CS 4173/5173
COMPUTER SECURITY

Midterm Review

TIME AND LOCATIONS

- Time:
  - Tuesday, March 04, 2025
  - 3:00 PM – 4:15 PM

- Location:
  - Dale Hall 0103

BASIC CONCEPTS

- Concepts of security, objectives, cryptography and attacks
  - Confidentiality
  - Integrity
  - Availability
- Difference between cryptography and steganography
- Perfect Secure

BASIC CONCEPTS

- Concepts of symmetric and asymmetric cryptographic methods
  - Number of keys
- Mode of operations
  - ECB, CBC, …

BASIC CONCEPTS

- Concepts of hash functions
  - 4 prosperities
- Denial of service attacks: concepts, attack and defense
- P and NP

PERFECT SECURE

- Basic concept

- One-time pad is perfect secure

- You should be able to use the concept of perfect secure to analyze if a design is good.

SYMMETRIC CRYPTO

- Block ciphers
  - Avalanche effects
  - Feistel cipher: architecture and computation
- DES
  - Parameters
  - Architecture
  - Double-DES and attacks
  - Triple-DES
- AES
  - Parameters

MODES OF OPERATIONS

- ECB
  - Architecture, pros/cons
- CBC
  - Architecture, pros/cons
- CFB
  - Architecture, pros/cons
- CTR
  - Architecture, pros/cons
- You should be able to choose one based on the application requirements.

HASH FUNCTIONS

- Basic properties
- Common hash functions and parameters
  - MD5, SHA1, SHA256
- Applications of hash functions
  - Message authentication: HMAC vs CBC-MAC
  - Message integrity check
  - Password with salt
  - Commitment protocols
  - …

MIDTERM RULES

- Content coverage:
  - Slide 1 – Slide 10
- Rules:
  - Please come 5-10 minutes earlier
  - Closed laptop/neighbor/cellphone
  - 100 pts, 2 sections.
- Cheat sheet:
  - ONE letter-sized (8.5 by 11 inches) cheat sheet, front and back.

FINAL: SECTION I

- Section I : Single Choice

Examples:

_____ Which of the following design is to achieve availability

[A] encrypt all data in a system [B] add redundant servers to process user request

[C] verify a user's password [D] use alias to hide a user's name

FINAL : SECTION III

- Section II : Answer Questions
  - 4-6 questions

  You will be asked analyze a given design (e.g., an authentication protocol or an encryption scheme)

  Examples:
  - What are the properties of hash function.
  - What is the meet-in-the-middle attack?
  - There will be at least one question about analyzing the security of a system design.

CS 4173/5173
COMPUTER SECURITY

High Level Introduction to Public Key Cryptography

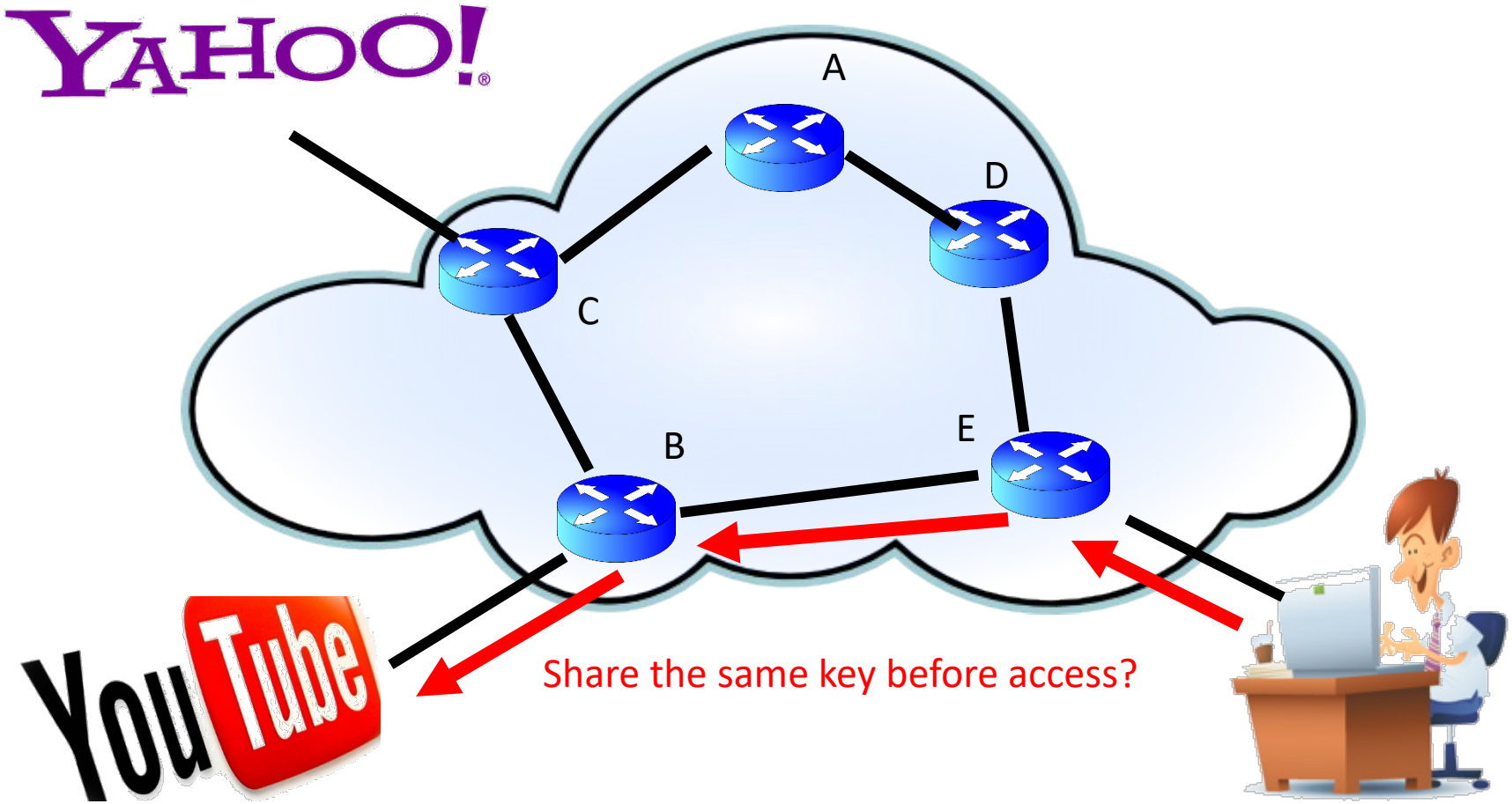
COMPANY A'S PROBLEM I

- Company A is a big web service company with over 10,000 employees.
- The president Bob wants to make sure that all employees can verify the authenticity of the announcement emails that he sends.
- Q: How to ensure authenticity of these emails.

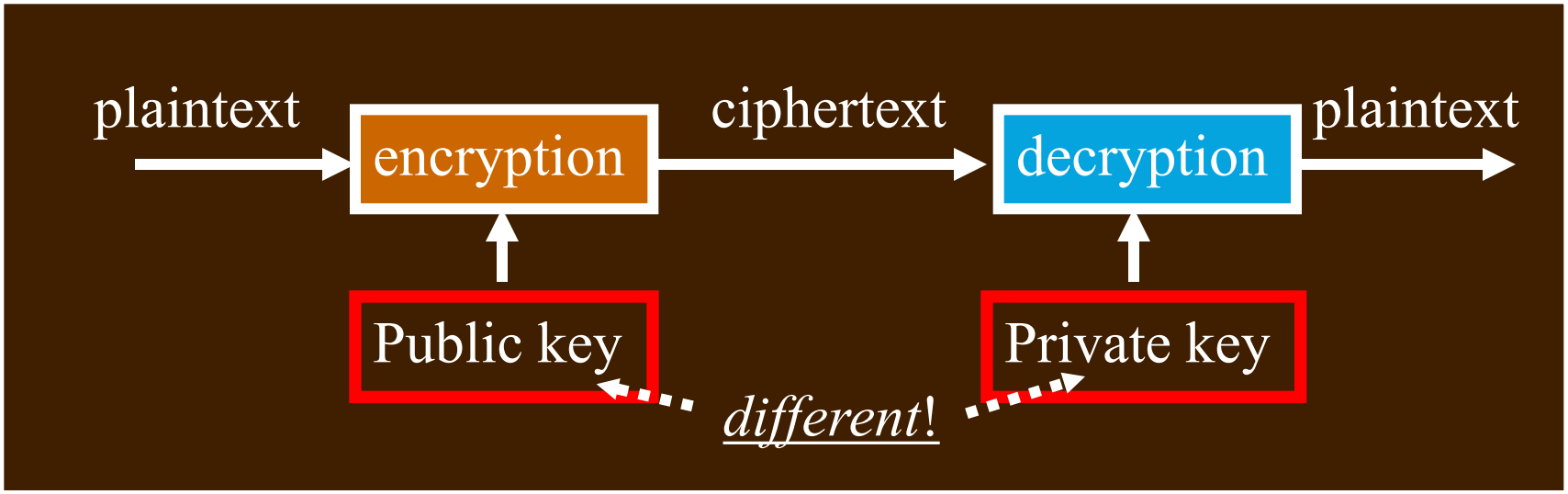
COMPANY A'S PROBLEM II

- Company A is accepting vulnerability report of their web system from the public.
- They need a design that someone can successfully send the report of a potential vulnerability via email to them.
- Q: How to ensure the confidentiality of reports?

HOW TO SECURELY SURF INTERNET



PUBLIC KEY CRYPTOGRAPHY

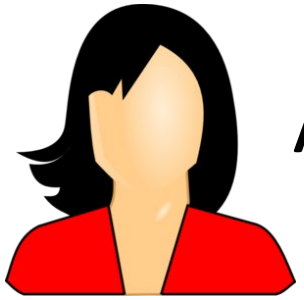


- Invented and published in 1975
- A *public / private key pair* is used
- Also known as *asymmetric* cryptography
- Much slower to compute than secret key cryptography

PUBLIC/PRIVATE KEY

- Public key – encrypt
- Private key – decrypt

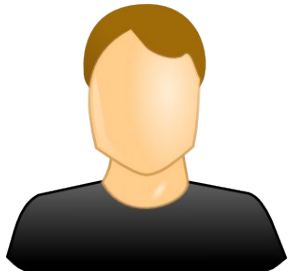
- How does the secret communication look like?



Alice

wants to send a message

Bob



PUBLIC/PRIVATE KEY

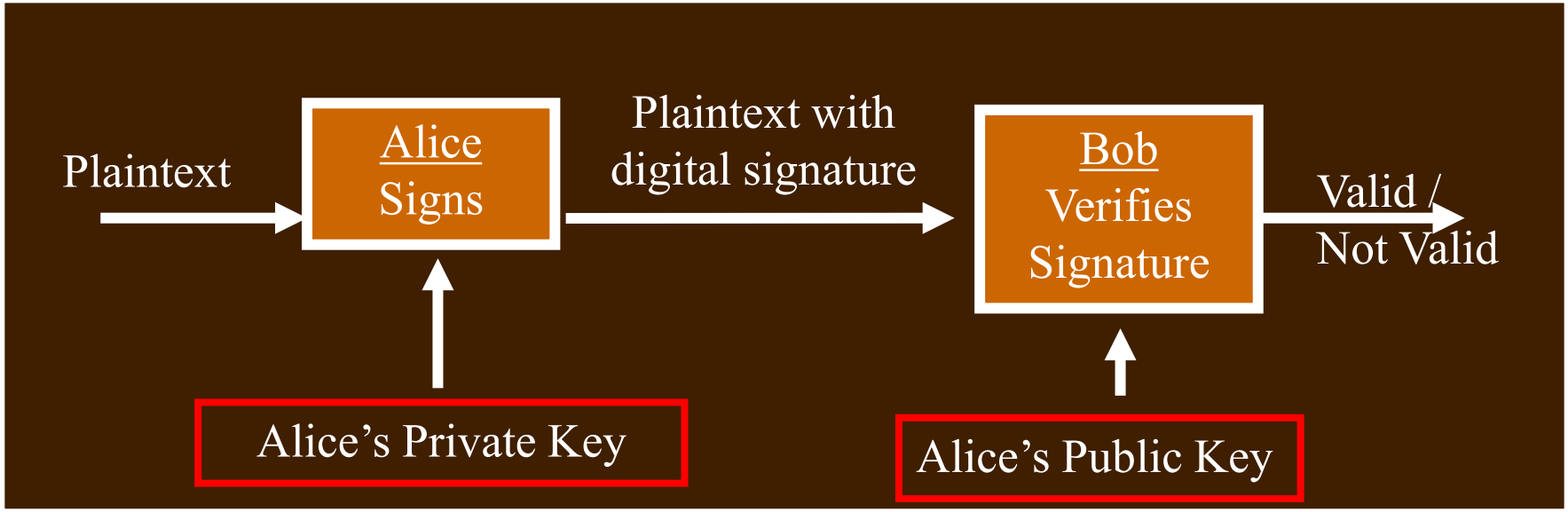
- Alice has her own public and private key pair
- Bob also has his own public and private key pair

- Public key
  - Can be released to the public

- Private Key
  - Must be kept secret.

AUTHENTICATION IN PUBLIC KEY CRYPTO

- Message integrity with digital signatures
- Alice computes hash, signs with her private key (no one else can do this without her key)
- Bob verifies hash on receipt using Alice's public key using the verification equation



AUTHENTICATION (CONT'D)

- Authentication in public key crypto:
  - Hash function to hash the message into a digest
  - The action of sign the digest with (private key)
  - The action of verify the digest with (public key)

PUBLIC-KEY REQUIREMENTS

- It must be computationally
  - easy to generate a public / private key pair
  - hard to determine the private key, given the public key
- It must be computationally
  - easy to encrypt using the public key
  - easy to decrypt using the private key
  - hard to recover the plaintext message from just the ciphertext and the public key

PUBLIC KEY ALGORITHMS

- Public key algorithms covered in this class, and their applications

System	Encryption / Decryption?	Digital Signatures?	Key Exchange?
RSA	Yes	Yes	Yes
Diffie-Hellman			Yes
DSA		Yes	

SOLVING COMPANY A'S PROBLEM I

- Company A is a big web service company with over 10,000 employees.
- The president Bob wants to make sure that all employees can verify the authenticity of the announcement emails that he sends.
- Answer:
  - Everyone knows Bob's public key.
  - Bob signs the email using his private key.
  - Everyone can verify the signed email using Bob's public key

SOLVING COMPANY A'S PROBLEM II

- Company A is accepting vulnerability report of their web system from the public.
- They need a design that someone can successfully send the report of a potential vulnerability via email to them.
- Answer:
  - Company A generates a key pair, then releases the public key to the public for vulnerability report.
  - Everyone uses the public key to encrypt the report.

PUBLIC KEY VS. SYMMETRIC KEY

Symmetric key	Public key
Two parties MUST trust each other	Two parties DO NOT need to trust each other
Both share same key	Two separate keys: a public and a private key
Typically faster	Typically slower
Examples: DES, RC5, AES, …	Examples: RSA, DSA, ECC…

COMPANY A'S PROBLEM III

- Company A provides an on-line chat service for vulnerability report.
  - Requirement 1: confidentiality.
  - Requirement 2: efficiency because there will be a number of message exchanges.

- Q: How to satisfy both requirements?

DIGITAL ENVELOPE: SYMMETRIC+ASYMMETRIC

1. Generate a secret key (called a session key) at random.
2. Encrypt the message using the session key and symmetric algorithm.
3. Encrypt the session key with the recipient's public key. This becomes the "digital envelope".
4. Send the encrypted message and the digital envelope to the recipient.

DIGITAL ENVELOPE (CONT'D)

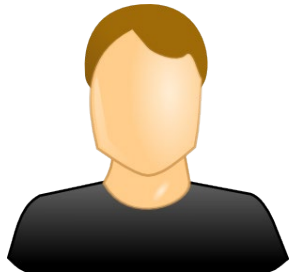
Alice (finds a vulnerability)

Bob (company representative)

Knows the public key: Kp

Generate a session key Ks

Encrypt message M using Ks
Encrypted Ks using Kp



Public key: Kp
Private key: Ki

1. Use Ki to decrypt Ks
2. Use Ks to decrypt M

Send a response using Ks

All remaining communication is based on Ks