in the block (P1, P2, …, Pm).

Not all square matrices have multiplicative inverses in Z_{26}, so Alice and Bob should be careful in selecting the key.

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

Hill cipher (contd)

Example 3.20

The plaintext is an l × m matrix in which l is the number of blocks.

The plaintext "code is ready" can make a 3 × 4 matrix when adding extra bogus character "z" to the last block and removing the spaces.

The ciphertext is "OHKNIHGKLISS".

Bob can decrypt the message using the inverse of the key matrix.

Figure 3.16 *Example 3.20*

$$\underset{\mathbf{C}}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} = \underset{\mathbf{P}}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} \underset{\mathbf{K}}{\begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}}$$

a. Encryption

Hill cipher (contd)

Figure 3.16 *Example 3.20*

$$\mathbf{C} = \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} = \mathbf{P} \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} \mathbf{K} \begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}$$

a. Encryption

$$\mathbf{P} = \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} = \mathbf{C} \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} \mathbf{K}^{-1} \begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}$$

b. Decryption

3.3 TRANSPOSITION CIPHERS

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

- A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext.
- A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext.

Transposition cipher reorders (transposes) the symbols.

Keyless Transposition Ciphers

Keyless transposition ciphers is the Simple transposition ciphers.

There are two methods for permutation of characters.

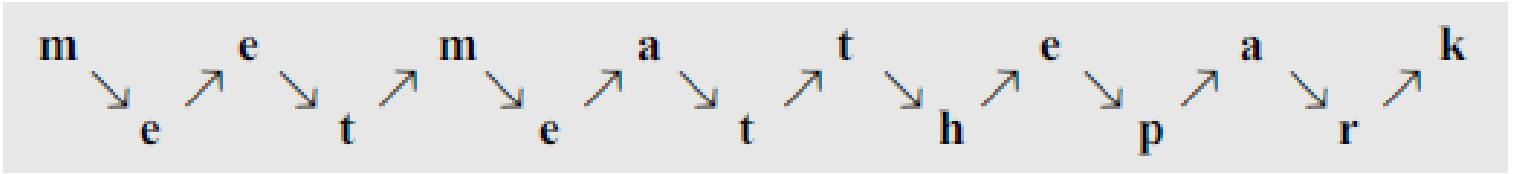
First method: the text is written into a table column by column and then transmitted row by row.

Second method: the text is written into the table row by row and then transmitted column by column.

Example : A good example of a keyless cipher using the first method is the rail fence cipher.

Here plaintext is arranged in two lines as a zigzag pattern (column by column); the ciphertext is created reading the pattern row by row.

Example : message “Meet me at the park”



ciphertext is : “MEMATEAKETETHPR”

The cryptanalysis of the ciphertext would be very easy for Eve

Example 3.23

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	

cipher text : “MMTAEEHREAEKTTP”

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

second character in the plaintext has moved to the fifth position in the ciphertext;
Third character has moved to the ninth position; and so on.

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

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 (row by row, for example) and reading it in another way (column by column, for example).

The permutation is done on the whole plaintext to create the whole cipher text.

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

Example 3.25

message “Enemy attacks tonight” .

Example: groups of 5 characters and then permute the characters in each group.

Grouping after adding a bogus character at the end to make the equal size group.

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.

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

3rd character in the plaintext block becomes the first character in the ciphertext block; the first character in the plaintext block becomes the second character in the ciphertext block; and so on.

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

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

Alice sends the ciphertext “EEMYNTAACTTKONSHITZG” to Bob.

Bob divides the ciphertext into 5-character groups and, using the key in the reverse order, finds the plaintext.

Combining Two Approaches

Encryption or decryption is done in three steps.

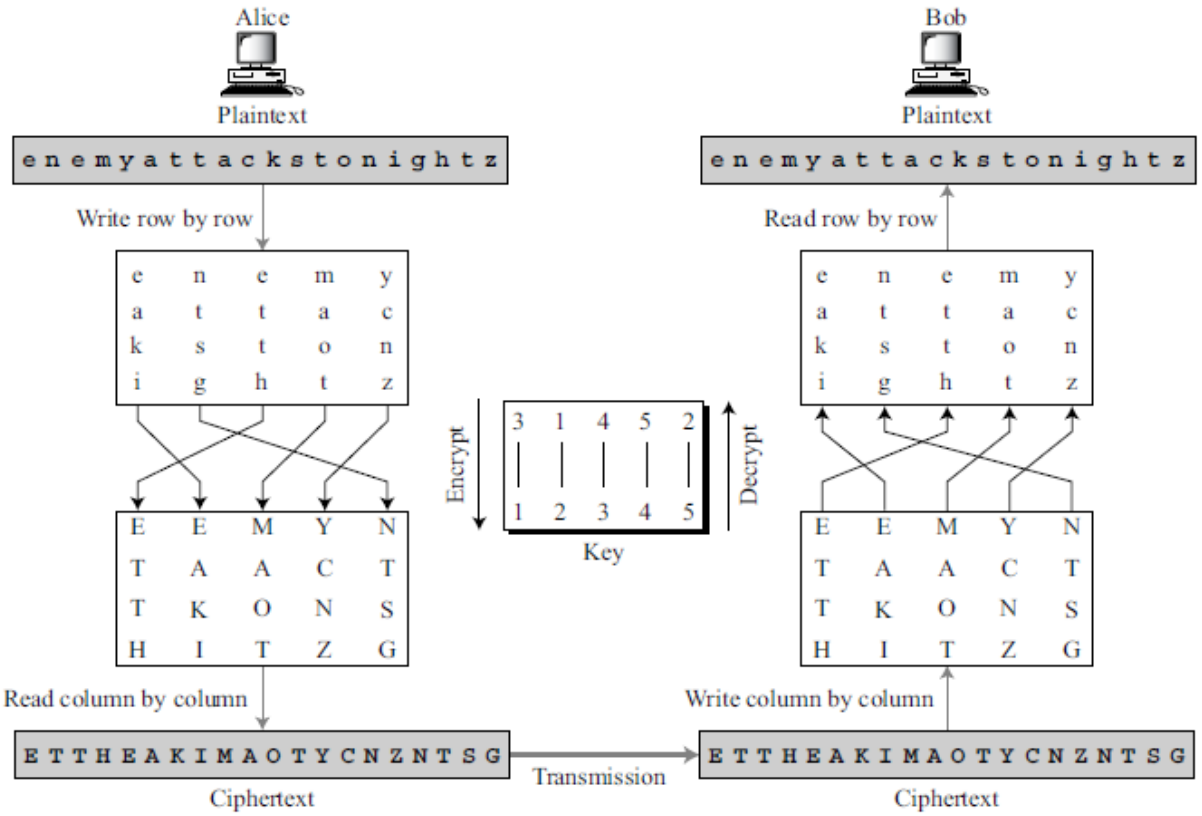
- First, the text is written into a table row by row.
- Second, the permutation is done by reordering the columns.
- Third, the new table is read column by column.

The first and third steps provide a keyless global reordering; the second step provides a blockwise keyed reordering.

These types of ciphers are often referred to as keyed columnar transposition ciphers or just columnar transposition ciphers.

Combining Two Approaches

Example 3.26: Encryption of "Enemy attacks tonight"



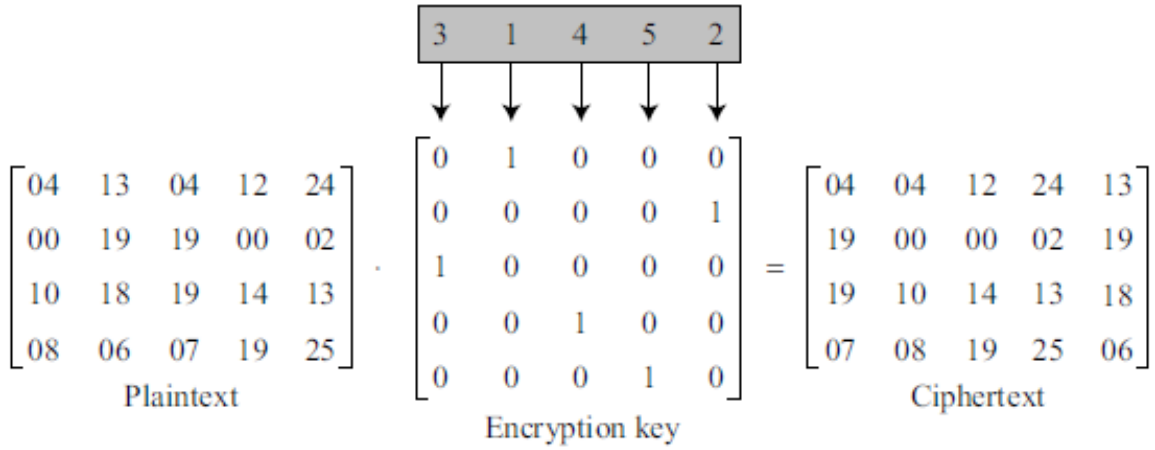
Using Matrices

The plaintext and cipher text are $l \times m$ matrices representing the numerical values of the characters;
the keys are square matrices of size $m \times m$.

In this case is the inverse of the encryption matrix, there is no need to invert the matrix, the encryption key matrix can simply be transposed to get the decryption key matrix.

Example 3.27

Note that the matrix multiplication provides only the column permutation of the transposition;



Representation of the key as a matrix in the transposition cipher

Cryptanalysis of Transposition Ciphers

Transposition ciphers are vulnerable to several kinds of ciphertext-only attacks.

Statistical Attack

A transposition cipher does not change the frequency of letters in the ciphertext;
So the first attack that can be applied is single-letter frequency analysis.

However, transposition ciphers do not preserve the frequency of digrams and trigrams. This means that Eve cannot use these tools.

Brute-Force Attack

Eve can try all possible keys to decrypt the message.

Number of keys can be huge (1! + 2! + 3! + . . . + L!), where L is the length of the ciphertext.

A better approach is to guess the number of columns. Eve knows that the number of columns divides L.

For example, if the length of the cipher is 20 characters, .

the number of columns can be a combination of these factors (1, 2, 4, 5, 10, 20).

The first (only one column) is out of the question and the last (only one row) is unlikely.

Example 3.28

ciphertext message “EEMYNTAACTTKONSHITZG”.

Message length L = 20. Number of columns can be 1, 2, 4, 5, 10, or 20.

a. If the number of columns is 2.

Two permutations are (1, 2) and (2, 1).

The first one means there would be no permutation.

Eve tries the second one.

Eve divides ciphertext into 2-character units: “EE MY NT AA CT TK ON SH IT ZG”.

She then tries to permute each of these getting “ee ym nt aa tc kt no hs ti gz”, which does not make sense.

Example 3.28

ciphertext message "EEMYNTAACTTKONSHITZG".

Message length L = 20. Number of columns can be 1, 2, 4, 5, 10, or 20.

b. If the number of columns is 4, there are 4! = 24 permutations.

The first one (1 2 3 4) means there would be no permutation.

Eve needs to try the rest. After trying all 23 possibilities, Eve finds no plaintext that makes sense.

c. If the number of columns is 5, there are 5! = 120 permutations.

The first one (1 2 3 4 5) means there would be no permutation.

Eve needs to try the rest.

The permutation (2 5 1 3 4) yields a plaintext "enemyattackstonightz" that makes sense after removing the bogus letter z and adding spaces

Pattern Attack

The ciphertext created from a keyed transposition cipher has some repeated patterns. Example:

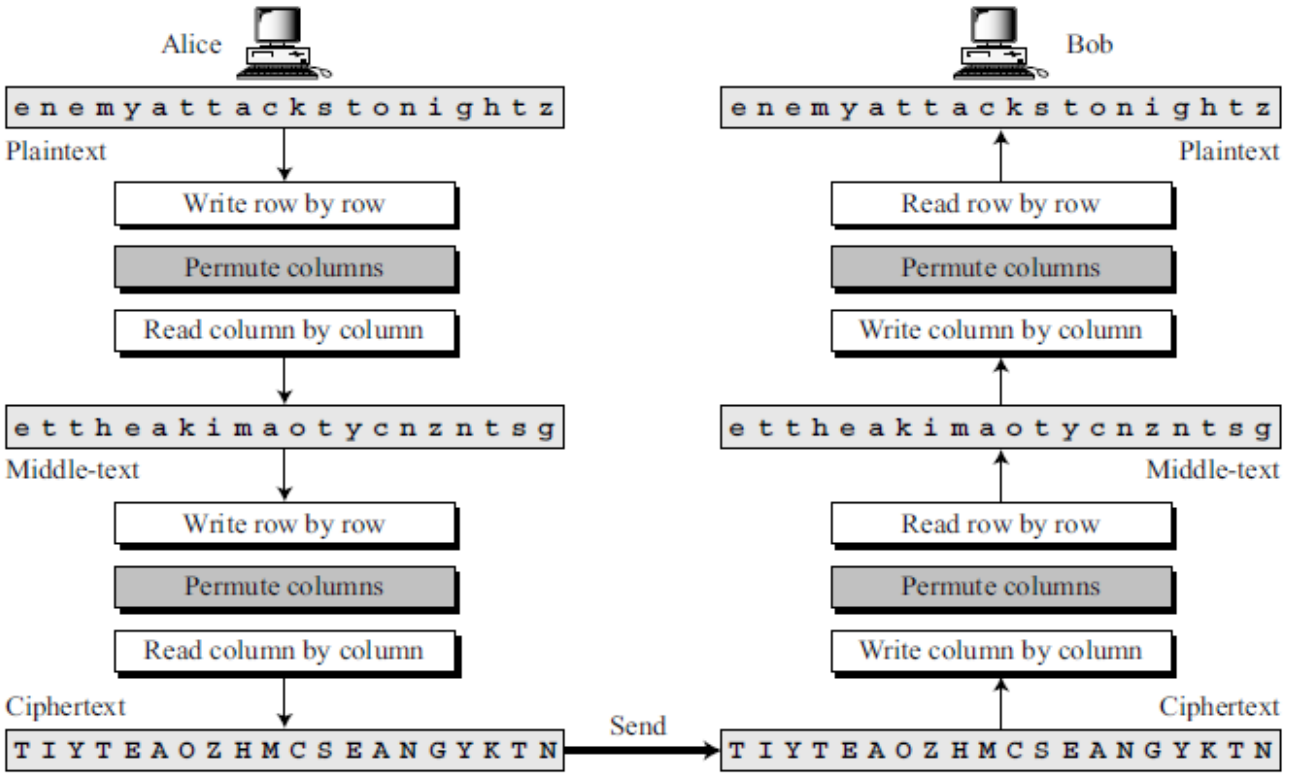
03	**08**	**13**	**18**	*01*	*06*	*11*	*16*	**04**	**09**	**14**	**19**	*05*	*10*	*15*	*20*	**02**	**07**	**12**	**17**

The 1st character in the ciphertext comes from the 3rd character in the plaintext. The 2nd character in the ciphertext comes from the 8th character in the plaintext and so on.

There is a pattern: We have five groups: (3, 8, 13, 18), (1, 6, 11, 16), (4, 9, 14, 19), (5, 10, 15, 20), and (2, 7, 12, 17). In all groups, the difference between the two adjacent numbers is 5.

If Eve knows or can guess the number of columns (5 in this case), she can organize the ciphertext in groups of four characters. Permuting the groups can provide the clue to finding the plaintext.

Double Transposition Ciphers



Double transposition ciphers can make the job of the cryptanalyst difficult.

An example of such a cipher would be the one that repeats twice the algorithm used for encryption and decryption.

A different key can be used in each step, but normally the same key is used.

Although, the cryptanalyst can still use the single-letter frequency attack on the ciphertext, a pattern attack is now much more difficult. The pattern analysis of the text shows

13	16	05	07	03	06	10	20	18	04	10	12	01	09	15	17	08	11	19	02

3.4 STREAM AND BLOCK CIPHERS

Symmetric ciphers into two broad categories: stream ciphers and block ciphers.

Although the definitions are normally applied to modern ciphers, this categorization also applies to traditional ciphers.

Stream Ciphers

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

We have a plaintext stream, a ciphertext stream, and a key stream.

$$P = P_1P_2P_3, \ldots \qquad C = C_1C_2C_3, \ldots \qquad K = (k_1, k_2, k_3, \ldots)$$

$$C_1 = E_{k1}(P_1) \qquad C_2 = E_{k2}(P_2) \qquad C_3 = E_{k3}(P_3) \ldots$$

Idea behind a stream cipher.

Characters in the plaintext are fed into the encryption algorithm, one at a time; the ciphertext characters are also created one at a time.

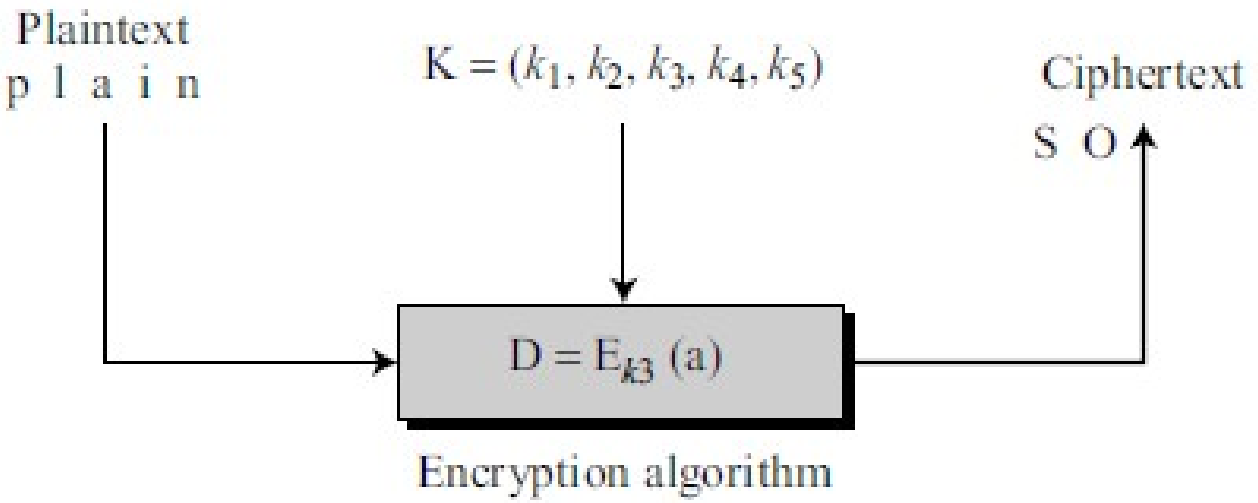
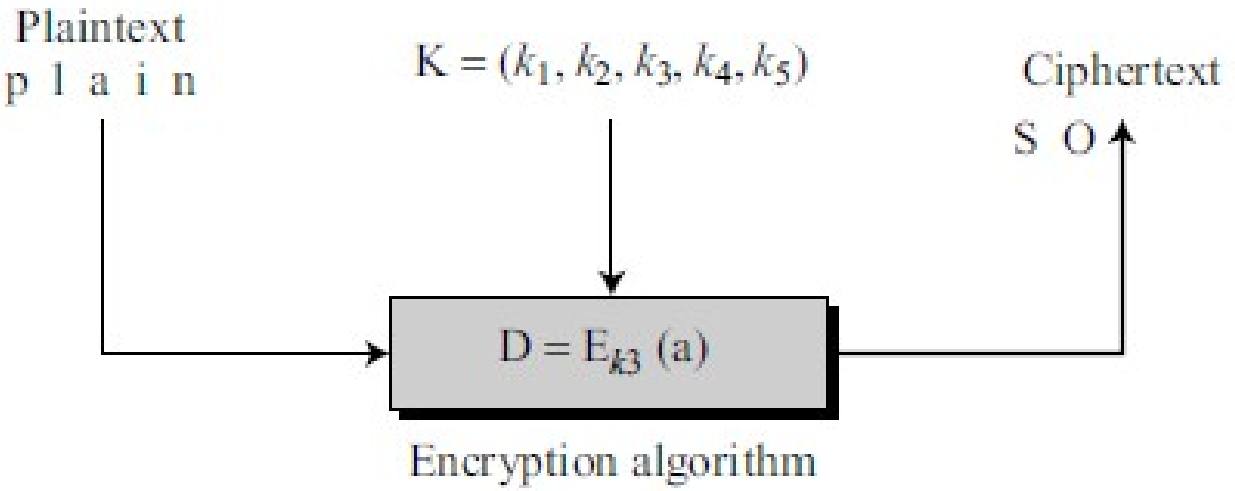


Figure shows the moment where the third character in the plaintext stream is being encrypted using the third value in the key stream. The result creates the third character in the ciphertext stream.

The key stream, can be created in many ways.

- ✓ It may be a stream of predetermined values;
- ✓ it may be created one value at a time using an algorithm.
- ✓ The values may depend on the plaintext or ciphertext characters.
- ✓ The values may also depend on the previous key values.



Example 3.30

Additive ciphers can be categorized as stream ciphers.
The key stream is considered as a predetermined stream of keys or K = (k, k, …, k).
Each character in the ciphertext depends only on the corresponding character in the plaintext,

Example 3.31

The monoalphabetic substitution ciphers are also stream ciphers.
Each value of the key stream in this case is the mapping of the current plaintext character to the corresponding ciphertext character in the mapping table.

Example 3.32

Vigenere ciphers are also stream ciphers.
The key stream is a repetition of m values, where m is the size of the keyword.

$$\mathrm{K} = (k_1, k_2, \ldots k_{\mathrm{m}}, k_1, k_2, \ldots k_m, \ldots)$$

Example 3.33

Dividing stream ciphers based on their key streams.

monoalphabetic vs polyalphabetic.

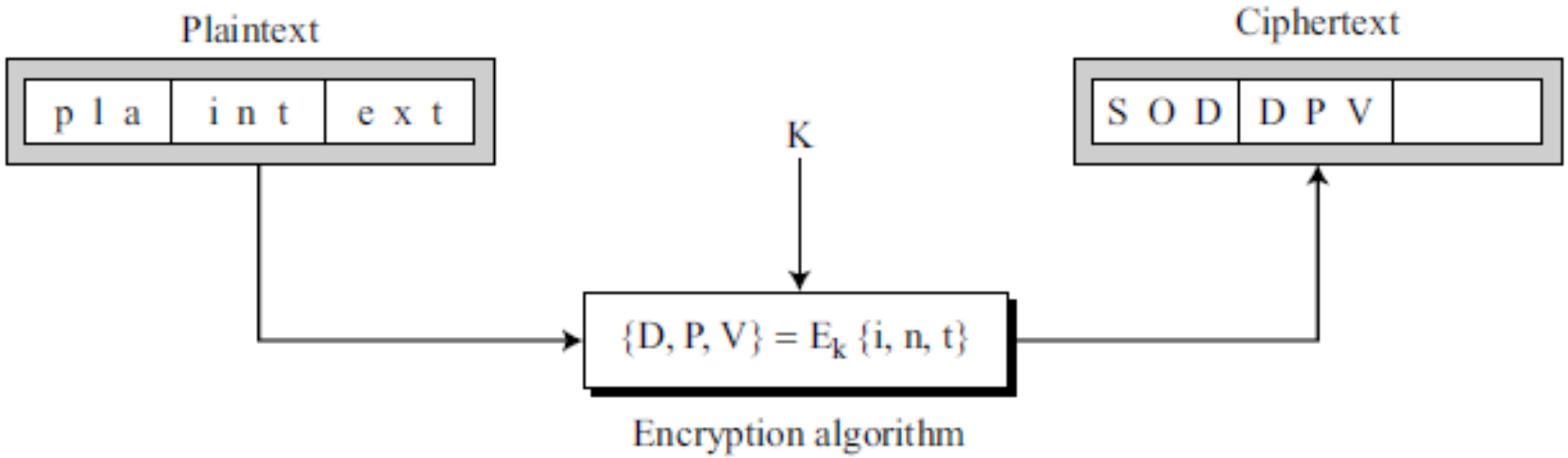
Additive ciphers are definitely monoalphabetic.

Monoalphabetic substitution ciphers are definitely monoalphabetic.

Vigenere ciphers are polyalphabetic.

Block Ciphers

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.
Single key is used to encrypt the whole block even if the key is made of multiple values.



Example 3.34
Playfair ciphers are block ciphers. The size of the block is m = 2.

Example 3.35
Hill ciphers are block ciphers.

Example 3.36
Every block cipher is a polyalphabetic cipher because each character in a ciphertext block depends on all characters in the plaintext block.