Fundamentals of Information & Network Security
ECE 471/571

Lecture #25: Digital Signature and Applications

Instructor: Ming Li

Dept of Electrical and Computer Engineering

University of Arizona

Digital Signature Schemes

- Definition of digital signatures
- RSA signatures
  - Construction
  - Correct usage
- Security of signature schemes
- Applications
  - How to combine encryption with signatures
  - Some example application scenarios

The RSA Signature Scheme

- Signing is equivalent to RSA decryption
- Verification is equivalent to RSA encryption

- Question: is the original RSA signature scheme secure?
  - Solutions?

Hash then sign!

Security of Signatures

- Attack goals
  - Total break--recovery of the private key.
  - Selective forgery: The adversary is given a message m and is able to find a signature σ such that $ver_K(m, \sigma)$=true.
  - Existential forgery: the adversary is able to find at least one valid (m, σ) pair.

- Attacker knowledge
  - Key-only attack--only public key is known.
  - Known message attack--think of known plaintext.
  - Chosen message attack--think of chosen plaintext

- Question: can a signature scheme be unconditionally secure?

Security Analysis of RSA Signature

- Existential forgery with key only attack
  - Yes
- Existential forgery with known message attack
  - Yes
- Selective forgery with chosen message attack
  - Yes

Combination with Hashes

- Existential forgery with known message attack
  - No
- Existential forgery with chosen message attack
  - No
- Existential forgery with key-only attack
  - No

PKCS—Public Key Cryptography Standard: Signature

- PKCS #1 for formatting a message to be signed:

0	1	at least eight octets of ff_{16}	0	ASN.1-encoded digest type and digest

- The encoding addresses several RSA threats: -

padding avoids smooth numbers w.h.p.

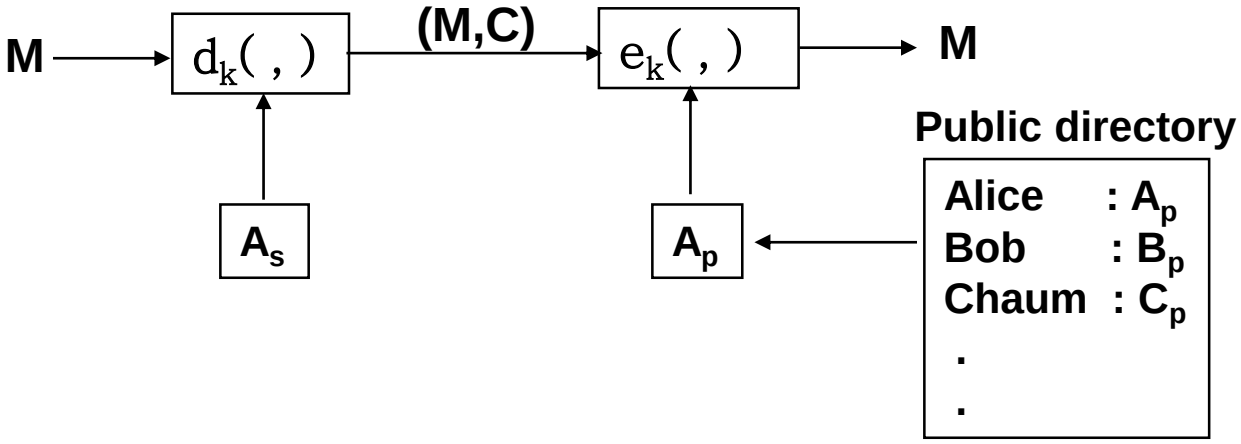
- avoids cube root problem
- including digest type avoids an obscure threat: MD4(m')=MD5(m) (why?)

Applications of Signatures

- Authentication (digital signature)
- Non-repudiation: Alice send a message to Bob. Later, Alice cannot deny having sent this message.

  - Sign M with Alice's private key : $C = d_K(A_s, M)$
  - Verify C with Alice's public key : $D = e_K(A_p, C)$

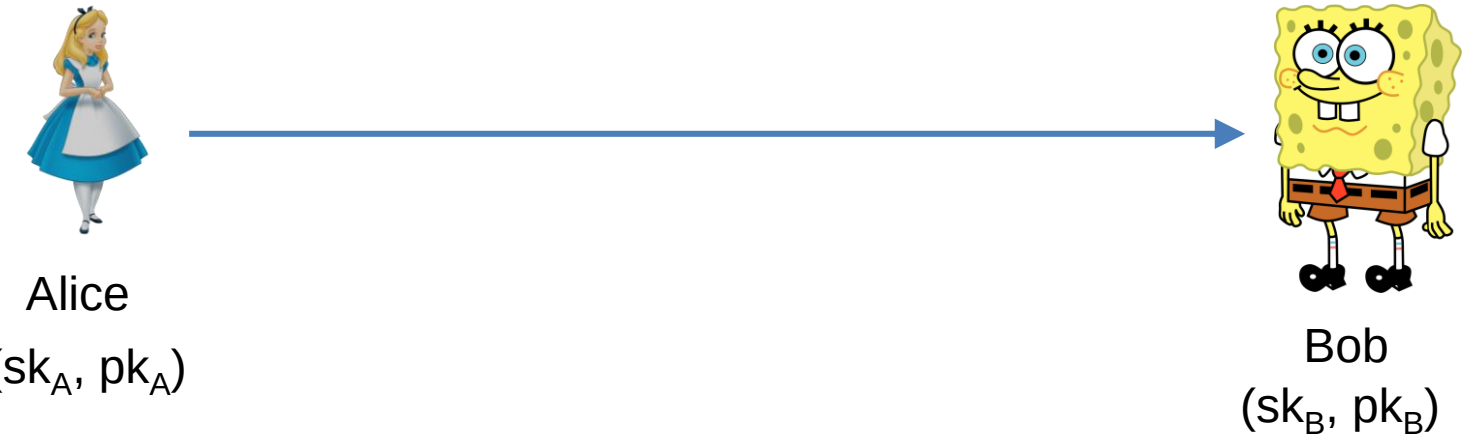
  * Only Alice can generate C, but anybody can verify C.



Combining Encryption with Signature

Send an encrypted and authenticated message x from Alice to Bob

Describe how Bob recovers and verifies x



Send an encrypted and authenticated message x from Alice to Bob

Alice
(sk_A, pk_A)

$E_{pkB}\ (x \parallel sig_{skA}\ (x))$

Bob
$(sk_B, pk_B), pk_A$

Bob decrypts the ciphertext using sk_B

Bob verifies the validity of Alice's signature by running $ver_{pkA}(sig_{skA}(x), x) = true$

Surreptitious Forwarding

Alice
(sk_A, pk_A)

$E_{pkB}\ (x \parallel sig_{skA}\ (x)\ )\ )$

Bob
$(sk_B, pk_B), pk_A$

$E_{pkC}\ (x \parallel sig_{skA}\ (x)\ )\ )$

Charlie

x: I love you!

Sign Bob's ID, then Encrypt

Alice
(sk_A, pk_A)

$E_{pkB}\ (x \parallel sig_{skA}\ (x, ID_B)\ )\ )$

Bob
$(sk_B, pk_B), pk_A$

Alice can also sign/encrypt/sign

Encrypt-then-Sign

Alice
(sk_A, pk_A)

$E_{pkB}(x) \,||\, sig_{skA}(E_{pkB}(x))$

Bob
$(sk_B, pk_B), pk_A$

pk_C

$E_{pkB}(x) \,||\, sig_{skC}(E_{pkB}(x))$

x: Proved Riemman's hypothesis conjecture

Encrypt Alice's Name – then Sign

$E_{pkB}(x, ID_A) \,||\, sig_{skA}(E_{pkB}(x)) \,||\, ID_A)$

Alice
(sk_A, pk_A)

Bob
$(sk_B, pk_B), pk_A$

Alice can also encrypt/sign/encrypt

Application Example

Country A

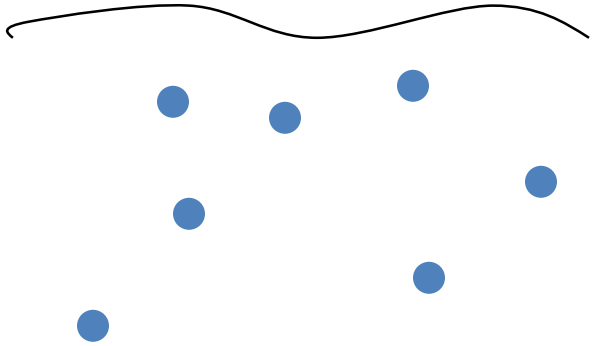
A wants to make sure that the data is not changed by B

Country B

B wants to make sure that the data does not contain anything else.

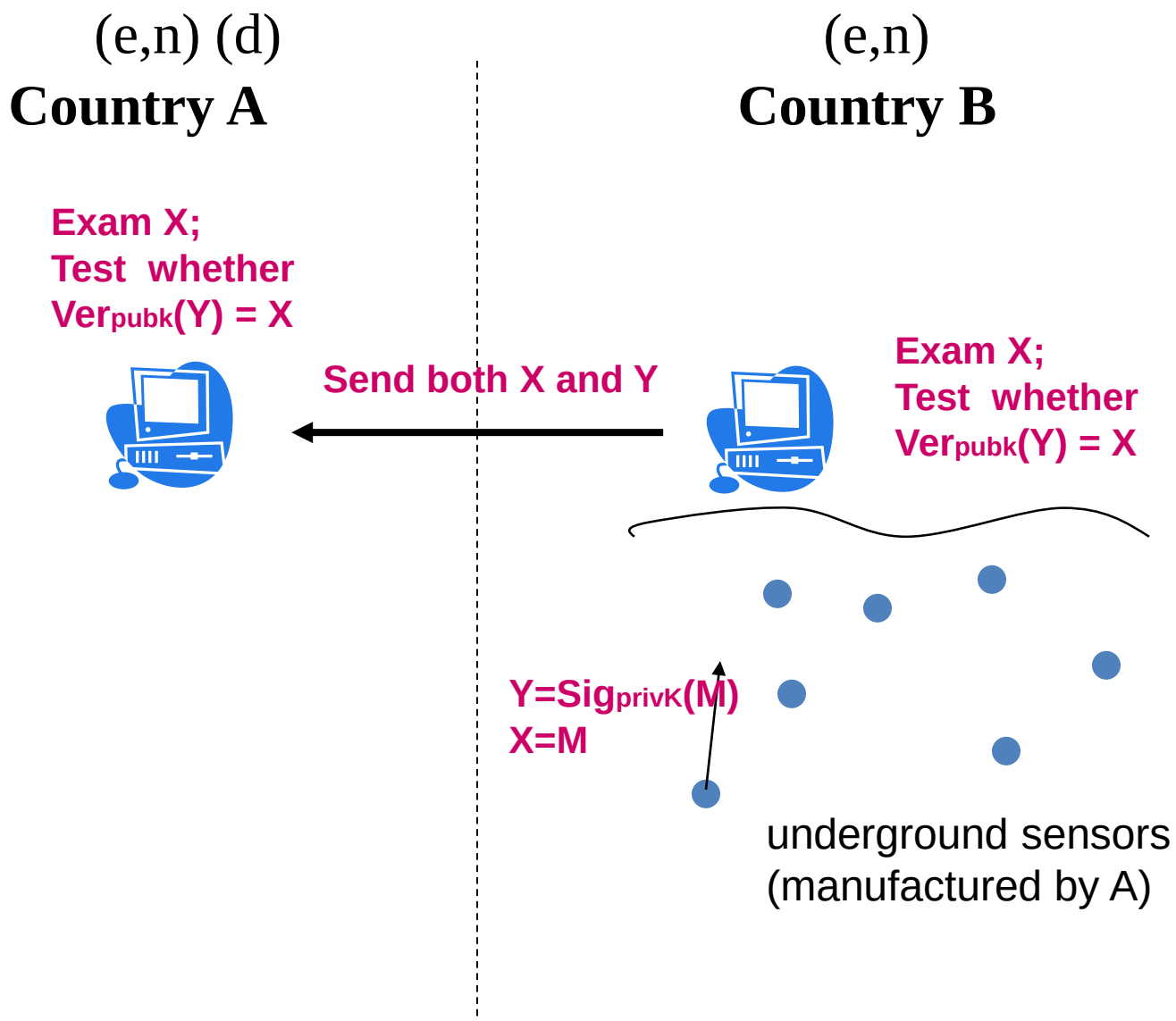
Send data to A

collect data from sensors



underground sensors (manufactured by A)

A and B signed a nuclear test ban treaty


(e,n) (d)
Country A
(e,n)
Country B
Exam X;
Test whether
Ver_pubk(Y) = X
Send both X and Y
Exam X;
Test whether
Ver_pubk(Y) = X
Y=Sig_privK(M)
X=M
underground sensors
(manufactured by A)