Cryptography and Network Security — Behrouz Forouzan

Chapter 3

Traditional Symmetric-Key Ciphers

Chapter 3

Objectives

- To define the terms and the concepts of symmetric key ciphers
- To emphasize the two categories of traditional ciphers: substitution and transposition ciphers
- To describe the categories of cryptanalysis used to break the symmetric ciphers
- To introduce the concepts of the stream ciphers and block ciphers
- To discuss some very dominant ciphers used in the past, such as the Enigma machine

3-1 INTRODUCTION

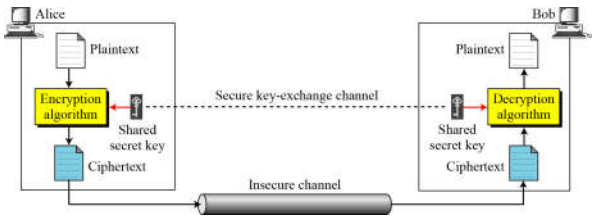
Figure 3.1 shows the general idea behind a symmetric-key cipher. The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key.

Topics discussed in this section:

3.1.1 Kerckhoff's Principle
3.1.2 Cryptanalysis
3.1.3 Categories of Traditional Ciphers

3.1 Continued

Figure 3.1 *General idea of symmetric-key cipher*



3.1 Continued

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

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

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

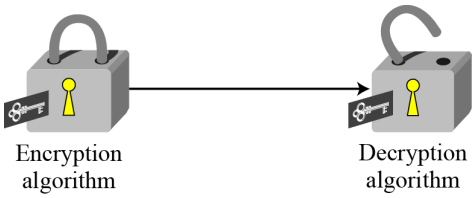
We assume that Bob creates P_1; *we prove that* $P_1 = P$:

Alice: $C = E_k(P)$

Bob: $P_1 = D_k(C) = D_k(E_k(P)) = P$

3.1 Continued

Figure 3.2 *Locking and unlocking with the same key*



3.1.1 Kerckhoff's Principle

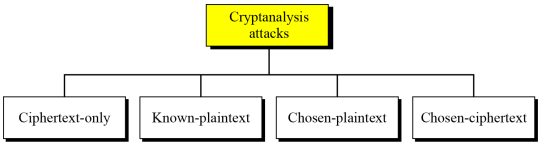
Based on Kerckhoff's principle, one should always assume that the adversary, Eve, knows the encryption/decryption algorithm. The resistance of the cipher to attack must be based only on the secrecy of the key.

3.7

3.1.2 Cryptanalysis

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

Figure 3.3 *Cryptanalysis attacks*

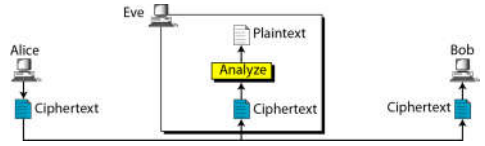


3.8

3.1.2 Continued

Ciphertext-Only Attack

Figure 3.4 *Ciphertext-only attack*

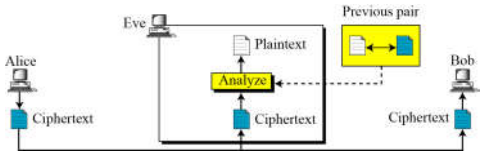


3.9

3.1.2 Continued

Known-Plaintext Attack

Figure 3.5 *Known-plaintext attack*

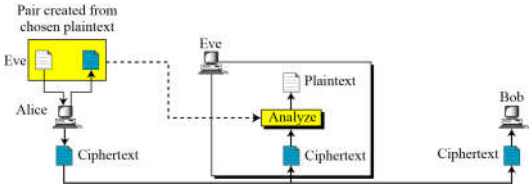


3.10

3.1.2 Continued

Chosen-Plaintext Attack

Figure 3.6 *Chosen-plaintext attack*

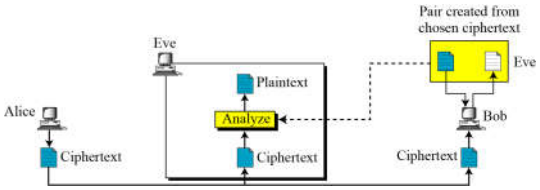


3.11

3.1.2 Continued

Chosen-Ciphertext Attack

Figure 3.7 *Chosen-ciphertext attack*



3.12

3-2 SUBSTITUTION CIPHERS

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

Note

A substitution cipher replaces one symbol with another.

Topics discussed in this section:

3.13

3.2.1 Monoalphabetic Ciphers

Note

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

3.14

3.2.1 Continued

Example 3.1

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

Example 3.2

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

Plaintext: hello **Ciphertext:** KHOOR

3.15

3.2.1 Continued

Additive Cipher

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.

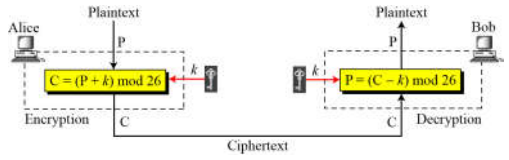
Figure 3.8 *Plaintext and ciphertext in Z_{26}*

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

3.16

3.2.1 Continued

Figure 3.9 *Additive cipher*



Note

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

3.17

3.2.1 Continued

Example 3.3

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

Solution

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

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

3.18

3.2.1 Continued

Example 3.4

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

Solution

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

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

3.19

3.2.1 Continued

Shift Cipher and Caesar Cipher

Historically, additive ciphers are called shift ciphers. Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes referred to as the Caesar cipher. Caesar used a key of 3 for his communications.

Note

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

3.20

3.2.1 Continued

Example 3.5

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

3.21

3.2.1 Continued

Table 3.1 *Frequency of characters in English*

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

Table 3.2 *Frequency of diagrams and trigrams*

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

3.22

3.2.1 Continued

Example 3.6

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

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Solution

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

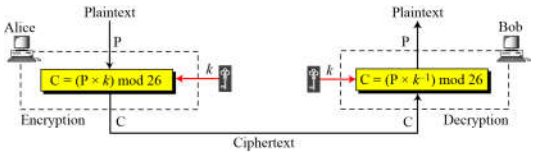
the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

3.23

3.2.1 Continued

Multiplicative Ciphers

Figure 3.10 *Multiplicative cipher*



Note

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

3.24

3.2.1 Continued

Example 3.7

What is the key domain for any multiplicative cipher?

Solution

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

Example 3.8

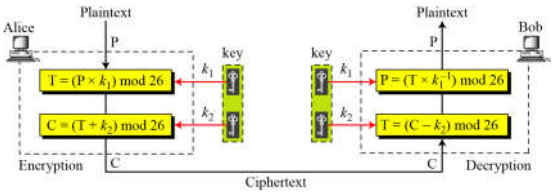
We use a multiplicative cipher to encrypt the message "hello" with a key of 7. The ciphertext is "XCZZU".

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

3.2.1 Continued

Affine Ciphers

Figure 3.11 *Affine cipher*



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

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

3.2.1 Continued

Example 3.09

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.

Example 3.10

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

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

3.2.1 Continued

Example 3.11

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

Solution

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

Example 3.12

The additive cipher is a special case of an affine cipher in which $k_1 = 1$. The multiplicative cipher is a special case of affine cipher in which $k_2 = 0$.