



Cryptography and Network Security

cuu duong than cong . com

Chapter 5

cuu duong than cong . com Digital Signatures

Lectured by
Nguyễn Đức Thái

Outline

- Digital Signatures
- Digital Signature Algorithm and Standard

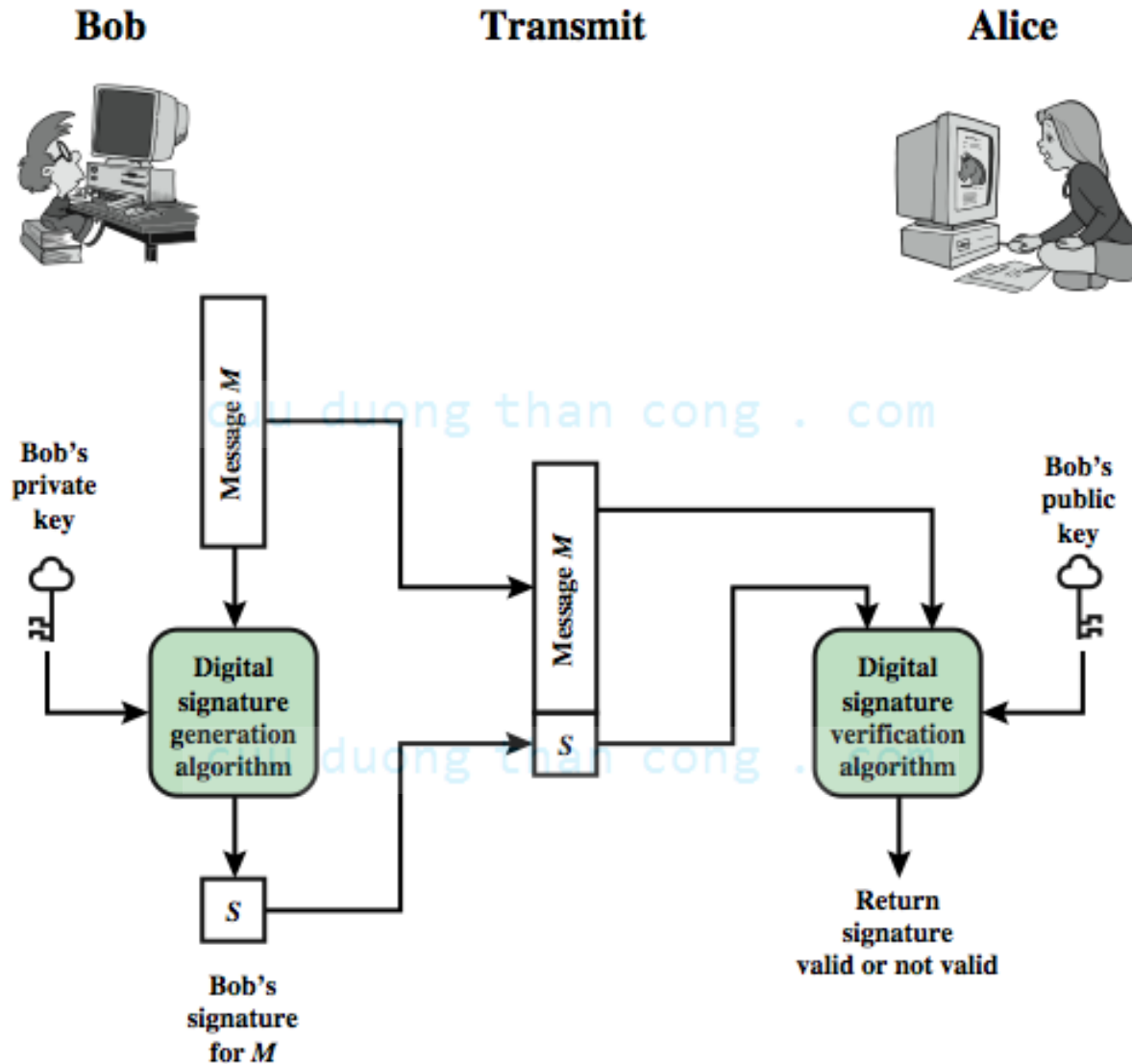
cuu duong than cong . com

cuu duong than cong . com

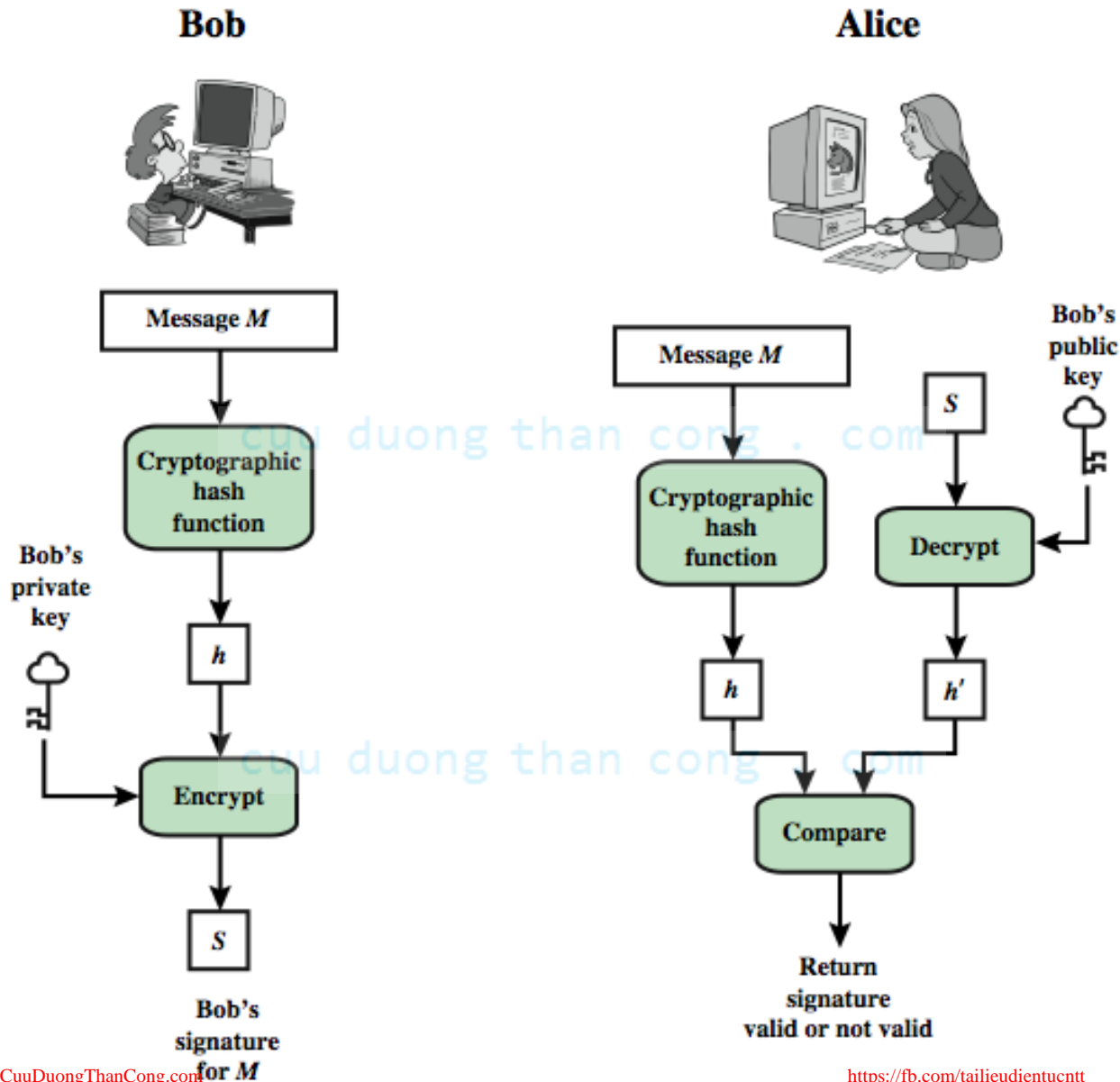
Digital Signatures

- A **digital signature** is an **authentication mechanism** that enables the creator of a message to attach a code that acts as a signature.
- Typically the signature is formed by taking the **hash of the message** and **encrypting the message with the creator's private key**.
- The signature guarantees the **source** and **integrity** of the message.
- The digital signature standard (DSS) is an NIST standard that uses the **secure hash algorithm** (SHA).

Digital Signature Model



Digital Signature Model



Attacks and Forgeries

■ attacks

- key-only attack
- known message attack
- generic chosen message attack
- directed chosen message attack
- adaptive chosen message attack

■ break success levels

- total break
- selective forgery
- existential forgery

Digital Signature Requirements

- must depend on the message signed
- must use information unique to sender
 - to prevent both forgery and denial
- must be relatively easy to produce
- must be relatively easy to recognize & verify
- be computationally infeasible to forge
 - with new message for existing digital signature
 - with fraudulent digital signature for given message
- be practical save digital signature in storage

Direct Digital Signatures

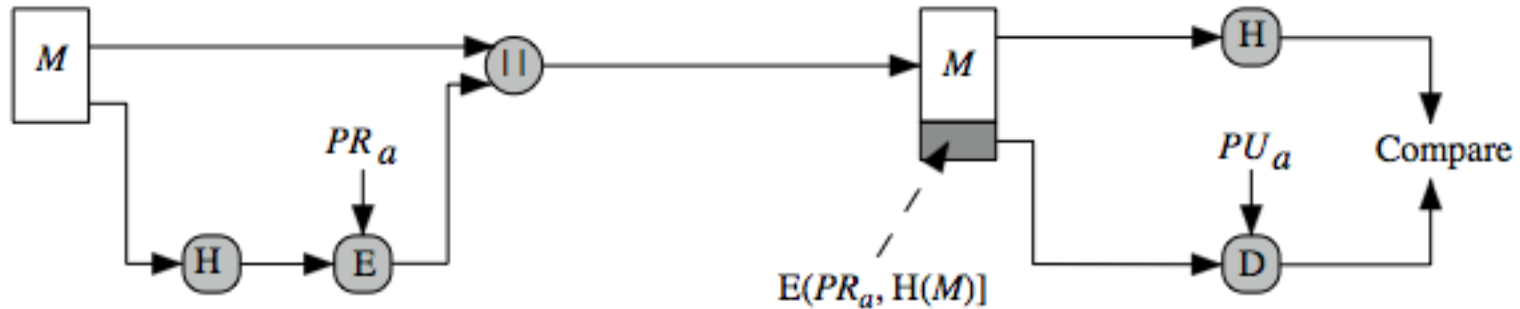
- involve only sender & receiver
- assumed receiver has sender's public-key
- digital signature made by sender signing entire message or hash with private-key
- can encrypt using receivers public-key
- important that **sign first** then encrypt message & signature
- security depends on sender's private-key

cuu duong than cong . com

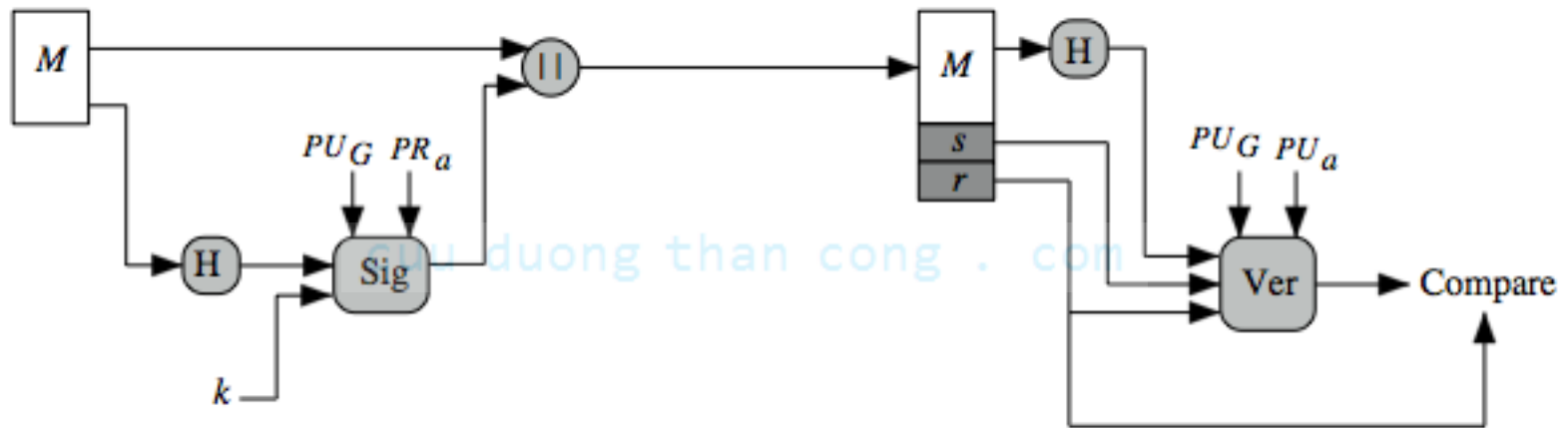
Digital Signature Standard (DSS)

- US Govt approved signature scheme
- designed by NIST & NSA in early 90's
- published as FIPS-186 in 1991
- revised in 1993, 1996 & then 2000
- uses the SHA hash algorithm
- DSS is the standard, DSA is the algorithm
- FIPS 186-2 (2000) includes alternative RSA & elliptic curve signature variants
- DSA is digital signature only unlike RSA
- is a public-key technique

DSS vs. RSA Signatures



(a) RSA Approach



(b) DSS Approach

Digital Signature Algorithm (DSA)

- creates a 320 bit signature
- with 512-1024 bit security
- smaller and faster than RSA
- a digital signature scheme only
- security depends on difficulty of computing discrete logarithms
- variant of ElGamal & Schnorr schemes

cuu duong than cong . com

DSA Key Generation

- **have shared global public key values (p,q,g):**
 - choose 160-bit prime number q
 - choose a large prime p with $2^{L-1} < p < 2^L$
 - o where $L = 512$ to 1024 bits and is a multiple of 64
 - o such that q is a 160 bit prime divisor of $(p-1)$
 - choose $g = h^{(p-1)/q}$
 - o where $1 < h < p-1$ and $h^{(p-1)/q} \bmod p > 1$
- **users choose private & compute public key:**
 - choose random private key: $x < q$
 - compute public key: $y = g^x \bmod p$

DSA Signature Creation

- **to sign a message M the sender:**
 - generates a random signature key k , $k < q$
 - Note: k must be random, be destroyed after use, and never be reused

- **then computes signature pair:**

$$r = (g^k \bmod p) \bmod q$$

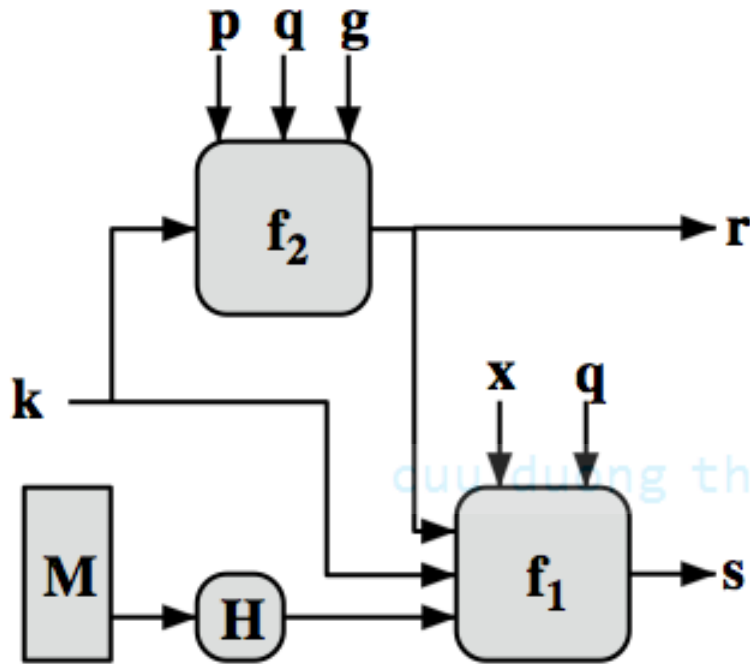
$$s = [k^{-1}(H(M) + xr)] \bmod q$$

- **sends signature (r,s) with message M**

DSA Signature Verification

- having received M & signature (r,s)
- to verify a signature, recipient computes:
 $w = s^{-1} \bmod q$
 $u_1 = [H(M)w] \bmod q$
 $u_2 = (rw) \bmod q$
 $v = [(g^{u_1} y^{u_2}) \bmod p] \bmod q$
- if $v=r$ then signature is verified
- see Appendix A for details of proof why

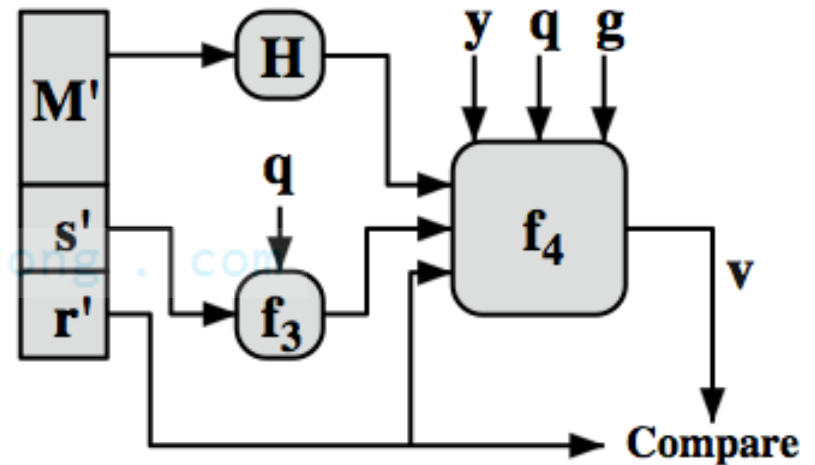
DSS Overview



$$s = f_1(H(M), k, x, r, q) = (k^{-1} (H(M) + xr)) \bmod q$$

$$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$$

(a) Signing



$$w = f_3(s', q) = (s')^{-1} \bmod q$$

$$v = f_4(y, q, g, H(M'), w, r')$$

$$= ((g^{H(M')w} \bmod q \cdot y^{r'w} \bmod q) \bmod p) \bmod q$$

(b) Verifying

Summary

We have discussed:

- Digital Signatures
- Digital Signature Algorithm and Standard

cuu duong than cong . com

cuu duong than cong . com

References

1. Cryptography and Network Security, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, 2013

cuu duong than cong . com

cuu duong than cong . com