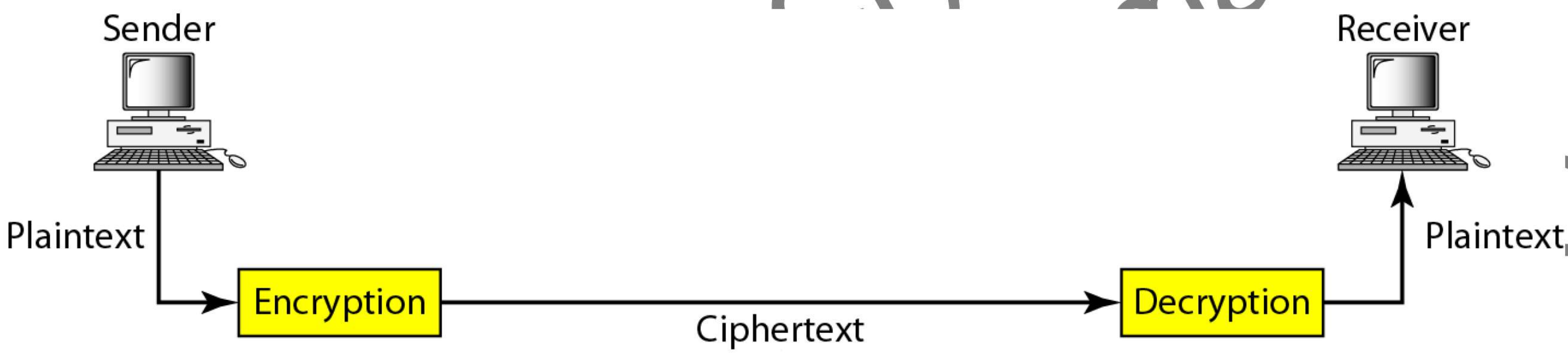
Cryptography and Network Security

Figure 30.1 *Cryptography components*



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

Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver

  $Y = E_K(X)$

  $X = D_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Types of encryption

- Symmetric Encryption
- Asymmetric Encryption

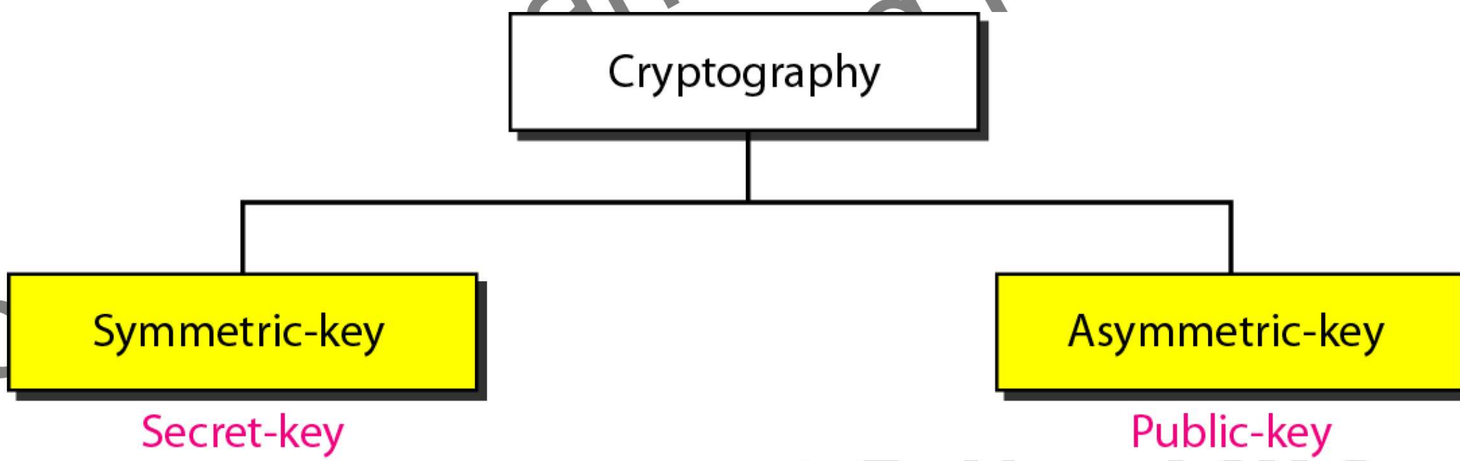
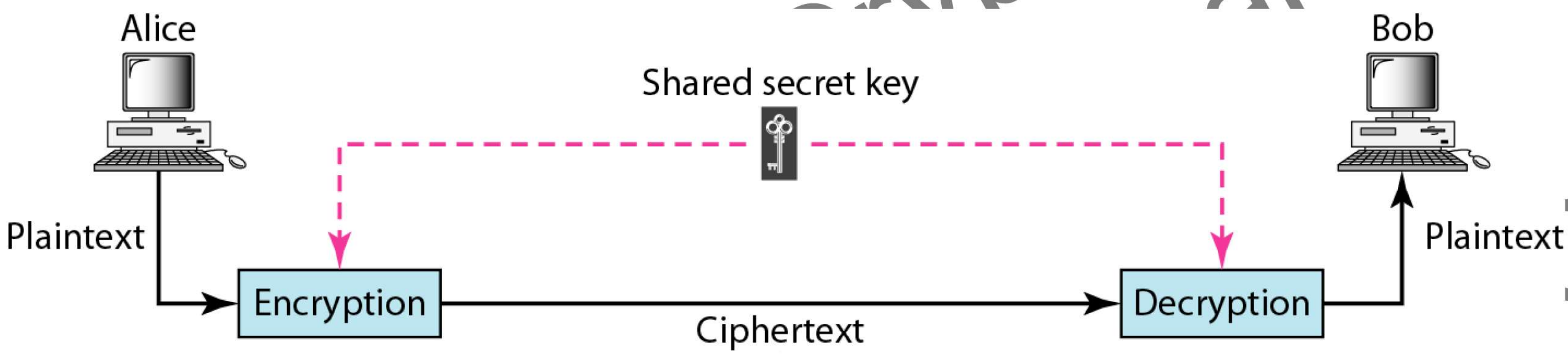


Figure 30.3 *Symmetric-key cryptography*



Symmetric Encryption

- A systems where by knowing the algorithm and the key, you can both encrypt and decrypt a message. This kind of encryption is known as symmetric encryption.
- The big advantage of this kind of encryption is that it is easy because it does not require complex math and much calculation to execute.
- On the other hand, it makes critical the key exchange moment and key management. In fact, the key has to be exchanged before the transmission can start between the parties, and it has to be done securely.

Block chain and CryptoCurrencies
Dr. Ahlad Kumar

Symmetric Encryption

- As for the key management problem, since both parties know the same secret (in fact, this kind of cryptography is also called shared secret), if you have multiple people that have to communicate with each other, you will need $n(n-1)/2$ keys
- This means that in a group of 20 people, you'll need 190 keys.

Symmetric Encryption

- The types of symmetric encryption that are used are as follows:
  – Stream cipher (ex, RC4) (WEP, WPA, SSL, TSL)
  – Block cipher (AES, DES, 3DES)

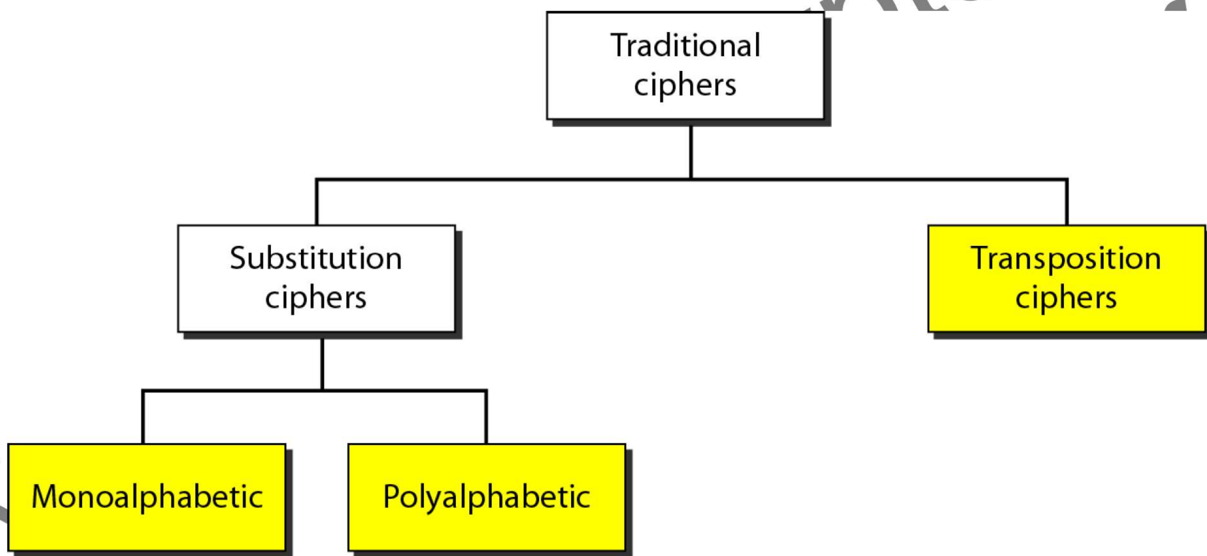
Note

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Cryptography

- can characterize by:
  - type of encryption operations used
    - substitution / transposition / product
  - number of keys used
    - single-key or private / two-key or public
  - way in which plaintext is processed
    - block / stream

Figure 30.7 *Traditional ciphers*



Monoalphabetic Ciphers

We first discuss a group of substitution ciphers called the **monoalphabetic ciphers.** In monoalphabetic substitution, a 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. For example, if the algorithm says that letter A in the plaintext is changed to letter D, every letter A is changed to letter D. In other words, the relationship between letters in the plaintext and the ciphertext is one-to-one.

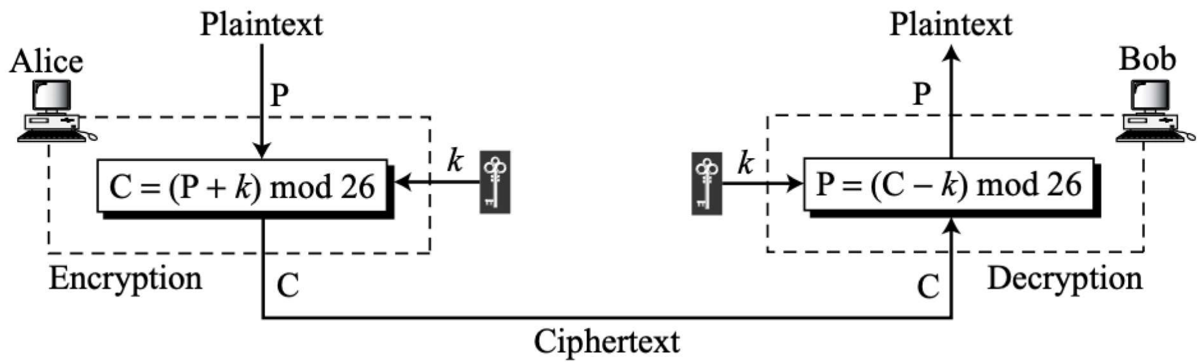
In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Figure 3.8 *Representation of plaintext and ciphertext characters in $\mathbf{Z}_{26}$*

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/Shift Cipher/Caesar Cipher

Figure 3.9 *Additive cipher*



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

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

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

The result is “WTAAD”. Note that the cipher is monoalphabetic because two instances of the same plaintext character (l’s) are encrypted as the same character (A).

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

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

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

Note

The shift cipher is sometimes referred to as the Caesar cipher. (monoalphabetic)

CryptAnalysis
BruteForce Attack

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

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

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

Crypt-Analysis
Statistical Attack

Table 3.1 *Frequency of occurrence of letters in an English text*

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		

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

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

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

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

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 shows that 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

Polyalphabetic Ciphers

Polyalphabetic Ciphers

In **polyalphabetic substitution,** each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many. For example, "a" could be enciphered as "D" in the beginning of the text, but as "N" at the middle. Polyalphabetic ciphers have the advantage of hiding the letter frequency of the underlying language. Eve cannot use single-letter frequency statistic to break the ciphertext.

Vigenère Cipher

One interesting kind of polyalphabetic cipher was designed by Blaise de Vigenere, a sixteenth-century French mathematician. A **Vigenere cipher** uses a different strategy to create the key stream. The 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 where $(k_1, k_2, \ldots, k_m)$ is the initial secret key agreed to by Alice and Bob.

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

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

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**

Transposition Ciphers

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. In other words, a transposition cipher reorders (transposes) the symbols.

Keyless Transposition Ciphers

Simple transposition ciphers, which were used in the past, are keyless. There are two methods for permutation of characters. In the first method, the text is written into a table column by column and then transmitted row by row. In the second method, the text is written into the table row by row and then transmitted column by column.

Keyless Transposition Cipher

A good example of a keyless cipher using the first method is the **rail fence cipher.** In this cipher, the plaintext is arranged in two lines as a zigzag pattern (which means column by column); 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**		**m**		**a**		**t**		**e**		**a**		**k**
	e		**t**		**e**		**t**		**h**		**p**		**r**	

ciphertext "MEMATEAKETETHPR"

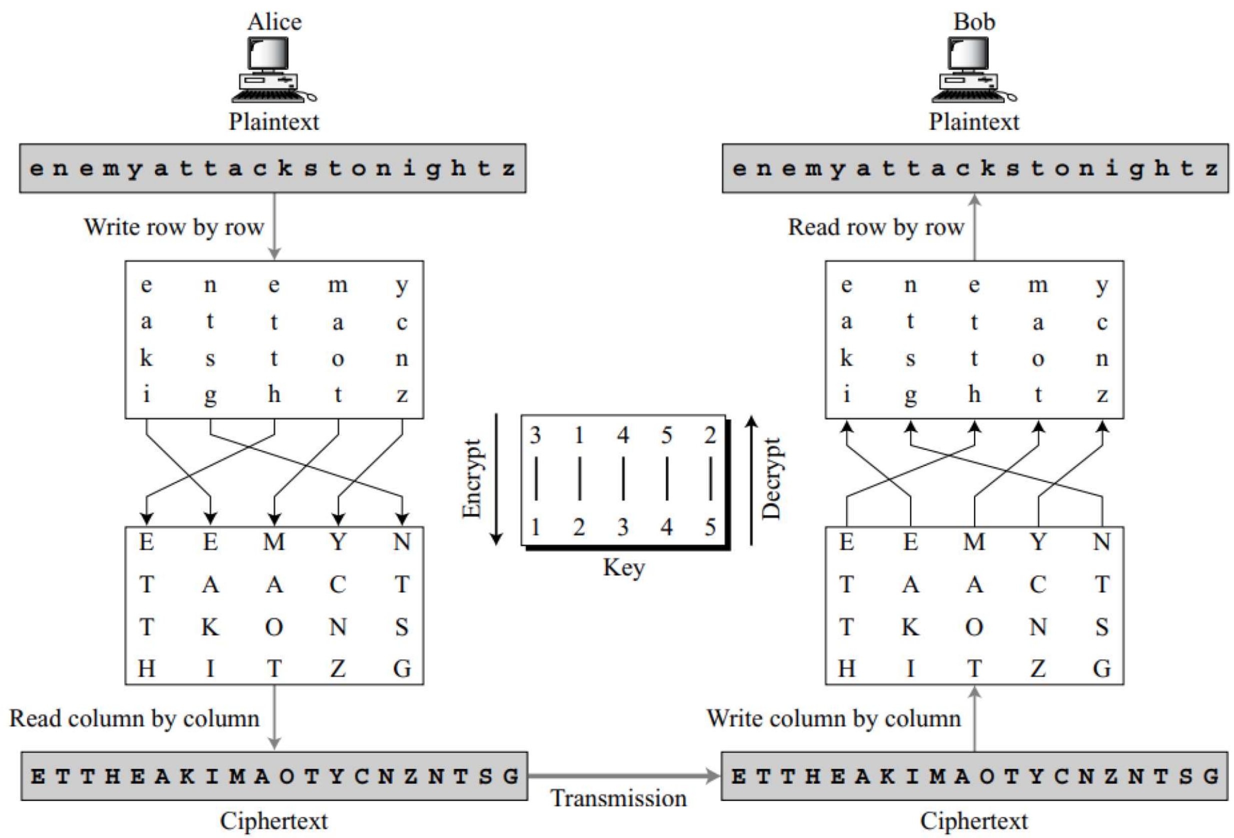
Keyless Transposition Cipher

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	

the ciphertext “MMTAEEHREAEKTTP”

Combination Transposition Cipher



Key Transposition Cipher

Alice needs to send the message “Enemy attacks tonight” to Bob. Alice and Bob have agreed to divide the text into groups of five characters and then permute the characters in each group. The following shows the grouping after adding a bogus character at the end to make the last group the same size as the others.

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. For this message, assume that Alice and Bob used the following key:

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

The third 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. 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.

Asymmetric Encryption

- Asymmetric encryption has some core differences from symmetric encryption.
- The first that you can immediately notice is that in asymmetric encryption there are two keys: one public key to encrypt and a private key to decrypt.
- From this concept, one of the names of asymmetric encryption is derived: public key encryption.
- This approach does simplify greatly the key exchange and key management. For the key management, you only need a pair of keys (private/public) for each person. So if you have 20 people that have to communicate between themselves, you'll only need 20 pairs of keys.

Figure 30.4 *Asymmetric-key cryptography*

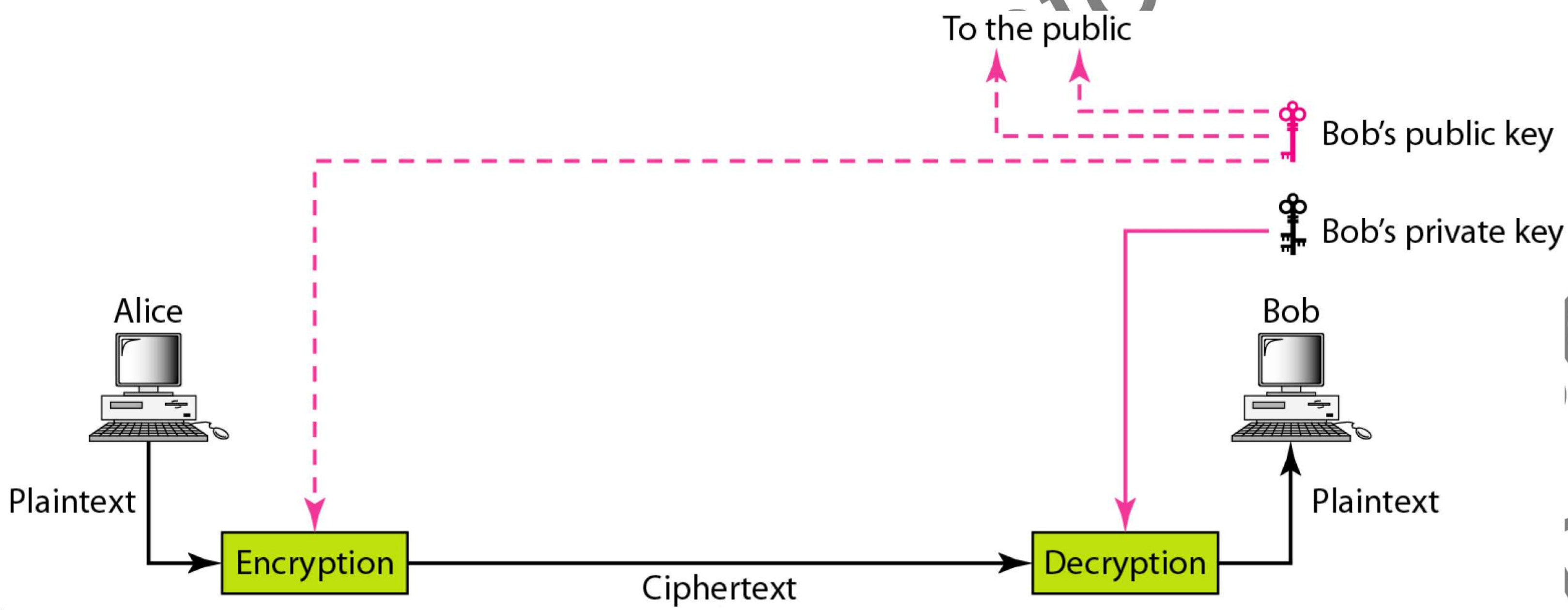
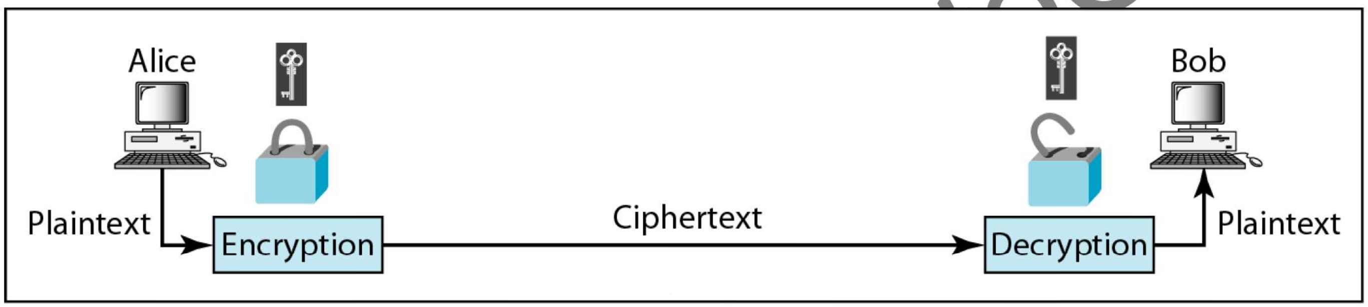
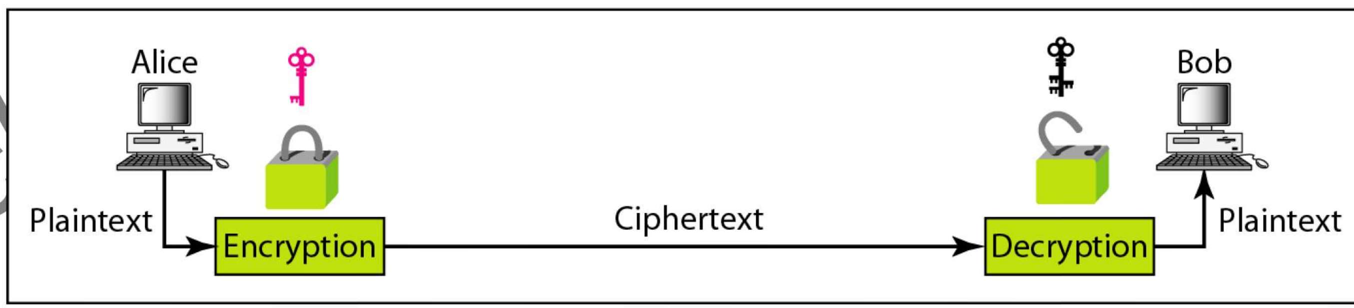


Figure 30.6 *Comparison between two categories of cryptography*

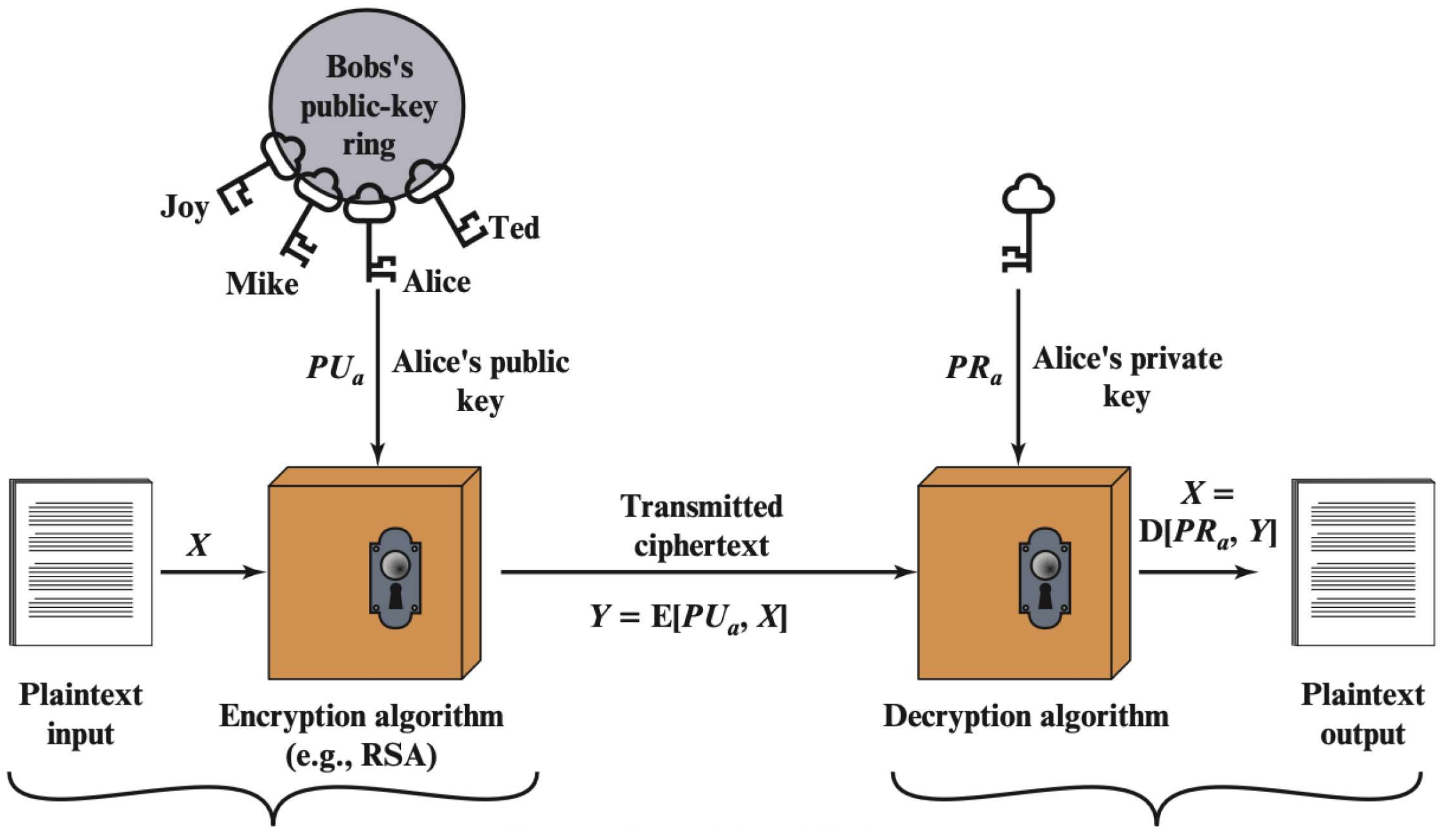


a. Symmetric-key cryptography



b. Asymmetric-key cryptography

Public Key Cryptography for Encryption/Decryption



(a) Encryption with public key

Public Key Cryptography for Digital Signatures

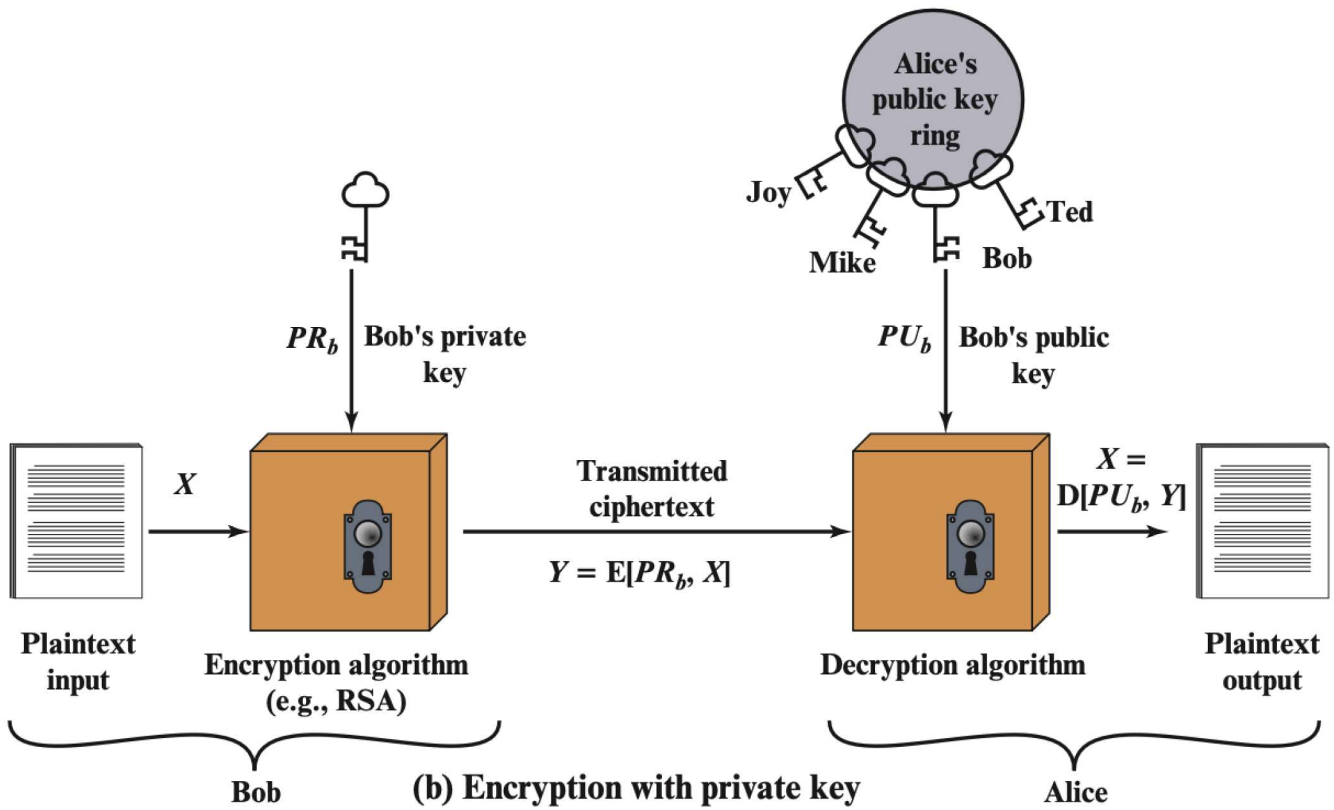


Figure 9.1 Public-Key Cryptography

comparison

Domain	Symmetric	Asymmetric
Able to grant	Confidential	Confidential, Offering Integrity, Authentication, and Non-repudiation
Needed keys	A single shared key	A public Key and A private Key
Key Exchange	Complex	Simple
Scalability	Not scalable, keys increase exponentially	Scalable
Key Size	small	Big
Implementation Speed	Fast	Slow
Best for	Bulk Data	Small amount of data, key exchange, digital envelopes, digital signatures and digital certificate