[Part 3] Integrity, Authenticity, and Key Management

Chapter 11

Message Integrity and Message Authentication

Chapter 11

Objectives

- To define message integrity.
- To define message authenticity.
- To define criteria for a cryptography hash function.
- To distinguish between an MDC and a MAC.
- To discuss some common MACs.

MDC: Modification Detection Code. || MAC : Massage Authentication Code. 1.2

Chapter 11 Contents

1.3

Chapter 11 Contents

1.4

Chapter 11

11.1 Introduction

- This chapter discusses general ideas related to cryptographic hash functions that are used to create a message digest from a message.
- Message digest guarantee the *integrity* of the message.
- We will discuss how simple message digests can be modified to authenticate the message.

- The standard cryptography cryptographic hash functions will be discussed in Chapter 12.

1.5

Chapter 11

Contents

1.6

Chapter 11

11.2 Message Integrity

Introduction

- The cryptography systems that discussed so far provide *secrecy* or *confidentiality*, but not *integrity*.
- However, there are occasions that may not even need confidentiality but instead must have integrity.
- Example:
  - Ahmad may write a will to distribute his estate upon his death.
  - The will does not need to be encrypted because anyone can examine the will after he died.
  - However, the integrity of the will needs to be preserved so that the contents of the will is unchanged.

1.7

Chapter 11

11.2 Message Integrity

Document and Fingerprint

- On way to preserve the integrity of a document is through the use of a *fingerprint*.
- If Alice needs to ensure the content of her document will not changed, she can put her fingerprint at the bottom of the document.
- Eve cannot modify the contents of the document or create a false document because she cannot she cannot forge Alice's fingerprint.

Q: How to ensure the document not been changed?

A: Compare Alice's fingerprint on the document with Alice's fingerprint on file.

1.8

Chapter 11

11.2 Message Integrity

Message and Message Digest

- The electronic equivalent of the document and fingerprint pair is the *massage* and *digest* pair.
- A message is passed through an algorithm called a *cryptographic hash function* to preserve the integrity.
- The function creates a compressed image of the message that can be used like a fingerprint.

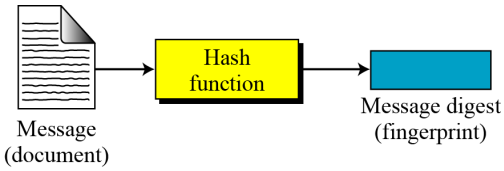

Figure 11.2: Message and digest

1.9

Chapter 11

11.2 Message Integrity

- The two pairs (document/fingerprint) and (message/ message digest) are similar, with some differences:
  - (document/fingerprint) are physically linked together.
  - (message/message digest) can be unlinked and send separately.
- The most important:
  - message digest needs to be safe from any change.

1.10

Chapter 11

11.2 Message Integrity

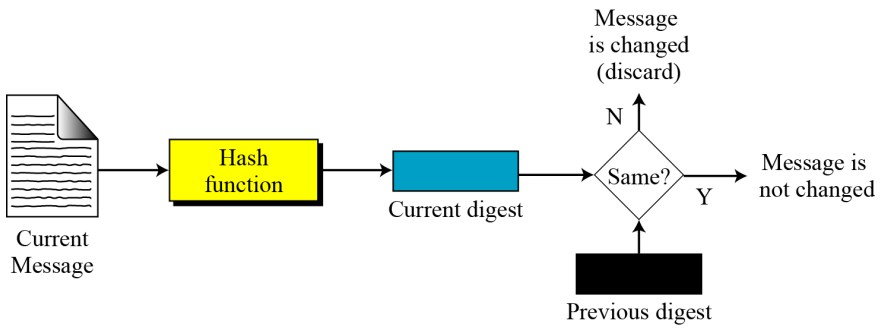

Figure 11.3: Checking integrity

1.11

Chapter 11

11.2 Message Integrity

Cryptographic Hash Function Criteria

- A cryptographic hash function must satisfy three criteria:

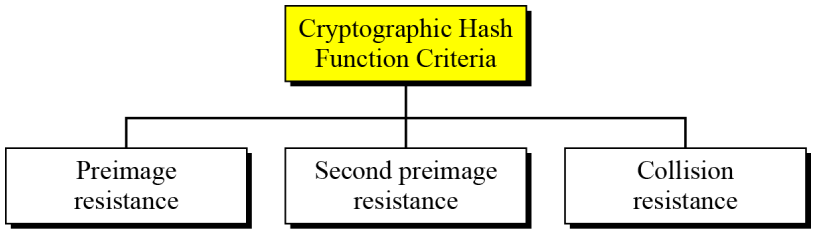

Figure 11.4: Criteria of a cryptographic hash function

1.12

Chapter 11 — 11.2 Message Integrity

(a) Preimage Resistance

- A cryptographic hash function must be preimage resistance.

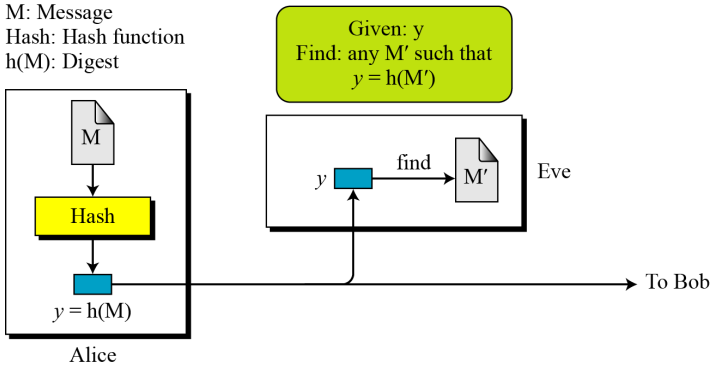

Figure 11.5: Preimage

1.13

Chapter 11 — 11.2 Message Integrity

(b) Second Preimage Resistance

- Ensure a message cannot easily be forged.

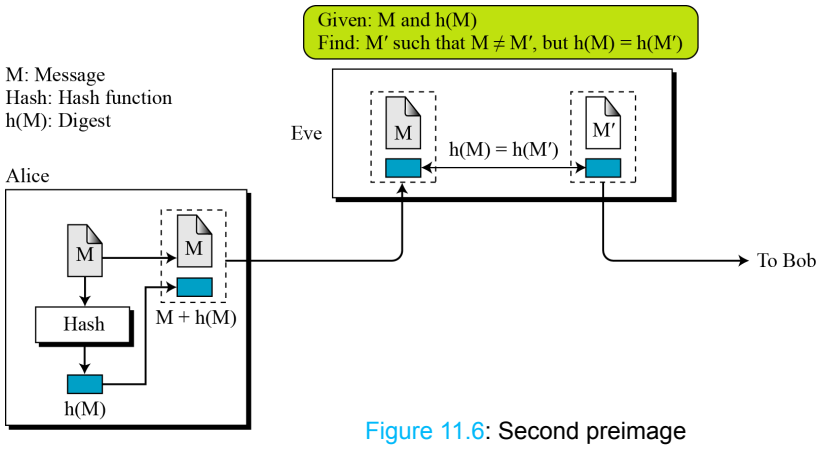

Figure 11.6: Second preimage

1.14

Chapter 11 — 11.2 Message Integrity

(c) Collision Resistance

- Ensure a message cannot easily be forged.

M: Message
Hash: Hash function
h(M): Digest

Find: M and M′ such that M ≠ M′, but h(M) = h(M′)

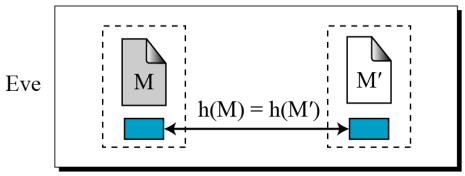

Figure 11.7: Collision preimage

1.15

Chapter 11 — Contents

1.16

Chapter 11

11.3 Message Authentication

Introduction

- The message digest guarantees the integrity of a message that not been changed.
- However, message digest does not authenticate the sender of the message.
- To provide message authentication, sender needs to provide proof that he/she sending the message and not an impostor.
- The digest created by a cryptographic hash function is called a *Modification Detection Code* (MDC).
  - detect any modification in the message.
- For message authentication, we need a *Message Authentication Code* (MAC).

1.17

Chapter 11

11.3 Message Authentication

Modification Detection Code (MDC)

- MDC is a message digest that can prove the integrity of the message that not been changed during transmission.

- Sender create a message digest MDC, and sends with the message to receiver.
- Receiver creates a new MDC from the message and **compare** the MDC received.
- If they are the same, the message has not been changed.
- Figure 11.8 illustrates the idea.

1.18

Chapter 11

11.3 Message Authentication

- The MDC needs to be transferred through a secure channel.

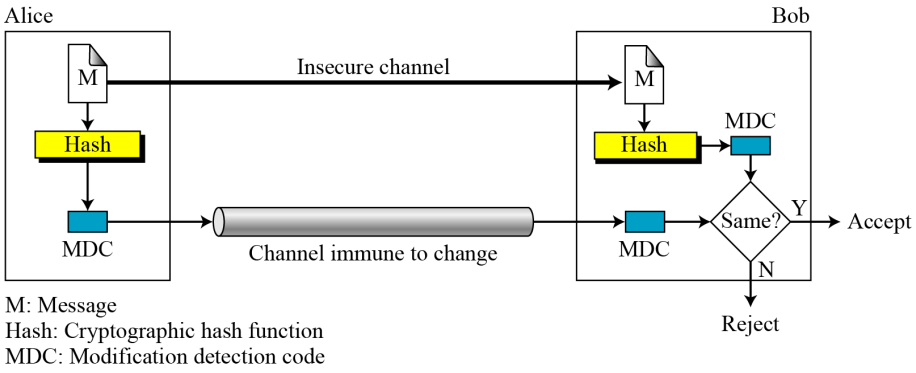

Figure 11.8: Modification Detection Code (MDC)

1.19

Chapter 11

11.3 Message Authentication

Message Authentication Code (MAC)

- To ensure the integrity of the message and the data origin authentication (message authentication), the MDC needs to be changed to a MAC.
- The different: the MAC included a **secret** between sender and receiver.

- Note that there is no need to use two channels in this case.
- Both message and MAC can be sent on the same insecure channel.
- Figure 11.9 illustrates the idea.

1.20

Chapter 11

11.3 Message Authentication

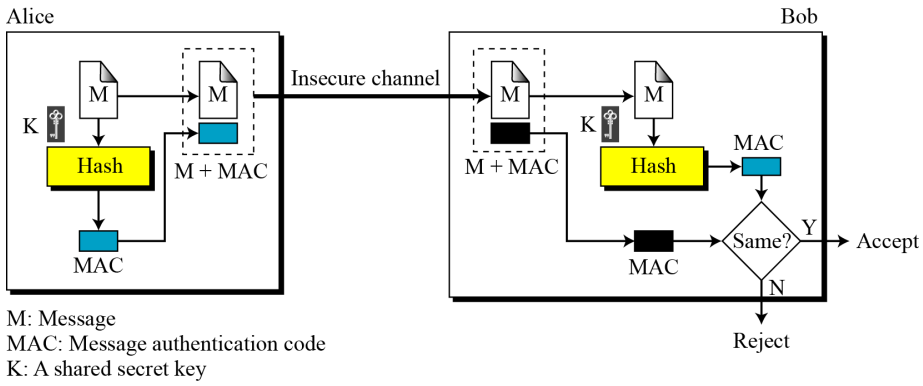

Figure 11.9: Message Authentication Code (MAC)

1.21

Chapter 9

Contents

1.22

Chapter 11

11.4 Summary

- A *fingerprint* or a *message digest* can be used to ensure the integrity of a document or a message:
  - ❑ To ensure the integrity of a document, both document and fingerprint are needed.
  - ❑ To ensure the integrity of a message, both message and message digest are needed.
- A *message digest* needs to be kept safe from change.

1.23

Chapter 11

11.4 Summary

- A cryptographic hash function creates a message digest out of a message that meets three criteria: *preimage resistance*, *second preimage resistance*, and *collision resistance*.
- A MDC is a message digest that can prove the integrity of the message that not been changed.
- To prove the integrity of a message and the data origin authentication (message authentication), we need to change MDC to MAC with a secret between sender and receiver.

1.24

Chapter 11

Exercises

Exercise 11.1:

a) Distinguish between *message integrity* and *message authentication*.

b) Define the criterions for a cryptographic hash function.

c) Distinguish between an MDC and a MAC.

Forouzan,B.A. Cryptography and Network Security (International Edition). Singapore: McGraw-Hill, 2008. (page 358)

1.25