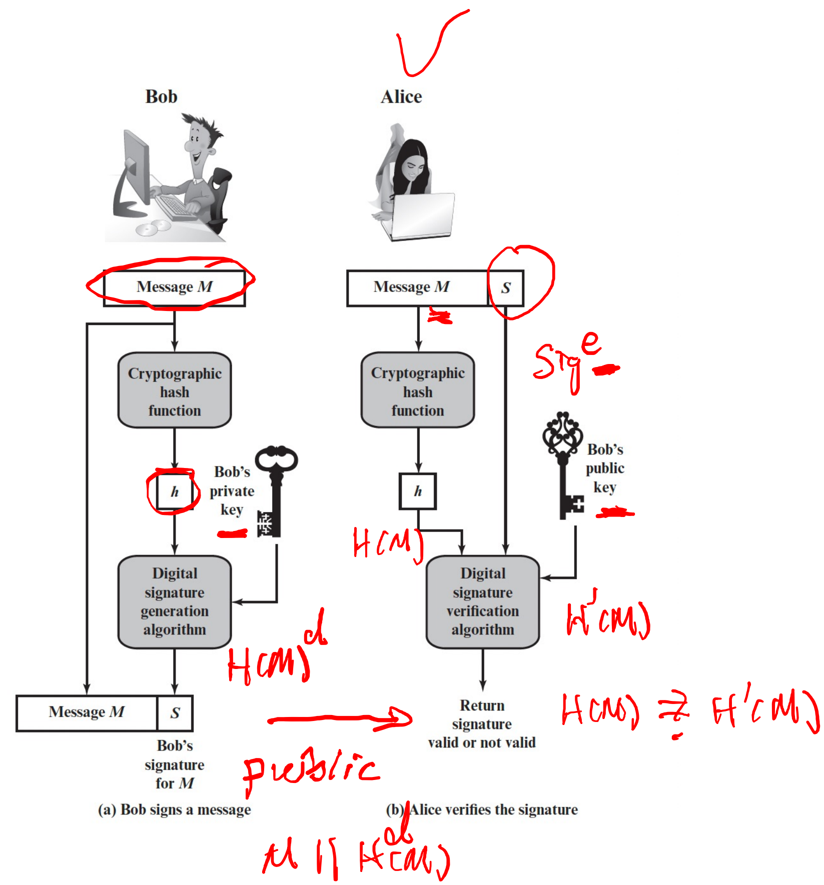
RSA Signatures

- Sign(d, M):
  - Compute $H(M)^d \bmod n$
- Verify(e, n, M, sig)
  - Verify that $H(M) \equiv sig^e \bmod n$



(a) Bob signs a message
(b) Alice verifies the signature

RSA Digital Signature Algo

Step1: Generate a hash value, or message digest, mHash from the message *M* to be signed

Step2: Pad mHash with a constant value padding1 and pseudorandom value salt to form *M'*

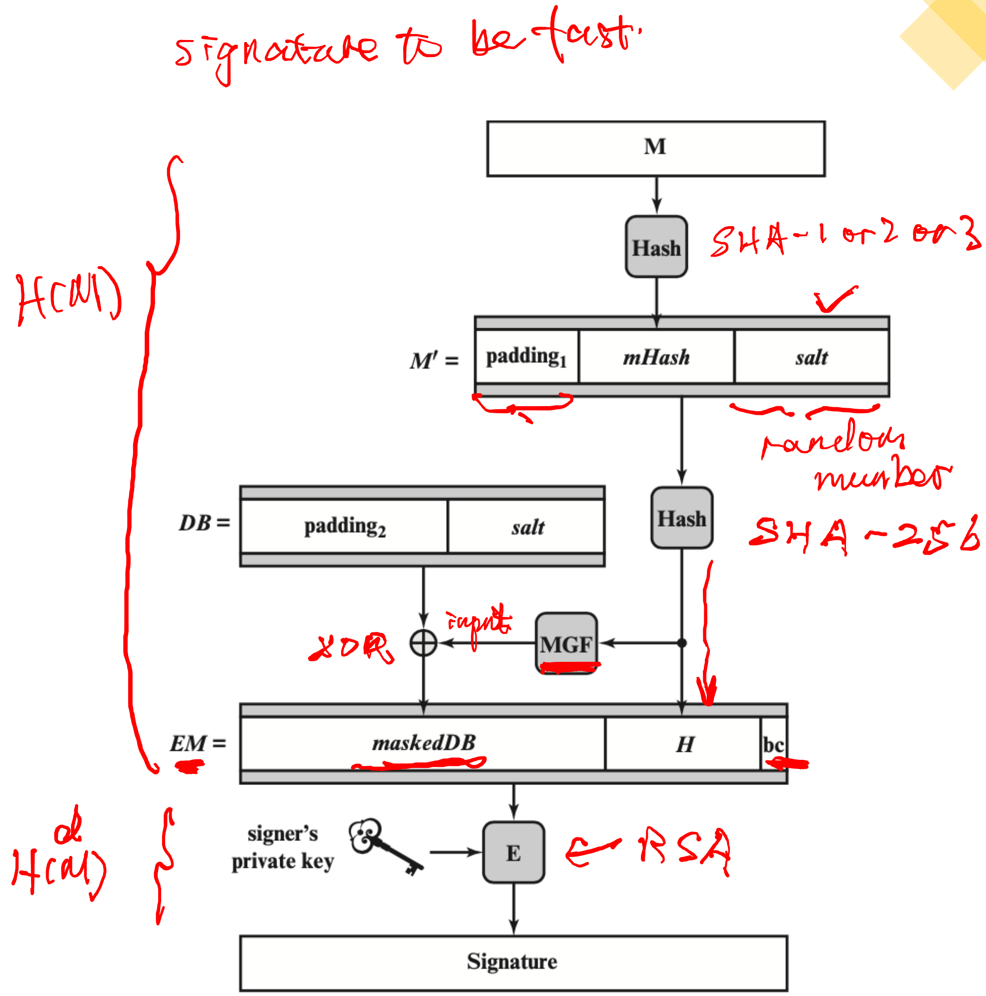
Step3: Generate hash value *H* from *M'*

Step4: Generate a block DB consisting of a constant value padding 2 and salt

Step5: Use the mask generating function MGF, which produces a randomized out-put from input *H* of the same length as DB

Step 6: Create the encoded message (EM) block by padding *H* with the hexadecimal constant bc and the XOR of DB and output of MGF

Step 7: Encrypt EM with RSA using the signer's private key



RSA Signatures: Correctness

Same prove process as RSA decryption

$H(M) \to$ { fast, less bandwidth }

Theorem: $sig^e \equiv H(M) \bmod N$

Proof:

Because $Sig = H(M)^d \bmod N$

$$sig^e = [H(M)^d]^e \bmod N = H(M)^{ed} \bmod N$$

$= H(M)^{de} \bmod N$ ① Because $d \cdot e \equiv 1 \bmod \phi(n)$

by definition of modular area

$d \cdot e = 1 + k \cdot \phi(n) \quad k \in \mathbb{Z}$

$= H(M)^{k \cdot \phi(N) + 1} \bmod N$

$= [H(M)^{\phi(N)}]^k \cdot H(M) \bmod N$

Euler's theorem

if $\gcd(M, N) = 1$

then $M^{\phi(N)} \equiv 1 \bmod N$

$= 1^k \cdot H(M) \bmod N$

$= H(M) \bmod N$ ∎

RSA Signatures: Correctness

Theorem: $sig^e \equiv H(M) \bmod N$

Proof:

$$sig^e = [H(M)^d\ ]^e \ mod\ N \quad = H(M)^{ed} \text{ mod N}$$

$$= H(M)^{k\phi(n)+1} \text{ mod N}$$

$$= [H(M)^{\phi(n)}]^k \cdot H(M) \quad \text{mod N}$$

$$= H(M) \quad \text{mod N}$$

RSA Digital Signature: Security

$(n, e) \to$ public channel

p ·

attacker

RSA Signature

$d = e^{-1} \bmod \phi(n)$

- **Necessary hardness assumptions:**
  - **Factoring hardness assumption:** Given *n* large, it is hard to find primes pq = n $p \cdot q$.
  - **Discrete logarithm hardness assumption:** Given *n* large, *hash*, and $hash^d$ *mod n*, it is hard to find *d*

Attacker: (n, e) $H(M)$ $H(M)^d$

M

$H(M)^d$

d

- Salt also adds security
  - Even the same message and private key will get different signatures

random number

$y = H(M)^d$

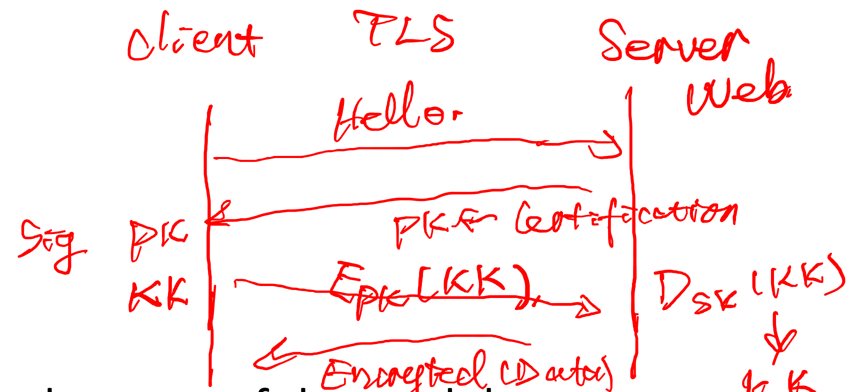
$d \log y = d \log H(M)^d$

sig

$= d\,[d \log H(M)]$

NP Hard

Hybrid Encryption



- Issues with public-key encryption
  - Notice: We can only encrypt small messages because of the modulo operator
  - Notice: There is a lot of math, and computers are slow at math
  - Result: We don't use asymmetric for large messages
- **Hybrid encryption**: Encrypt data under a randomly generated key *K* using symmetric encryption, and encrypt *K* using asymmetric encryption
  - Enc_{Asym}(PK, K); Enc_{Sym}(K, large message)
  - Benefit: Now we can encrypt large amounts of data quickly using symmetric encryption, and we still have the security of asymmetric encryption

Homework (Textbook) – no submission

- Review Question: 3.1, 3.2, 3.3, 3.4, 3.5, 3.6
- Problems:
  - prove correctness of RSA digital signature
  - 3.14 & 3.15

Homework 2 - individual

- For Chapter 3
- Deadline Friday, Nov. 1 before class
- 10% penalty per day for late submission

Thank you!

Network Security

Chapter 4

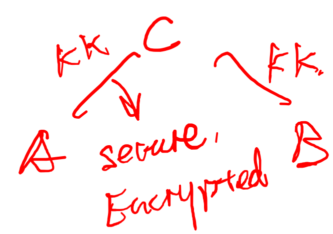
Key Distribution

Symmetric Key Distribution and User Authentication

4.2

Ways to achieve symmetric key distribution

- A key could be selected by A and physically delivered to B
- A third party could select the key and physically deliver it to A and B
  PK, symmetric key
- If A and B have previously and recently used a key, one party could transmit the new key to the other, using the old key to encrypt the new key
  KK
- If A and B each have an encrypted connection to a third-party C, C could deliver a key on the encrypted links to A and B



Terminologies

- Session key
- Permanent key
- key distribution center (KDC)
  - third party authority, centralized infrastructure
  - give permissions for two parties to communicate

Diffie-Hellman Key Exchange

Section 3.5

In class quiz on Wednesday

- We will have a short quiz on Wednesday, Oct. 30, in class
- A short quiz will cover the materials taught that day.
- Please be on time for class to avoid missing the quiz questions.