CE/CZ4052 Cloud Computing

Cloud Security

Dr. Tan, Chee Wei

Email: cheewei.tan@ntu.edu.sg

Office: N4-02c-104

“Three people can keep a secret only if two of them are dead!”

– Benjamin Franklin

Outline

- Principles of security
- Plain Text and Cipher Text
- Encryption/Decryption
  - Symmetric key cryptography
  - Asymmetric key cryptography

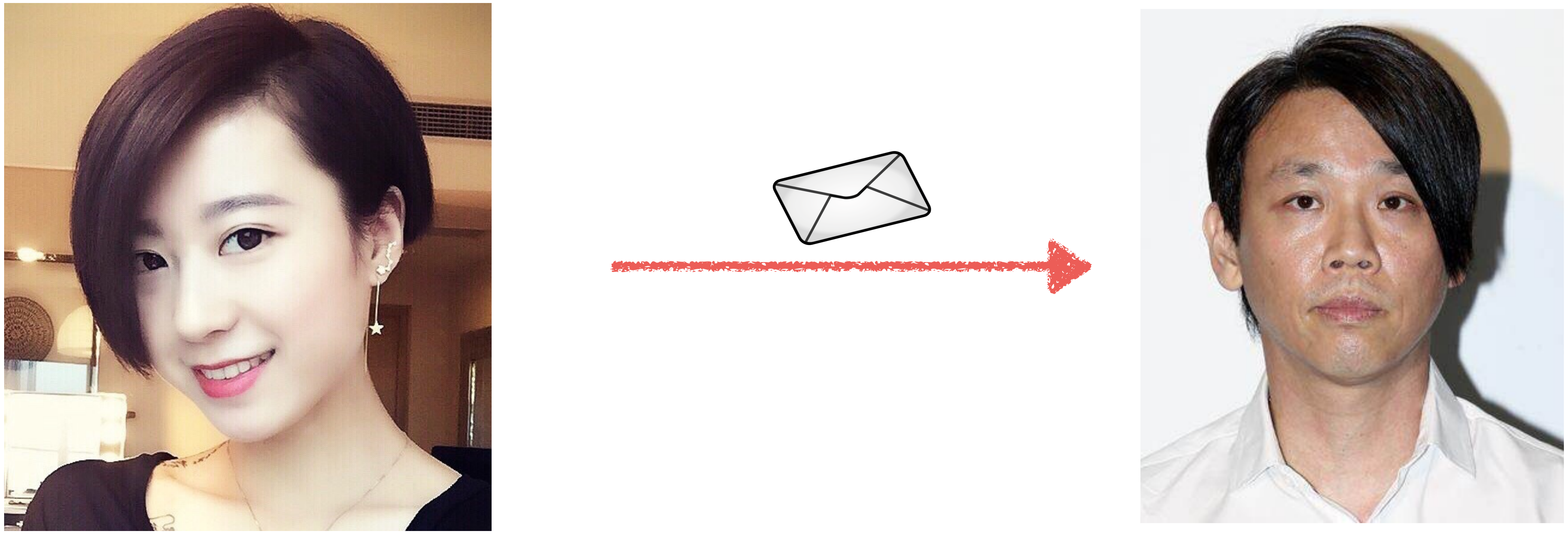
Principles of security

Principles

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

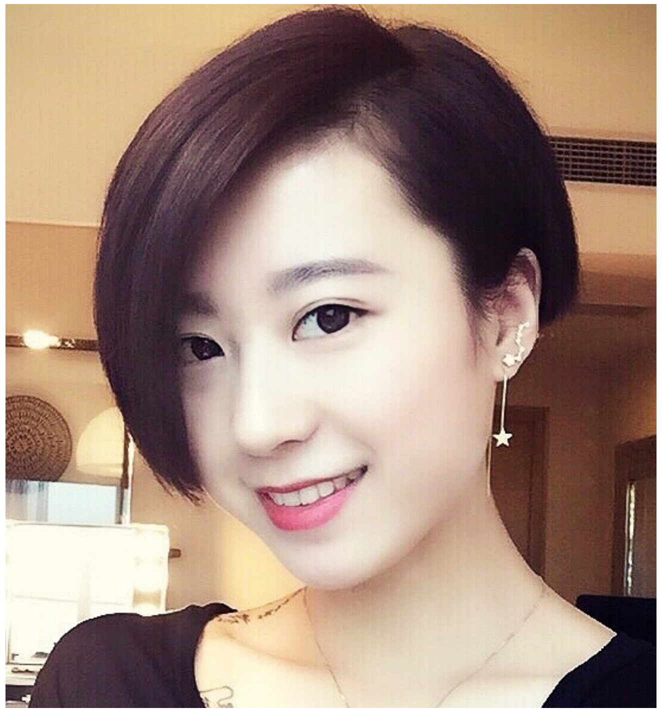
Confidentiality

- Alice wants to make sure no one except Bob gets the envelop, and even if someone else gets it, that person does not come to know about the details of the envelope.
- Otherwise, headline of tabloids, career deep-dive



Integrity

- An attacker may not know the details of the envelope, but he/ she can intercept and burn the envelop…
- Alice and Bob want to make sure no one can temper with the contents of the message (location, date, etc.)



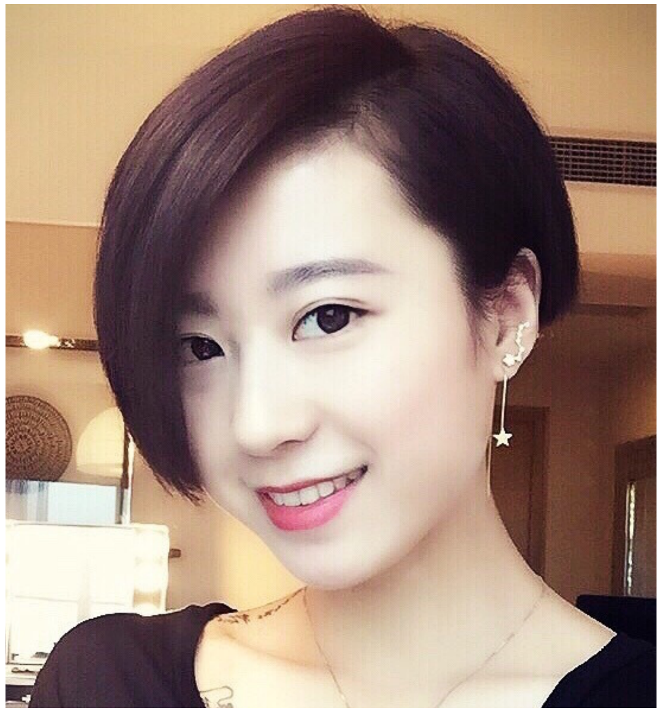
Authentication

- Bob wants to make sure that the invite is indeed from Alice, not from someone else posing as Alice.
- Otherwise, could be embarrassing…

Non-repudiation

- Later some tabloids found out about Alice’s invite, but Alice claimed that she never sent the message to Bob, i.e. Alice repudiates (happens a lot…)

- There should be some mechanism to defeat such a possibility of denying something which you have done.



“I didn’t invite him. He invited me to the hotel!”

Plain Text and Cipher Text

Plain text

- Can be understood by anyone knowing the language

Hi Bob,

I really like you and I know you have some problems with your new movie. Maybe you wanna talk about it with me, say this Saturday 8pm at Hotel A?

Alice

Cipher text

- Use some scheme to codify the message, so that it’s not easily understood by someone who doesn’t know the coding scheme.

Kl Ere,

L uhdoob olnh brx dqg L nqrz brx kdyh vrph sureohpv zlwk brxu qhz prylh. Pdbeh brx zdqqd wdon derxw lw zlwk ph, vdb wklv Vdwxugdb 8sp dw Krwho D?

Dolfh

Two methods

- There are two primary ways in which a plain text message can be codified to obtain a cipher text:
- Substitution and Transposition
- The previous cipher text is a result of Caesar Cipher, which substitutes each alphabet by shifting it three places down the line
- “A” -> “D”, “b” -> “e”

Substitution

- **Modified Caesar Cipher:** each alphabet is replaced by one that is k places down the line, where k is from 1 to 25.

- You need 25 attempts at most to crack k and decipher the cipher text

- Instead of a uniform substitution scheme, you can have random substitution

- **Polygram Substitution Cipher:** replace a block of alphabets with another. “HELLO” -> “YUQQW”, “HELL” -> “TEUI”

Transposition

- In addition to replacing the alphabets, we also perform some permutation over them
- Rail Fence Technique
  - Write down the plain text as a sequence of diagonals
  - Read the text written as above as a sequence of rows

Transposition

- Plain text: “Come home tomorrow”

C m h m t m r o

o e o e o o r w

Cipher text: Cmhmtmrooeoeoorw

Some concepts

- Cryptography: a mechanism of encoding messages so that they can be sent securely
- Brute-force attack: try all combinations and permutations to decipher a message
- Encryption: encoding the plain text into cipher text
- Decryption: the reverse process

Some concepts

- Encryption/decryption involves two aspects: the algorithm, and the key

- The sender and receiver must agree on a common algorithm for encryption/decryption

- The key is used to make the process of cryptography secure

- The algorithm is known to everybody

Cryptography

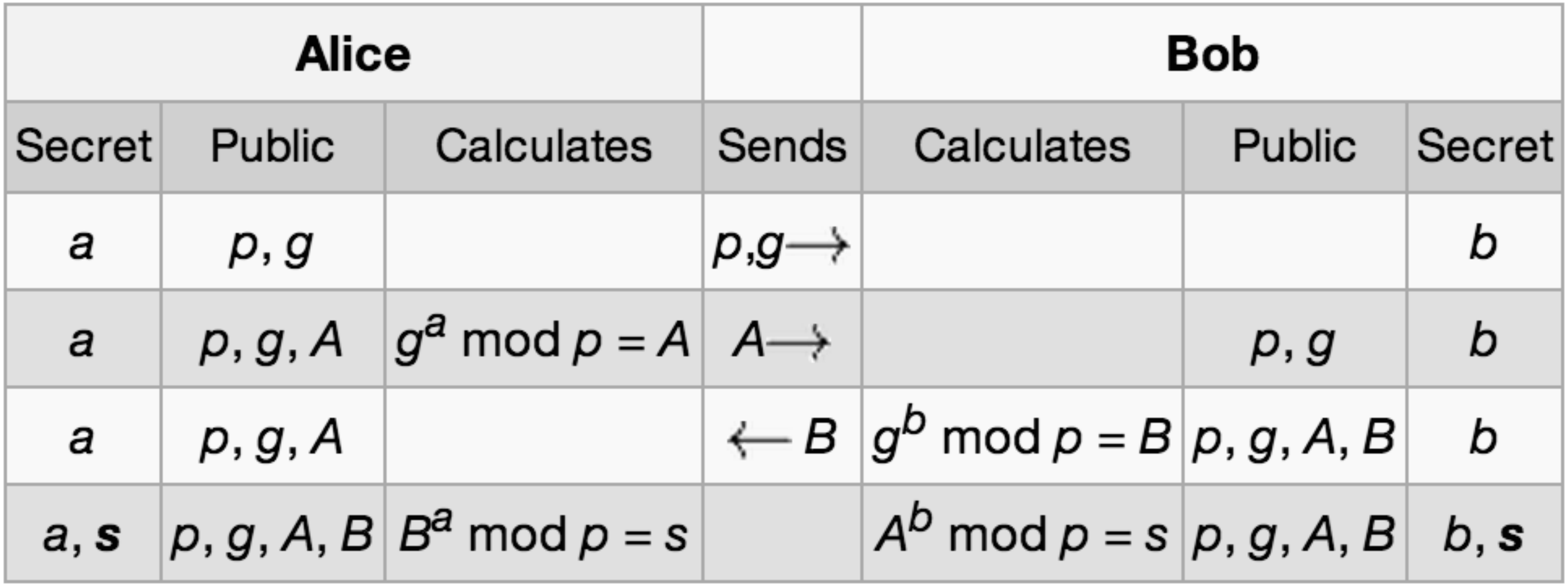
- Broadly, there are two mechanisms used in cryptography
- Symmetric Key Cryptography: the same key is used for encryption and decryption
- Asymmetric Key Cryptography: two different keys are used

Symmetric key cryptography

- The communication channel is insecure. How can we settle on the key to be used for cryptography over this insecure channel?

- Diffie-Hellman key exchange algorithm (1976)

- p, g: prime numbers. a, b: random numbers



Alice				**Bob**		
Secret	Public	Calculates	Sends	Calculates	Public	Secret
a	p, g		$p,g \longrightarrow$			b
a	p, g, A	$g^a \bmod p = A$	$A \longrightarrow$		p, g	b
a	p, g, A		$\longleftarrow B$	$g^b \bmod p = B$	p, g, A, B	b
$a, \mathbf{s}$	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	$b, \mathbf{s}$

Diffie-Hellman key exchange

- Alice computes s=g^{ba} mod p. Bob computes s=g^{ab} mod p.
- Example: Alice and Bob agree to use p=23 and g=5 (publicly). Alice secretly uses a=6, and Bob secretly chooses b=15.

Alice sends to Bob A = g^a mod p = 5^6 mod 23 = 8

Bob sends to Alice B = g^b mod p = 5^{15} mod 23 = 19

Alice computes s = B^a mod p = 19^6 mod 23 = 2

Bob computes s = A^b mod p = 8^{15} mod 23 = 2

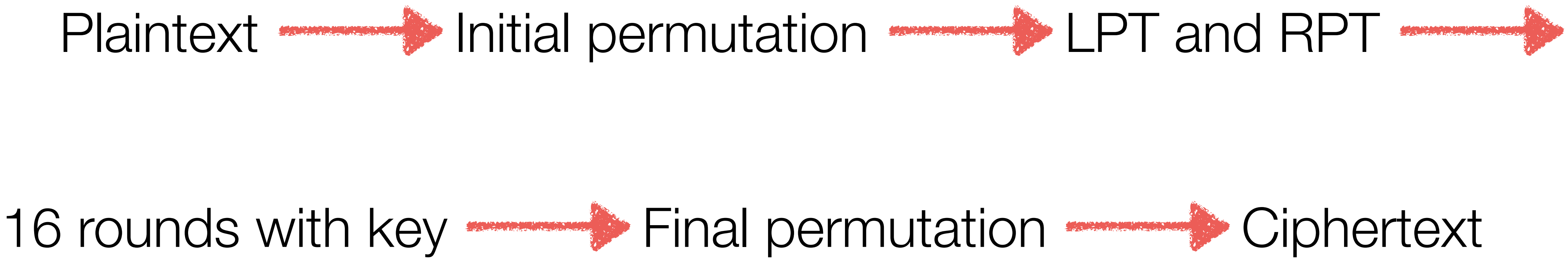
Diffie-Hellman key exchange

- If Alice and Bob can independently calculate the secret key s, so can an attacker who knows p, g, A, and B, right? — Not so easily

- If a, b, and p are large numbers, it's mathematically difficult to calculate a and b from p, g, A, and B only

DES

- Data Encryption Algorithm. Been used for over two decades.
- DES is a block cipher. It encrypts data in blocks of 64 bits. The key is 56 bits.



Plaintext → Initial permutation → LPT and RPT →

16 rounds with key → Final permutation → Ciphertext

Asymmetric key cryptography

- Also called Public Key Cryptography. A pair of keys are used
- Public key: used for encryption
- Private key: used for decryption. Only known to the owner. Only the corresponding private key can decrypt
- Requirements:
  - It’s computationally infeasible to find the private key given only the algorithm and public key
  - It’s computationally easy to en/decrypt a message using the relevant key

RSA

- The most popular and proven asymmetric key cryptography algorithm

- By Rivest, Shamir and Adleman of MIT, 1977

- It relies on a mathematical fact that it’s easy to find and multiple two large prime numbers, but it’s extremely difficult to factor their product back into two primes

RSA – Key generation

- Choose two large prime numbers P and Q. P=7, Q=17
- Calculate N=P*Q. N=119
- Select the public key E such that it is not a factor of (P-1)(Q-1). (P-1)(Q-1)=6*16. Let’s choose E=5
- Select the private key D such that the following is true:
    - (D*E) mod (P-1)(Q-1) = 1
- Let’s choose D=77, because 77*5 mod 96 = 1

RSA – En/decryption

- Suppose the keys are generated by Bob. Bob gives Alice its public key E and the number N.
- Alice wants to send a character “F” to Bob. She’ll use Bob’s public key to encrypt it
    - CT = PT^E mod N = PT^E mod P*Q
    - Alice sends 6^5 mod 119 = 41
- Bob uses the following: PT = CT^D mod N
    - Bob gets 41^{77} mod 119 = 6

RSA

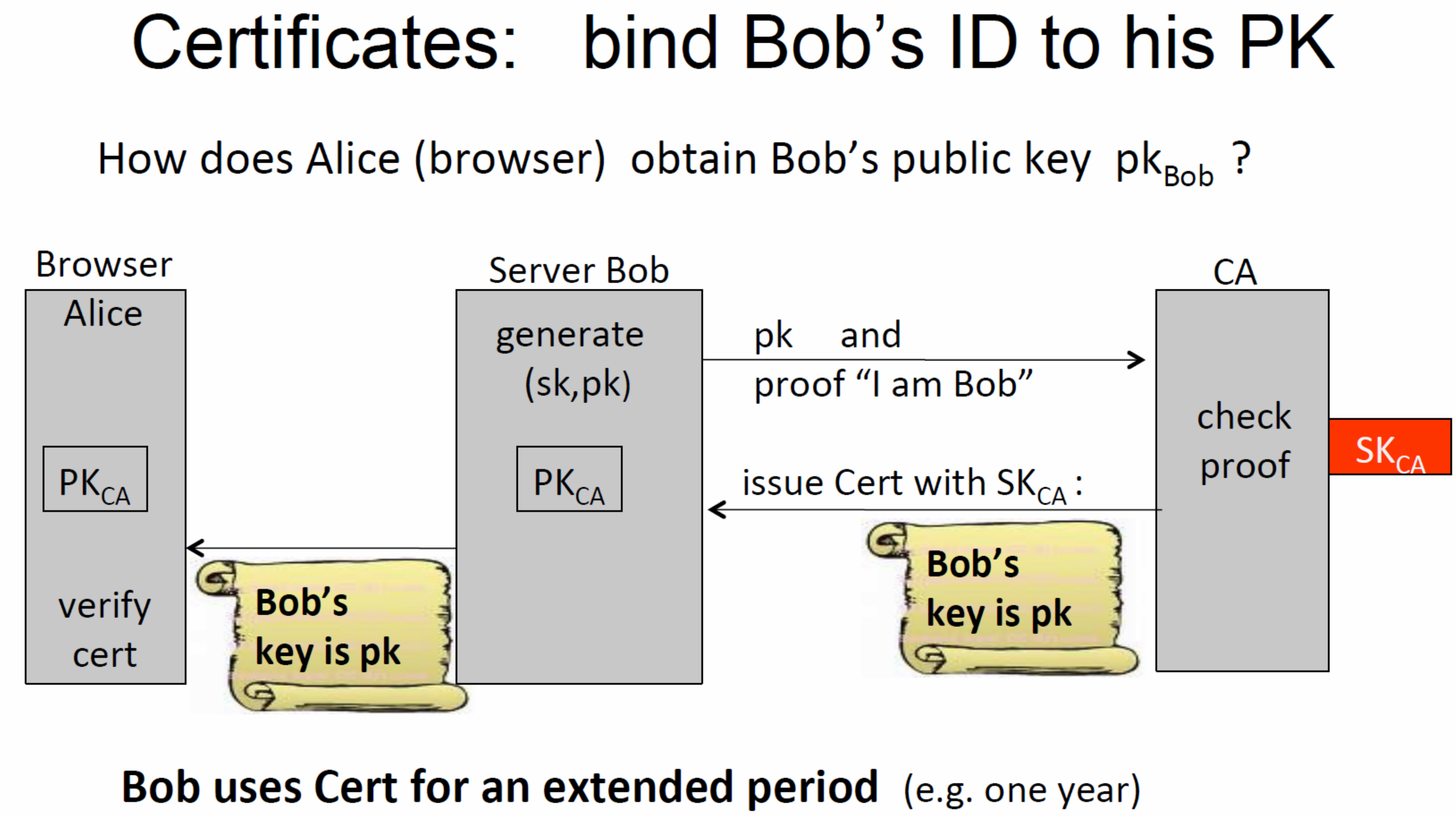
- For an attacker to crack the message, he needs to find the values of P and Q using N. This is extremely difficult for large primes.
- Takes more than 70 years if N is 100 digit
- If Alice and Bob use RSA, it'll be difficult to crack their communication

“Factoring as a Service” (https://eprint.iacr.org/2015/1000.pdf), published in 2015, used Amazon EC2 cloud resources to factorize a 512-bit RSA modulus in just four hours for $75. What are the implications for network security?

Digital signatures

- When A sends to B, A uses B’s public key to encrypt, so the message is confidential
- In many situations we need “signatures” to verify the identity of someone
- We can use a different scheme
    - A uses his private key to encrypt a message
    - Anyone can check the message is signed by A by using A’s public key
    - Only A can sign the message

Digital certificates



Certificates: bind Bob’s ID to his PK

How does Alice (browser) obtain Bob’s public key pk_{Bob} ?

Browser

Alice

PK_{CA}

verify cert

Server Bob

generate (sk,pk)

PK_{CA}

pk and proof “I am Bob”

CA

check proof

SK_{CA}

issue Cert with SK_{CA} :

Bob’s key is pk

Bob’s key is pk

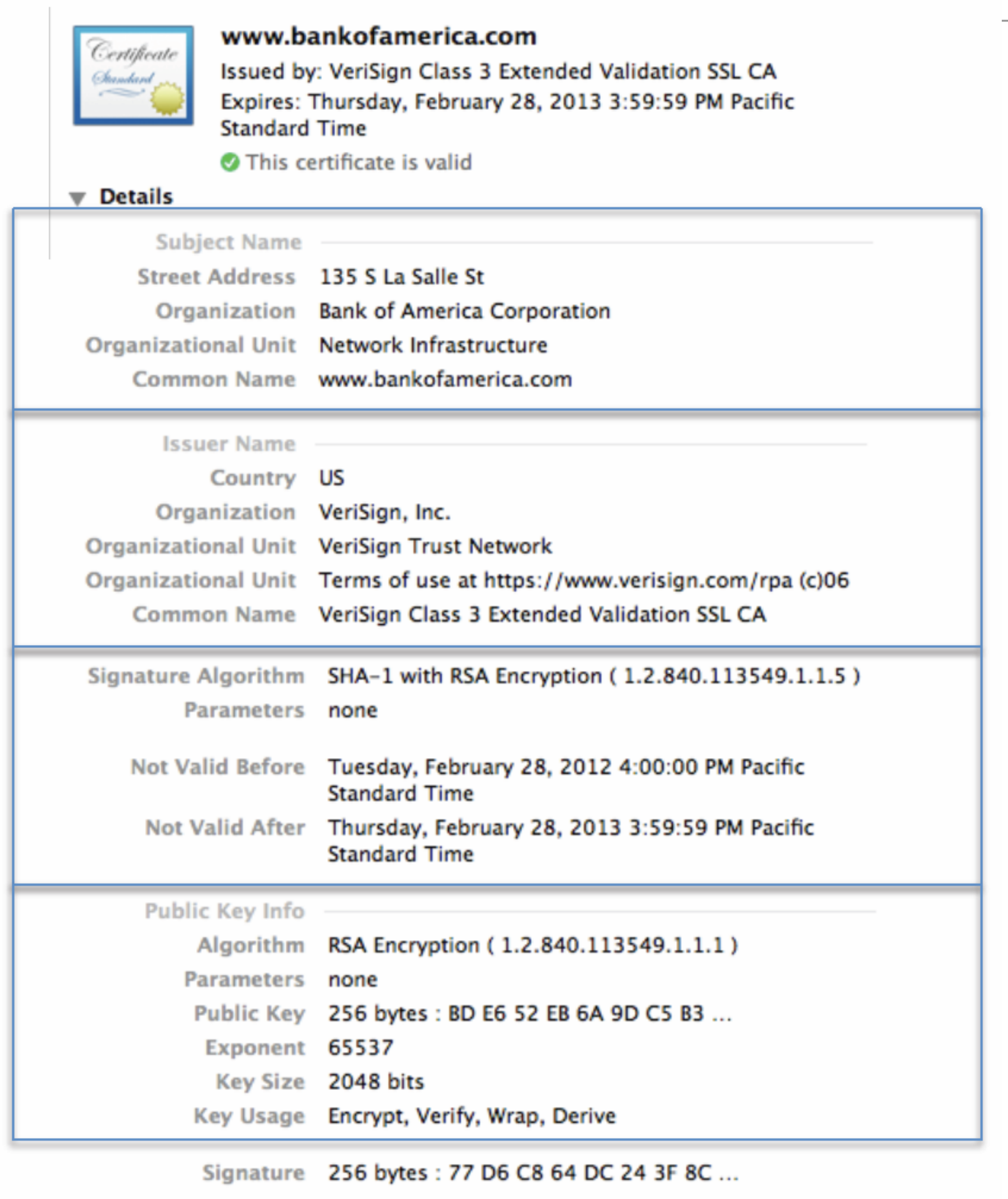
Bob uses Cert for an extended period (e.g. one year)

Public key infrastructure – PKI

- How do we know a key belongs to Bob?
- One solution: PKI
  - Trust certification/root authority (VeriSign, etc.)
    - Everyone must know the public key of root authority
    - Check your browser, you can find many
  - Root authority can sign certificates
  - Certificates identify others, including other authorities

DocuSign is a SaaS product that businesses use to send electronic signatures
https://en.wikipedia.org/wiki/DocuSign

Sample certificates



www.bankofamerica.com
Issued by: VeriSign Class 3 Extended Validation SSL CA
Expires: Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time
✓ This certificate is valid

▼ **Details**

Subject Name	
Street Address	135 S La Salle St
Organization	Bank of America Corporation
Organizational Unit	Network Infrastructure
Common Name	www.bankofamerica.com
Issuer Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)06
Common Name	VeriSign Class 3 Extended Validation SSL CA
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday, February 28, 2012 4:00:00 PM Pacific Standard Time
Not Valid After	Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : BD E6 52 EB 6A 9D C5 B3 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 77 D6 C8 64 DC 24 3F 8C ...