# Cryptography and Security

**Cunsheng DING**

**HKUST, Hong Kong**

**Version 3**

# Lecture 01: Introduction to Cryptography

## Outline of This Lecture

A brief introduction to:

- data confidentiality, encryption/decryption;
- 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 stored in a storage system could be very sensitive and only authorized people are allowed to read.

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

# How to Achieve Data Confidentiality

By ENCRYPTION, i.e., use a secret 1-to-1 mapping (function) $f$ to map a plaintext $m$ into a ciphertext $c$, i.e., $c = f(m)$.

To recover the plaintext $m$ from the ciphertext $c$, apply the inverse mapping $f^{-1}$ to $c$, yielding

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

This is called DECRYPTION.

# 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 mapping $f$ by

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

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

Then the plaintext "kill" is encrypted into

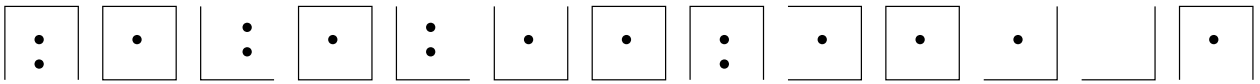
$$f(kill) = f(k)f(i)f(l)f(l) = nloo.$$

**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:** Very hard to break without the secret key.

# Data Integrity

**Data integrity:** For data in transmission or stored in a storage system the following could happen:

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

**Remark:** The **prevention** of an unauthorised modification or replacement of a piece of data is possible by access control techniques. But there is no guarantee for it.

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

**Answer:** Protocols for "providing this service" will be introduced later.

**Attention: Providing the data integrity service** means the detection of an unauthorised modification or replacement of a piece of data.

# Authenticity of Sender and Receiver

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

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

**Remark:** Detailed techniques for authentication of a message's sender will be introduced later.

# 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.

# 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.

# Signer Nonrepudiation

**Remark:** If I wrote you a letter, saying that I will pay you US$100,000 if you finish that job for me, I could not deny this offer later because I must have signed on this letter.

**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 a 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 son 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 does the following:

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

Suppose that you have an algorithm for doing each of the jobs 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.
- *Data 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).

With the implementation of e-cash, almost everyone will have to use cryptography directly or indirectly!

# Who Works on Cryptography?

1. Computer Scientists.
2. Mathematicians.
3. Electrical Engineers.

The researchers are working for two sectors:

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