

# Cryptography in OS

Chapter 9.5

Di Xiao

CS646

11/29/2021

# Learning outcomes:

## To understand the key concepts of

- Encryption process
- Hash functions
- Digital signature
- Trusted Platform Module (TPM)

# The web

- Document-based middleware

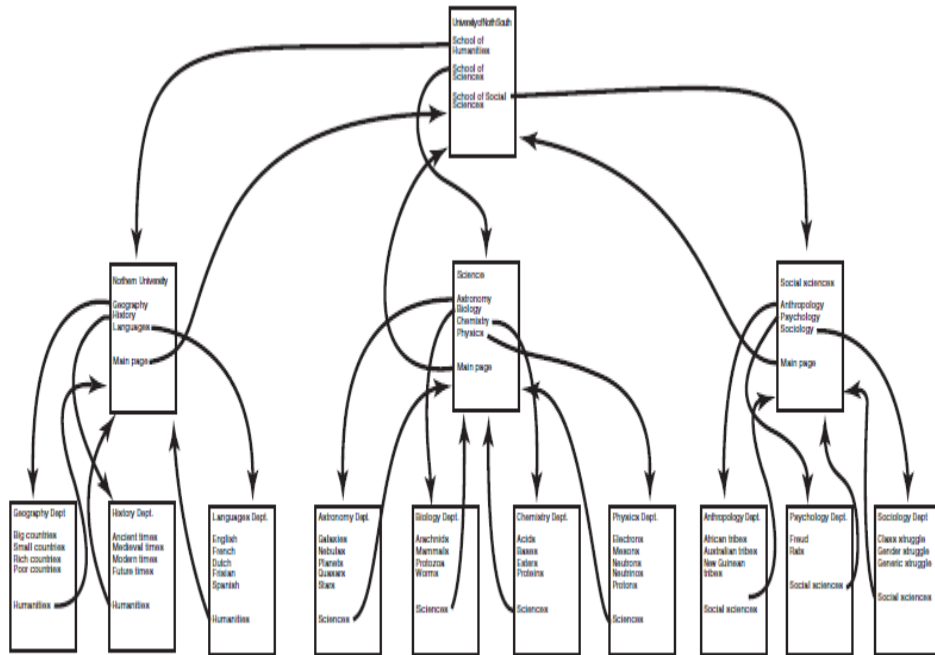
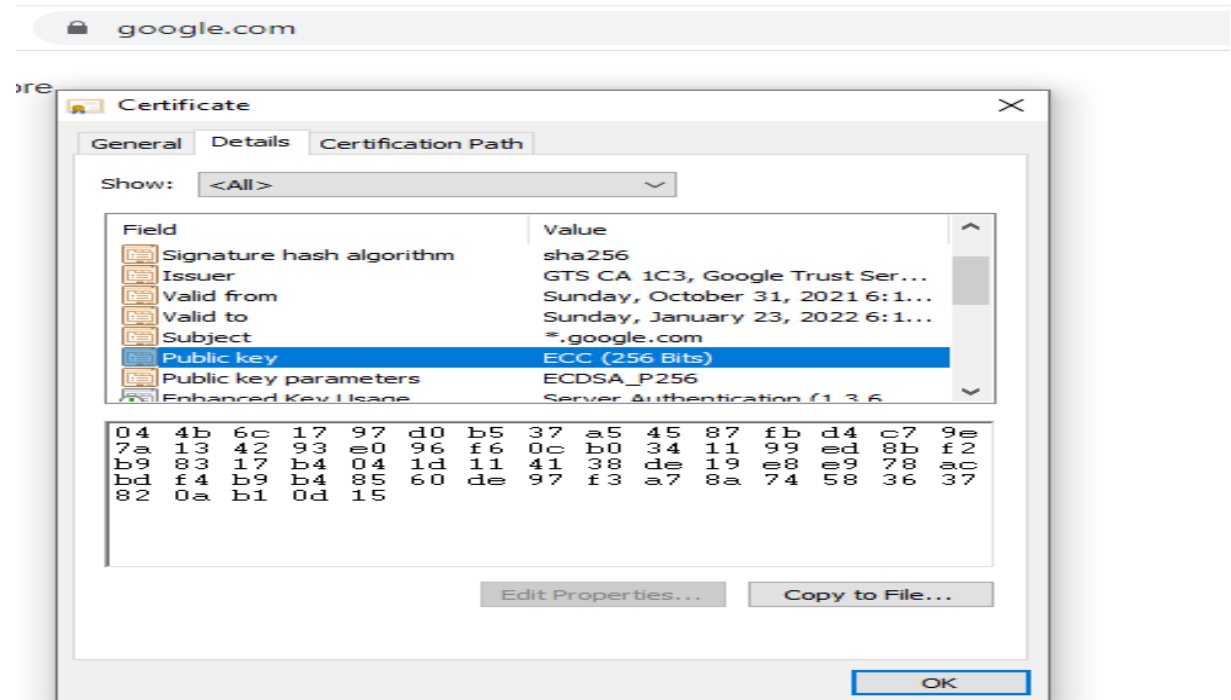


Figure 8-32. The Web is a big directed graph of documents.

- How security issues are addressed?
- 85% webpages are encrypted and decrypted at the server side.



Field	Value
Signature hash algorithm	sha256
Issuer	GTS CA 1C3, Google Trust Ser...
Valid from	Sunday, October 31, 2021 6:1...
Valid to	Sunday, January 23, 2022 6:1...
Subject	*.google.com
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Enhanced Key Usage	Server Authentication (1.3.6

04 4b 6c 17 97 d0 b5 37 a5 45 87 fb d4 c7 9e  
7a 13 42 93 e0 96 f6 0c b0 34 11 99 ed 8b f2  
b9 83 17 b4 04 1d 11 41 38 de 19 e8 e9 78 ac  
bd f4 b9 b4 85 60 de 97 f3 a7 8a 74 58 36 37  
82 0a b1 0d 15

# Encryption process

- Public-key encryption:  
Web browsers, email,...
- Algorithms: RSA, ECC,...
- Key pair: (E, D ), Plaintext: m
- $D(E(m))=m$
- RSA example:

$$(m^e)^d \equiv m \pmod{n}$$

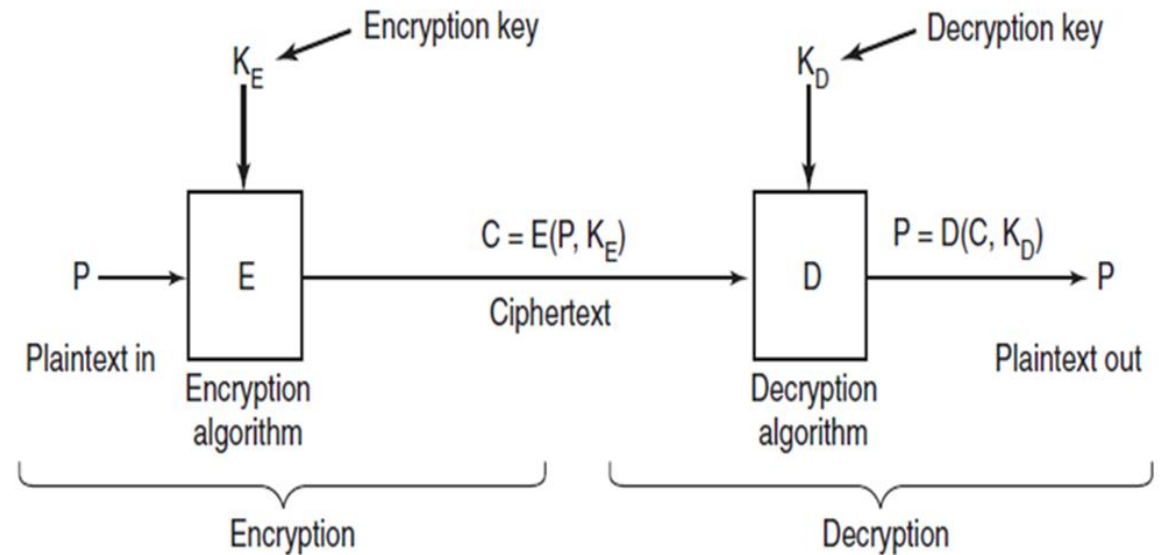


Figure 9-15. Relationship between the plaintext and the ciphertext.

# Hash functions

- Map data of any size to fixed-size values
- Only one output for each input
- One way functions:  $f(x) = y, f^{-1}(y) = ?$
- Many to one functions
- Fixed sized output
- Save time and space.
- Widely used Hash functions:
  - Sha256: 32bytes output
  - Sha512: 64bytes output
- Hash collisions

# Digital signature

- Tampering problem
- Verify the identity of senders
- Algorithms: RSA, ECC,...
- Key pair: (E, D), Hashed doc: m
- $E(D(m))=m$
- RSA example:

$$(m^d)^e \equiv m \pmod{n}$$

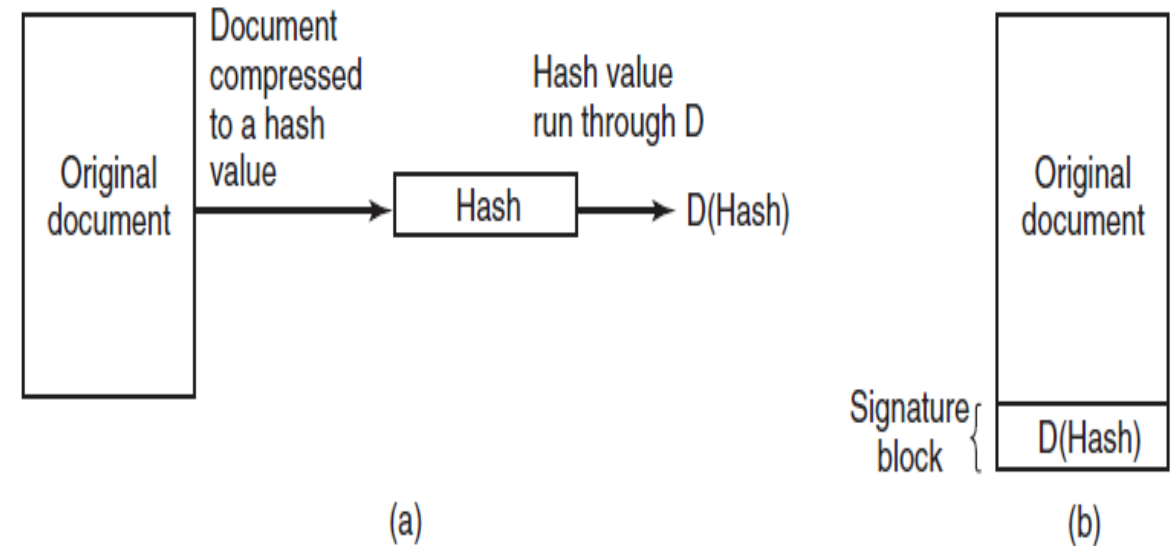


Figure 9-16. (a) Computing a signature block. (b) What the receiver gets.

# Trusted Platform Modules (TPM)

- For key storing: A crypto processor with nonvolatile storage
- Binding: Encrypting data
- Detecting unauthorized software
- Remote attestation
- Prevention of online-gaming cheating