Cryptography

Cunsheng DING, HKUST

COMP5631

Lecture 01: Introduction to Cryptography

Outline of this Lecture

A brief introduction to:

- data confidentiality, and encryption-decryption systems;
- data integrity;
- sender authentication, receiver authentication;
- anti-replay, data origin authentication, signer nonrepudiation;
- secret sharing;
- cryptographic protocols;
- history of cryptography.

Data Confidentiality

Data in transmission or in storage could be very sensitive and only authorized people are allowed to read.

Data confidentiality means the **prevention** of unauthorized reading of a piece of data.

Remark: It is very hard to **detect** an unauthorized reading of a piece of data. We will not consider the **detection** of unauthorized reading of data in this course.

How Is Data Confidentiality Provided?

By ENCRYPTION, i.e., one uses a secret 1-to-1 function f to map a plaintext m to a ciphertext c, i.e., $c = f(m)$. This is to hide the information m from unauthorised reading.

To recover the plaintext m from the ciphertext c, one applies the inverse function f^{-1} to c, obtaining

$$f^{-1}(c) = f^{-1}(f(m)) = (f^{-1} \circ f)(m) = m.$$

This is called DECRYPTION.

Remark: Such an encryption-decryption system is called a **cipher**. It can be used by a single person who should keep f confidential. It can also be used by a group of people who share f but keep f confidential.

First Example of Encryption

Consider the English alphabet arranged in the order

$$a, b, c, d, \cdots, w, x, y, z$$

Define the 1-to-1 function f by

$$f(\text{letter}) = \text{ the third letter after the letter,}$$

where the 3rd letter after x, y, z is resp. a, b, c.

Then the plaintext "kill" is encrypted into

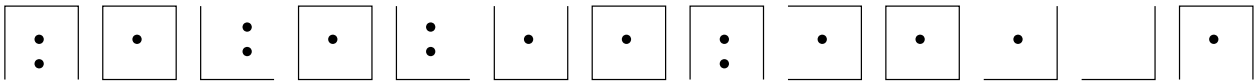
$$f(kill) = f(k)f(i)f(l)f(l) = nloo.$$

Question: What is f^{-1}? How to decrypt?

Remark: Used by Julius Caesar (the Roman Emperor)

Second Example of Encryption

Churchyard Cipher: It was engraved on a tombstone in St. Paul's Churchyard, New York, in 1796.



a ·	b ·	c ·
d ·	e ·	f ·
g ·	h ·	i ·

k :	l :	m :
n :	o :	p :
q :	r :	s :

t	u	v
w	x	y
z	j	

Question: What is the original plaintext?

Remark: It is hard to recover the plaintext without the secret function f (the three tables above).

Data Integrity

For data in transmission or in storage the following could happen:

- It could be modified by an unauthorized person.
- It could be replaced with another data by an unauthorized person.

Question: How do we **detect** an unauthorised modification or replacement of data?

Answer: Protocols for such detection will be introduced later.

Data integrity: it means **only** the **detection** of an unauthorised modification or replacement of a piece of data in this course.

Remark: The **prevention** of an unauthorised modification or replacement of data in storage is possible by "access control techniques", but there is no guarantee for such prevention. The **prevention** of an unauthorised modification or replacement of data in transmission is difficult.

Anti-replay

Replay attack: An attacker intercepted a message from Alice to Bob earlier and sends it to Bob later (assuming that the attacker has control of the communication channel).

Anti-replay: The **detection** of a replayed message.

Question: How do we detect a replayed message?

Answer: Techniques will be covered later.

Warning: Our anti-replay means the detection of a replayed message, not the prevention of replaying a message.

Comment: It is very hard to prevent someone from replaying an earlier message, as we use public communication channels.

Authenticity of Sender and Receiver

Question: If you have received a message with alleged sender X, how could you be sure that the sender is indeed X?

Sender authentication: it means the verification of the identity of the sender of a message.

Question: If you have sent a message to a receiver Y, how could you be sure that the receiver indeed received the message?

Receiver authentication: it means the verification that an intended receiver of an earlier message has indeed received the message.

Remark: Detailed techniques for sender authentication and receiver authentication will be introduced later.

Data Origin Authentication

Definition: The verification of the creator (i.e., source) of a piece of data or message.

Remark: Detailed techniques for data origin authentication will be introduced later.

Remark: The sender of a message may or may not be the creator of the message. Hence, sender authentication and data origin authentication are different.

Example: Eva intercepted a message from Alice to Bob yesterday and replays it to Bob now. In this case, Alice is the creator of the current message, but Eva is the sender of the current message.

Signer Nonrepudiation

Hand written signature: If I wrote you a hard-copy letter, saying that I will pay you US$100,000 if you finish that job for me, I could not repudiate my promise later because I must have signed on this letter. In this case, the handwritten signature is used for nonrepudation.

Question: If I sent you an electronic message that orders you to kill someone, but later denying that I sent you this message, how could you prove that I indeed sent you this message?

Solution: Digital signature (introduced later).

Signer nonrepudiation: The **detection** of the repudiation of the signature of a signer on a document.

Secret Sharing

Problem: A father has put a lot of treasure into a secure room with an electronic key k. He has three sons, and would have his three sons to share the electronic key in some way so that the following conditions are satisfied:

(1) Each of his sons has a share (could be a number), which gives zero information about k.

(2) When any two of his sons come together with their shares, they get no information at all about the electronic key.

(3) Only when all the three sons come together with their shares, they are able to recover k with their shares.

How could the father design a system for sharing the electronic key?

Cryptographic Protocols

Problem: A group of banks would have an electronic funds transfer system that can provide the following security services:

"Data confidentiality, data integrity, sender authentication, and singer nonrepudiation"

Suppose that you have an algorithm for providing each of the services above. How do you combine these algorithms so that they work as a whole?

Solution: Cryptographic protocols.

Main Topics of Cryptography

- *Data confidentiality*, and the design and analysis of encryption and decryption algorithms for providing this service.
- *Sender authentication and data integrity* and protocols for providing these services.
- *Anti-replay, data origin authentication*, and protocols for providing these services.
- *Signer nonrepudiation* and protocols for providing this service.
- *Secret sharing* and protocols for providing this service.
- Cryptographic protocols.

History of Cryptography

- Cryptography has a history of five thousand years, starting with human writings.
- At the early stage, they are called **codes**. Encryption and decryption were done by hands.
- Cipher devices were invented in about 1817.
- Cryptography has played an important role during World War I and II. Sixty Japanese navy ciphers were broken during World War II.
- Modern cryptography started with Shannon's paper

  "Communication Theory of Secrecy Systems, Bell System Technical Journal 28 (1949) 656–715."

References on the History

The history of cryptography is too rich to be covered here. The following references are recommended:

1. David Kahn, The Codebreakers: The Story of Secret Writing, Scribner, revised edition, 1996 (First Edition 1967).
2. Cipher Devours, David Kahn, Louis Kruh, Greg Mellen, Brian Winkel, Cryptology: Machines, history and Methods, Artech House, 1989.
3. Fred B. Wrixon, Codes and Ciphers, Prentice Hall, 1992.

Who Are Using Cryptography?

1. Diplomatic personnel, military personnel, police organizations, government officials.
2. Banks.
3. Business companies for communications between their divisions and for keeping their documents confidential.
4. Gangsters, Mafia and other criminal organizations.
5. Ordinary people (email, mobile phones, faxes, computers, online shopping and banking).

In view that most people are using a mobile phone, most people are using cryptography daily!

Who Works on Cryptography?

1. Mathematicians.
2. Computer scientists.
3. Electrical engineers.

These people are working for two sectors:

- the secret sector (military and government organizations),
- the public sector (research institutions and universities).