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

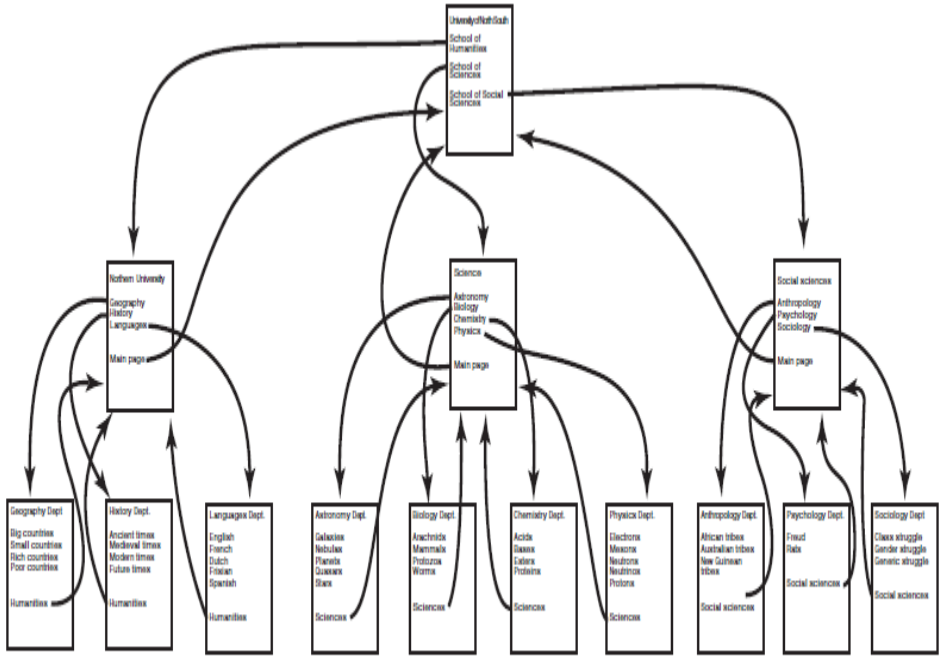
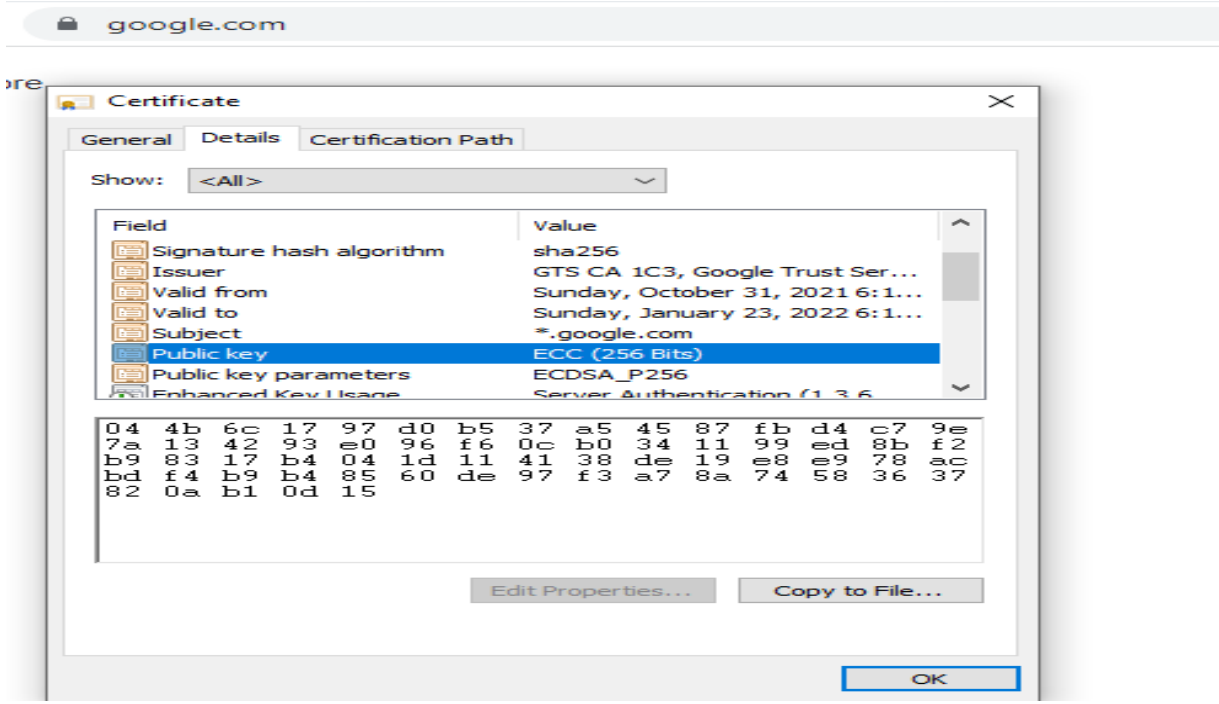


Figure 8-32. The Web is a big directed graph of documents.

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



Encryption process

- Public-key encryption:

  Web browsers, email,…
- Algorithms: RSA, ECC,…
- Key pair: (E, D), Plaintext: m
- D(E(m))=m
- RSA example:

$$(m^e)^d \equiv m(mod\ n)$$

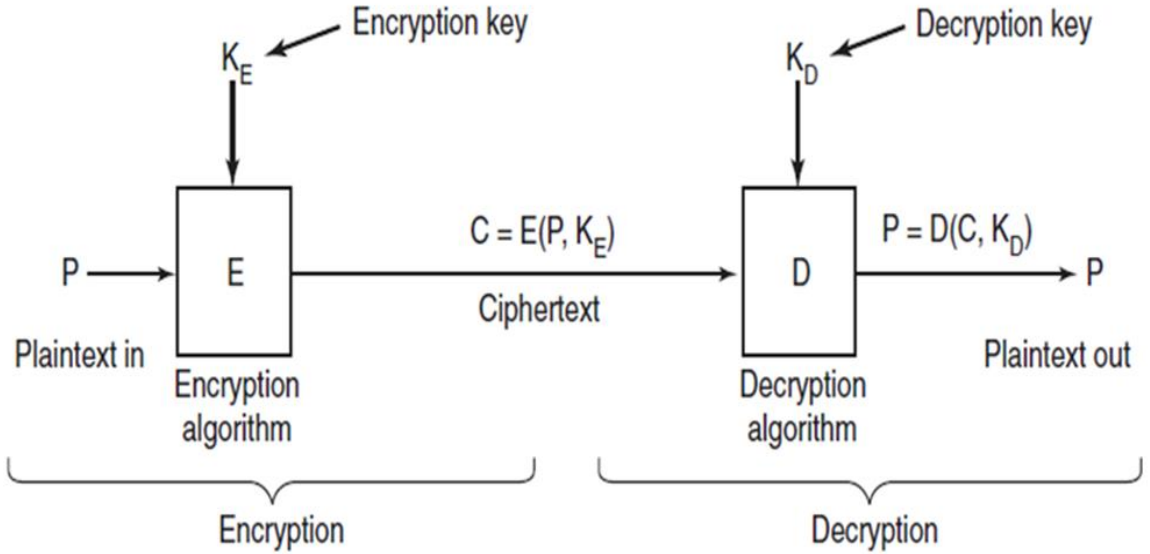


Figure 9-15. Relationship between the plaintext and the ciphertext.

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:

$$(m^d)^e \equiv m(mod\ n)$$

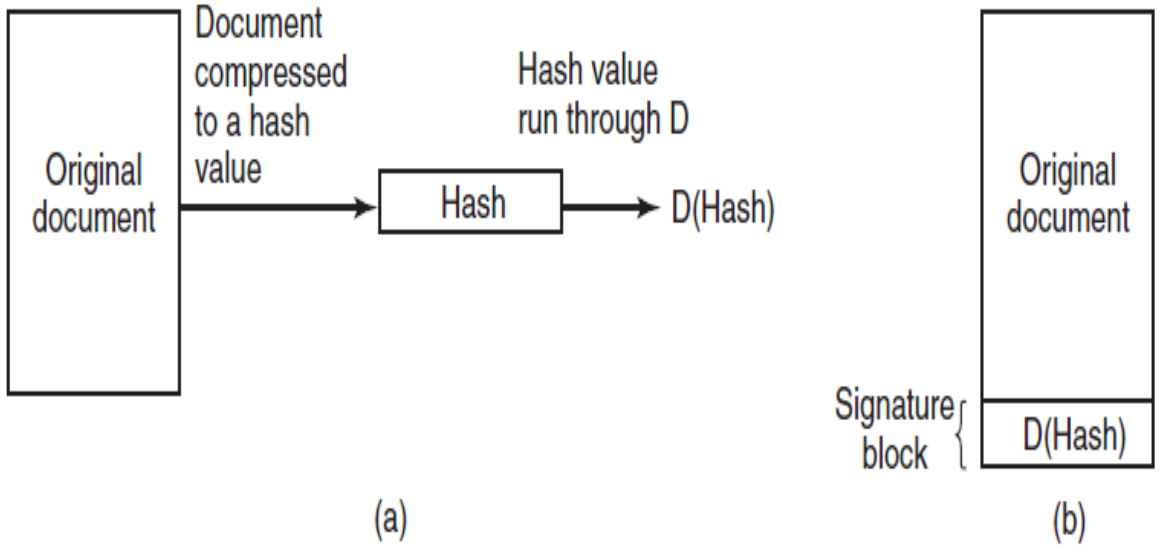


Figure 9-16. (a) Computing a signature block. (b) What the receiver gets.

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