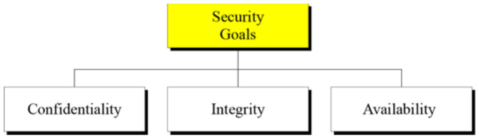
Introduction

1-1 THREE SECURITY GOALS

Figure 1.1 *Taxonomy of security goals*



1.1 Continued

***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.*

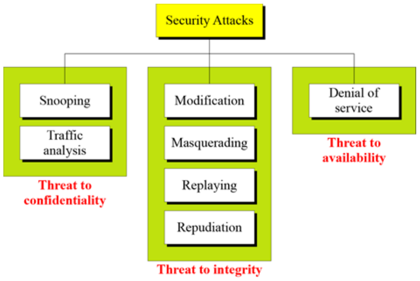
*Information needs to be changed constantly. **Integrity** means that changes need to be done only by authorized entities and through authorized mechanisms.*

*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.*

1-2 ATTACKS

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

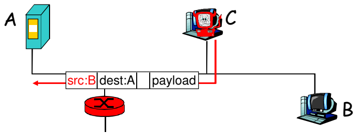
Figure 1.2 *Taxonomy of attacks with relation to security goals*



1.2.1 Attacks Threatening Confidentiality

***Snooping** refers to unauthorized access to or interception of data.*

e.g. IP spoofing: send packet with false source address

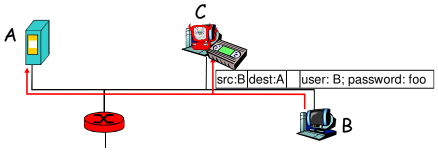


***Traffic analysis** refers to obtaining some other type of information by monitoring online traffic.*

1.2.2 Attacks Threatening Integrity

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

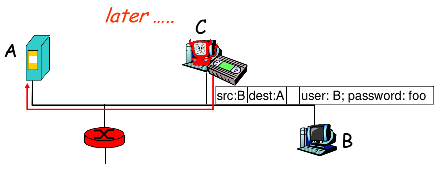
***Replaying** means the attacker obtains a copy of a message sent by a user and later tries to replay it.*



1.2.2 Attacks Threatening Integrity

***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.*



1.2.2 Attacks Threatening Integrity

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

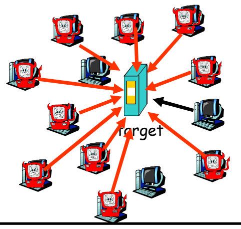
***Repudiation** means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.*

1.2.3 Attacks Threatening Availability

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

- *attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic*

1. *select target*
2. *break into hosts around the network*
3. *send packets toward target from compromised hosts*



1.2.4 Passive Versus Active Attacks

Table 1.1 ***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

In a passive attack, the attacker's goal is just to obtain information. The attack does not modify data or harm the system, and the system continues with its normal operation.

An active attack may change the data or harm the system.

1-3 SERVICES AND MECHANISMS

The International Telecommunication Union-Telecommunication Standardization Section (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..

Topics discussed in this section:

1.3.1 Security Services
1.3.2 Security Mechanism
1.3.3 Relation between Services and Mechanisms

1.3.1 Security Services

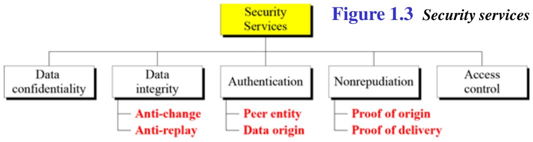


Figure 1.3 ***Security services***

Data confidentiality protects data from disclosure attack.

Data integrity protect data from modification, insertion, deletion, and replaying attacks.

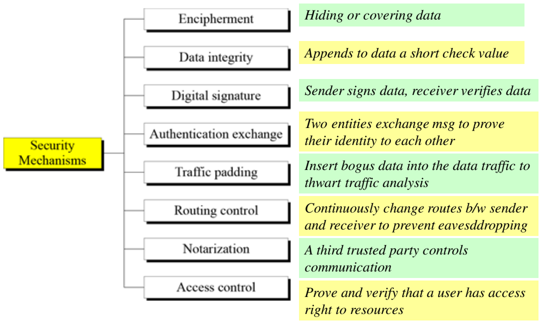
Authentication provides proof of sender, or receiver, or source of the data.

Nonrepudiation protects against repudiation by either the sender to the reveiver.

Access control provides protection again unauthorized access to data.

1.3.2 Security Mechanism

Figure 1.4 *Security mechanisms*


Security Mechanisms
Encipherment
Hiding or covering data
Data integrity
Appends to data a short check value
Digital signature
Sender signs data, receiver verifies data
Authentication exchange
Two entities exchange msg to prove their identity to each other
Traffic padding
Insert bogus data into the data traffic to thwart traffic analysis
Routing control
Continuously change routes b/w sender and receiver to prevent eavesddropping
Notarization
A third trusted party controls communication
Access control
Prove and verify that a user has access right to resources

1.3.3 Relation between Services and Mechanisms

Table 1.2 *Relation between security services and mechanisms*

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

1-4 TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.

Topics discussed in this section:

1.4.1 Cryptography
1.4.2 Steganography

1.4.1 Cryptography

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Cryptanalysis: the art and science of decrypting messages.

Cryptology: cryptography + cryptanalysis

1.4.2 Steganography

- Steganography is the art and science of hiding information into covert channels so as to conceal the information and prevent the detection of the hidden message.
- Today, steganography refers to hiding information in digital picture files and audio files.

1.4.2 Steganography

- Hide a message by using the least significant bits of frames on a CD
- Kodak photo CD format's maximum resolution is 2048 by 3072 pixels, with each pixel containing 24 bits of RGB color information.
- The least significant bit of each 240bit pixel can be changed without greatly affecting the quality of the image.
- Drawbacks:
  - Overhead
  - Worthless once discovered (encryption)

1.4.2 Steganography

- Steganography conceals the existence of the message
- Cryptography render the message unintelligible to outsides by various transformations of the text.
- Examples:
  - Hide a msg in an image: http://mozaiq.org/encrypt/
  - Wikipedia: http://en.wikipedia.org/wiki/Steganography
  - http://petitcolas.net/fabien/steganography/image_downgrading/index.html

The image in which we want to hide another image

The image we wish to hide: 'F15'

The stego-image (i.e., after the hiding process)

The image extracted from the stego-image

1.4.2 Steganography

- Steganography is defined as "hiding information within a noise; a way to supplement (not replace) encryption, to prevent the existence of encrypted data from being detected".
- Steganography and Cryptography are cousins in the data hiding techniques.
- Cryptography is the practice of scrambling a message to an obscured form to prevent others from understanding it.
- Steganography is the study of obscuring the message so that it cannot be seen.
- More tools: http://www.dmoz.org/Computers/Security/Products_and_Tools/Cryptography/Steganography//

Crypto and Info Sec Related Movies

"Windtalkers" (2002) - about the secret code used by American military during world war II which baffled the Japanese.

"Breaking the Code“ (1996) - about British mathematician, Alan Turing, "Father of computer science", who worked on breaking German military code during World War II. http://www.turing.org.uk/turing/

"A Beautiful Mind" (2001) - Oscar-winning movie about US mathematician and Nobel laureate John Nash. Nash worked for the US military on secret codes.

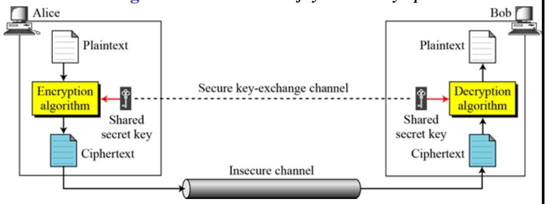
Others: **"U-571" (2000)**, **“Swordfish” (2001)**, **"Enigma" (2001)**, **“Hackers” (1995)**

Check www.imdb.com for details.

Traditional Symmetric-Key Ciphers

3-1 INTRODUCTION

Figure 3.1 ***General idea of 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.

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

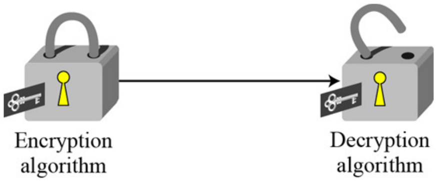
We assume that Bob creates P_1*; we prove that* $P_1 = P$*:*

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***



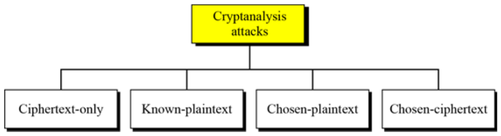
3.1.1 Kerckhoff's Principle

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.

3.1.2 Cryptanalysis

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

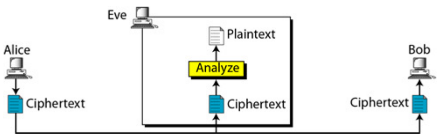
Figure 3.3 ***Cryptanalysis attacks***



3.1.2 Continued

Ciphertext-Only Attack

Figure 3.4 ***Ciphertext-only attack***



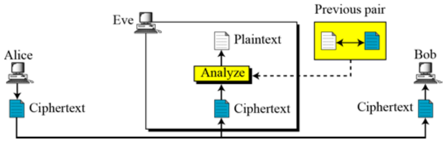
Ciphertext + algorithm → key and the plaintext

- Brute-Force attack: exhaustive key search attack
- Statistical attack: benefit from inherent characteristics of the plaintext language. E.g. E is the most frequently used letter.
- Pattern attack: discover pattern in ciphertext.

3.1.2 Continued

Known-Plaintext Attack

Figure 3.5 ***Known-plaintext attack***



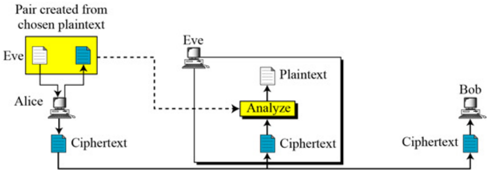
Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext.

Eve uses the relationship b/w the previous pair to analyze the current ciphertext.

3.1.2 Continued

Chosen-Plaintext Attack

Figure 3.6 ***Chosen-plaintext attack***

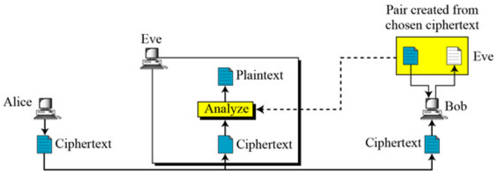


The plaintext/ciphertext pairs have been chosen by the attacker herself.

3.1.2 Continued

Chosen-Ciphertext Attack

Figure 3.7 ***Chosen-ciphertext attack***



Eve chooses some ciphertext and decrypts to form a ciphertext/plaintext pair. This can happen if Eve has access to Bob's computer.

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:

3.2.1 Monoalphabetic Ciphres
3.2.2 Polyalphabetic Ciphers

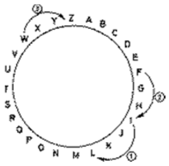
3.2.1 Monoalphabetic Ciphers

Note

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

Monoalphabetic Ciphers, Shift Cipher, Addictive Cipher

- replace letters of a message by other distinct letters a fixed distance away
- Famous shift cipher: **Caesar Cipher**
  - Shift by **3** letters
  - reputedly used by Julius Caesar (100 – 44 B.C.)
- Plaintext: **I CAME I SAW I CONQUERED**
  Ciphertext: **L FDPH L VDZ L FRQTXHUHG**



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.

A shift cipher can also be described as

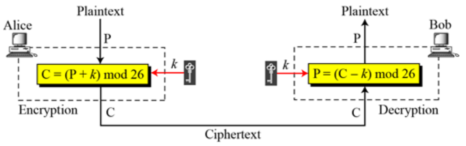
Encryption EK(x) = x + K mod 26
Decryption DK(x) = x - K mod 26

for English alphabet by setting up a correspondence between alphabetic characters and residues modulo 26.

K=3 in **Caesar Cipher**.

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}.

3.2.1 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

Encryption EK(x) = x + K mod 26

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

Decryption DK(x) = x - K mod 26

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.

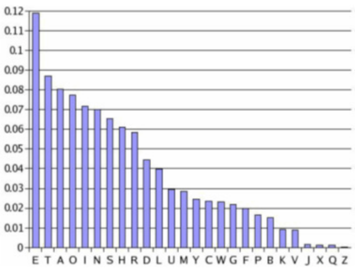
Solution

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

Frequency of characters in English



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

3.2.1 Continued

Example 3.6

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

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Solution

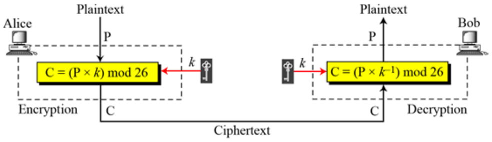
When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4 because the distance b/w e and I is 4 (e.f.g.h.i).

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

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}*.

3.2.1 Continued

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.

Figure 3.12 *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

3.2.1 Continued

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

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

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

3.2.2 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.

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

3.2.2 Continued

Example 3.14

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**

3.2.2 Continued

Playfair Cipher

Figure 3.13 *An example of a secret key in the Playfair cipher*

Secret Key =

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

Example 3.15

Let us encrypt the plaintext "hello" using the key in Figure 3.13.

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

3.2.2 Continued

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 3.16

We can encrypt the message "She is listening" using the 6-character keyword "PASCAL" (15, 0, 18, 2, 0, 11).

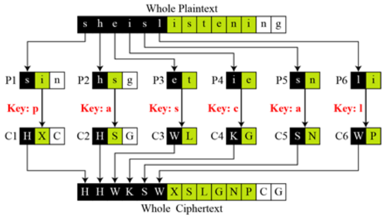
Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**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

3.2.2 Continued

Example 3.17

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

Figure 3.14 *A Vigenere cipher as a combination of m additive ciphers*



3.2.2 Continued

Vigenere Cipher (Crypanalysis)

Example 3.19

Let us assume we have intercepted the following ciphertext:

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-
VTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFZMVVWLGYHCUSWXQH-
KVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVWVWJWIXGFWLTSHGJOUEEHH-
VUCFVGOWICQLTJSUXGLW

The Kasiski test for repetition of three-character segments yields the results shown in Table 3.4.

String	*First Index*	*Second Index*	*Difference*
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60
MPH	119	127	8

3.2.2 Continued

Example 3.19 (Continued)

The greatest common divisor of differences is 4, which means that the key length is multiple of 4. First try $m = 4$.

```
C1: LWGWCRAOKTEPGTQCTJVUEGVGUQGECVPRPVJGTJEUGCJG
P1: jueuapymircneroarhtsthihytrahcieixsthcarrehe
C2: IGGGQHGWGKVCTSOSQSWVWFVYSHSVFSHZHWWFSOHCOQSL
P2: ussctsiswhofeaeceihcetesoecatnpntherhctecex
C3: OFDHURWQZKLZHGVVLUVLSZWHWKHFDUKDHVIWHUHFWLUW
P3: lcaerotnwhiwedssirsiirhketehretltiideatrairt
C4: MEVHCWILEMWVVXGETMEXLMLCXVELGMIMBWXLGEVVITX
P4: iardysehaisrrtcapiafpwtethecarhaesfterectpt
```

In this case, the plaintext makes sense.

Julius Caesar used a cryptosystem in his wars, which is now referred to as Caesar cipher. It is an additive cipher with the key set to three. Each character in the plaintext is shifted three characters to create ciphertext.

3.2.2 Continued

Hill Cipher

Figure 3.15 *Key in the Hill cipher*

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

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

Note

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

3.2.2 Continued

Example 3.20

For example, 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".

Figure 3.16 *Example 3.20*

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

a. Encryption

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

b. Decryption

3.2.2 Continued

Example 3.21

Assume that Eve knows that *m* = 3. She has intercepted three plaintext/ciphertext pair blocks (not necessarily from the same message) as shown in Figure 3.17.

Figure 3.17 *Example 3.21*

$$\begin{bmatrix} 05 & 07 & 10 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 03 & 06 & 00 \end{bmatrix}$$

$$\begin{bmatrix} 13 & 17 & 07 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 14 & 16 & 09 \end{bmatrix}$$

$$\underset{P}{\begin{bmatrix} 00 & 05 & 04 \end{bmatrix}} \longleftrightarrow \underset{C}{\begin{bmatrix} 03 & 17 & 11 \end{bmatrix}}$$

3.2.2 Continued

Example 3.21 (Continued)

She makes matrices P and C from these pairs. Because P is invertible, she inverts the P matrix and multiplies it by C to get the K matrix as shown in Figure 3.18.

Figure 3.18 *Example 3.21*

$$\underset{K}{\begin{bmatrix} 02 & 03 & 07 \\ 05 & 07 & 09 \\ 01 & 02 & 11 \end{bmatrix}} = \underset{P^{-1}}{\begin{bmatrix} 21 & 14 & 01 \\ 00 & 08 & 25 \\ 13 & 03 & 08 \end{bmatrix}} \underset{C}{\begin{bmatrix} 03 & 06 & 00 \\ 14 & 16 & 09 \\ 03 & 17 & 11 \end{bmatrix}}$$

Now she has the key and can break any ciphertext encrypted with that key.

3.2.2 Continued

One-Time Pad

- One of the goals of cryptography is perfect secrecy.
- A study by Shannon has shown that perfect secrecy can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain.
- This idea is used in a cipher called one-time pad, invented by Vernam.
- Provably unbreakable.

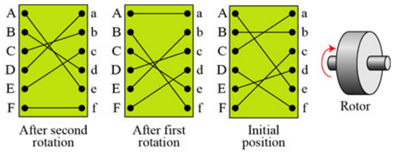
3.2.2 Continued

- **Warning**: keys ***must*** be random, or you can attack the cipher by trying to regenerate the key.
- Approximations, such as using computer pseudorandom number generators to generate keys, are *not* random.

3.2.2 Continued

Rotor Cipher

Figure 3.19 *A rotor cipher*



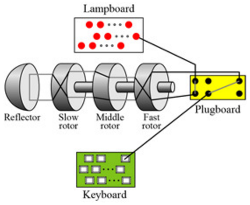
Enigma Machine

- The Enigma was a commercial crypto device adopted by various military and governmental services including Nazi Germany during World War II
- Computer science pioneer Alan Turing helped decrypting the Enigma
- Reuse of keys helped
- It is conjectured that two years of war were prevented by decrypting the Enigma

3.2.2 Continued

Enigma Machine

Figure 3.20 ***A schematic of the Enigma machine***



3-3 TRANSPOSITION CIPHERS

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

Note

A transposition cipher reorders symbols.

Topics discussed in this section:

3.3.1 Keyless Transposition Ciphers
3.3.2 Keyed Transposition Ciphers
3.3.3 Combining Two Approaches

3.3.1 Keyless Transposition Ciphers

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

Example 3.22

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

She then creates the ciphertext “MEMATEAKETETHPR”.

3.3.1 Continued

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	

She then creates the ciphertext “MMTAEEHREAEKTTP”.

3.3.1 Continued

Example 3.24

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.

3.3.2 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.

3.3.2 Continued

Example 3.25

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

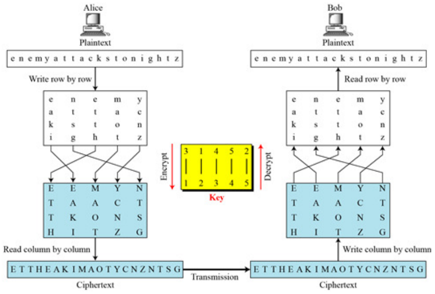
The permutation yields

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

3.3.3 Combining Two Approaches

Example 3.26

Figure 3.21

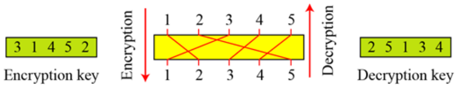


3.3.3 Continued

Keys

In Example 3.27, 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.

Figure 3.22 *Encryption/decryption keys in transpositional ciphers*



3.3.3 Continued

Using Matrices

Example 3.27

We can use matrices to show the encryption/decryption process for a transposition cipher. Figure 3.24 shows the encryption process. Multiplying the 4 × 5 plaintext matrix by the 5 × 5 encryption key gives the 4 × 5 ciphertext matrix.

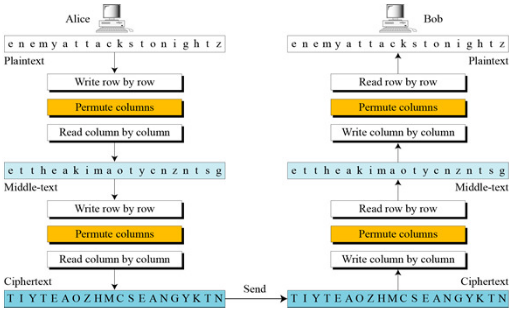
Figure 3.24 *Representation of the key as a matrix in the transposition cipher*

$$\underset{\text{Plaintext}}{\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 00 & 19 & 19 & 00 & 02 \\ 10 & 18 & 19 & 14 & 13 \\ 08 & 06 & 07 & 19 & 25 \end{bmatrix}} \times \overset{\begin{array}{ccccc} \boxed{3} & \boxed{1} & \boxed{4} & \boxed{5} & \boxed{2} \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{array}}{\underset{\text{Encryption key}}{\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}}} = \underset{\text{Ciphertext}}{\begin{bmatrix} 04 & 04 & 12 & 24 & 13 \\ 19 & 00 & 00 & 02 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 07 & 08 & 19 & 25 & 06 \end{bmatrix}}$$

3.3.3 Continued

Double Transposition Ciphers

Figure 3.25 *Double transposition cipher*



3-4 STREAM AND BLOCK CIPHERS

The literature divides the 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.

Topics discussed in this section:

3.4.1 Stream Ciphers
3.4.2 Block Ciphers
3.4.3 Combination

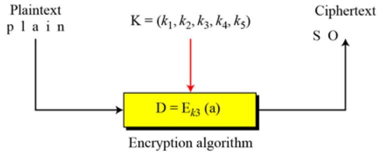
3.4.1 Stream Ciphers

Call the plaintext stream P, the ciphertext stream C, and the key stream K.

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

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

Figure 3.26 *Stream cipher*



3.4.1 Continued

Example 3.30

Additive ciphers can be categorized as stream ciphers in which the key stream is the repeated value of the key. In other words, the key stream is considered as a predetermined stream of keys or K = (k, k, …, k). In this cipher, however, each character in the ciphertext depends only on the corresponding character in the plaintext, because the key stream is generated independently.

Example 3.31

The monoalphabetic substitution ciphers discussed in this chapter are also stream ciphers. However, 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.

3.4.1 Continued

Example 3.32

Vigenere ciphers are also stream ciphers according to the definition. In this case, the key stream is a repetition of m values, where *m* is the size of the keyword. In other words,

$$K = (k_1, k_2, \ldots k_m, k_1, k_2, \ldots k_m, \ldots)$$

Example 3.33

We can establish a criterion to divide stream ciphers based on their key streams. We can say that a stream cipher is a monoalphabetic cipher if the value of k_i does not depend on the position of the plaintext character in the plaintext stream; otherwise, the cipher is polyalphabetic.

3.4.1 Continued

Example 3.33 (Continued)

- ❑ **Additive ciphers are definitely monoalphabetic because k_i in the key stream is fixed; it does not depend on the position of the character in the plaintext.**

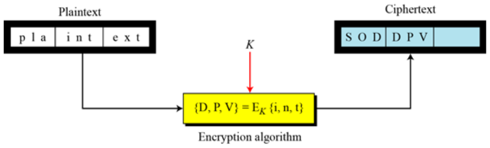
- ❑ **Monoalphabetic substitution ciphers are monoalphabetic because k_i does not depend on the position of the corresponding character in the plaintext stream; it depends only on the value of the plaintext character.**

- ❑ **Vigenere ciphers are polyalphabetic ciphers because k_i definitely depends on the position of the plaintext character. However, the dependency is cyclic. The key is the same for two characters *m* positions apart.**

3.4.2 Stream 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. A single key is used to encrypt the whole block even if the key is made of multiple values. Figure 3.27 shows the concept of a block cipher.

Figure 3.27 *Block cipher*



3.4.2 Continued

Example 3.34

Playfair ciphers are block ciphers. The size of the block is *m* = 2. Two characters are encrypted together.

Example 3.35

Hill ciphers are block ciphers. A block of plaintext, of size 2 or more is encrypted together using a single key (a matrix). In these ciphers, the value of each character in the ciphertext depends on all the values of the characters in the plaintext. Although the key is made of *m* × *m* values, it is considered as a single key.

Example 3.36

From the definition of the block cipher, it is clear that every block cipher is a polyalphabetic cipher because each character in a ciphertext block depends on all characters in the plaintext block.

3.4.3 Combination

In practice, blocks of plaintext are encrypted individually, but they use a stream of keys to encrypt the whole message block by block. In other words, the cipher is a block cipher when looking at the individual blocks, but it is a stream cipher when looking at the whole message considering each block as a single unit.