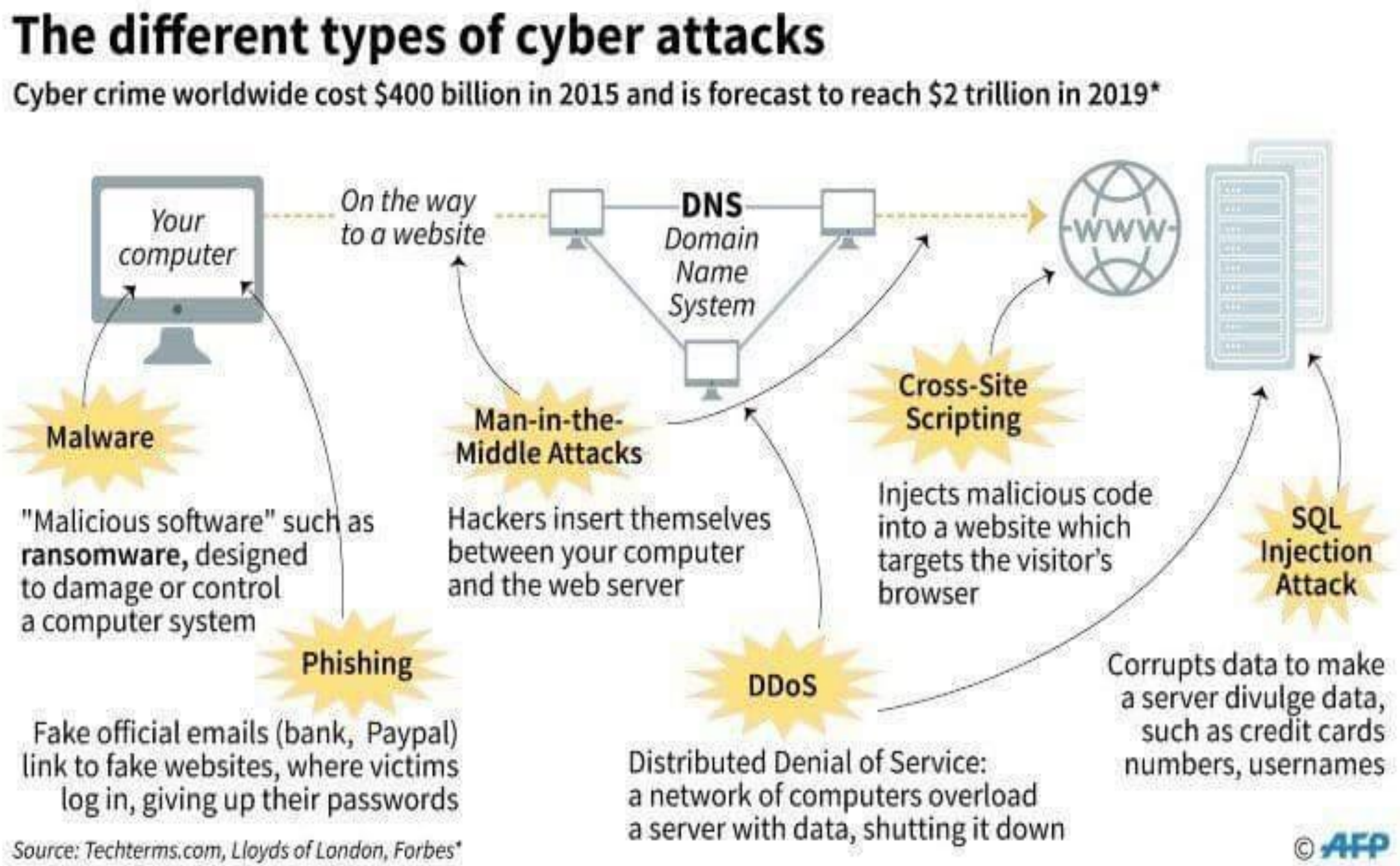
Introduction

Mahendra Pratap Singh
Assistant Professor
Dept. of Computer Science and Engineering

Acknowledgement: Slides drawn from Kurose & Ross

Present Scenario



Information Security Advice

- WhatsApp has become a common messenger now a days.
- With the help of mobile you can check the profile photo of the particular user.
- This may not be safe if the number falls into wrong hands.
- They may misuse your photo.
- To avoid this, set the privacy settings of your profile photo only to my contacts.

Why We Should Care about Security ?

- We use internet for many things
  - Online banking
  - Online shopping
  - Booking tickets …

- We store many things in computers
  - Photos
  - Files
  - Credit Card Number…..

Vulnerability and Attack

- Vulnerability: a weakness in system which allows a malicious user to gain access.
- Attack: a successful strategy to exploit a vulnerability in order to gain illegal access.
  - Active
  - Passive
- Attacker: someone who crafts an attack
  - Insider attacker- e.g., Employee, Vendor, Partner
  - Outside attacker- e.g., Cyber-criminals, Spies, Hackers, Malware, Nation-state intelligence agencies, etc.

Active Attack

- An active attack attempts to alter system resources or affect their operations.

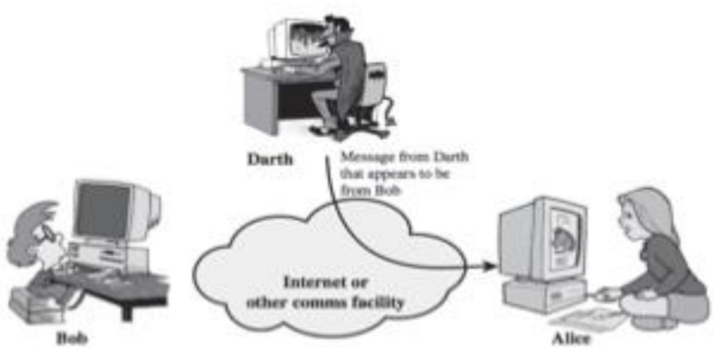


Figure 1.7 Masquerade

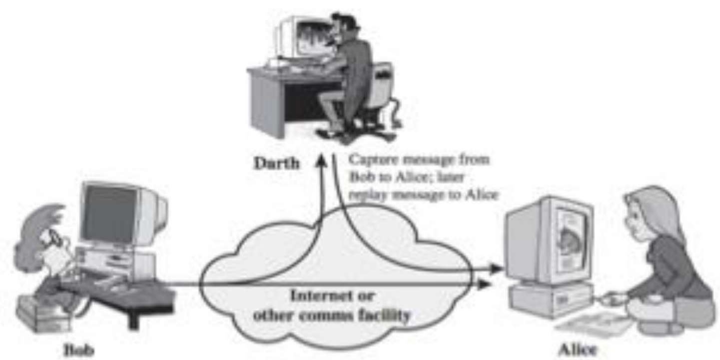


Figure 1.7 Replay

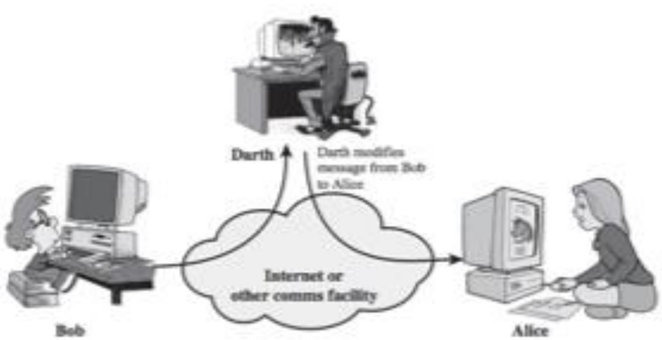


Figure 1.7 Modification of Messages

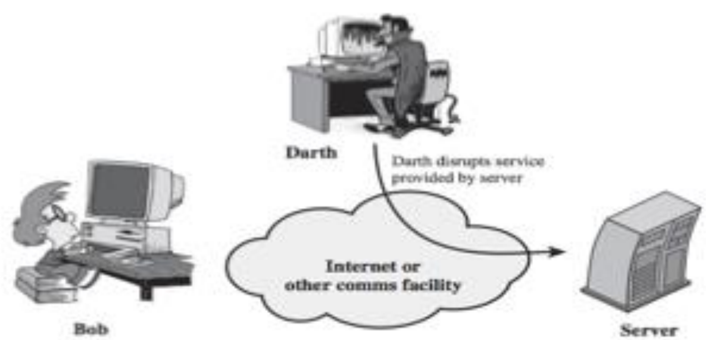


Figure 1.7 Denial of Service (DoS)

Passive Attack

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.

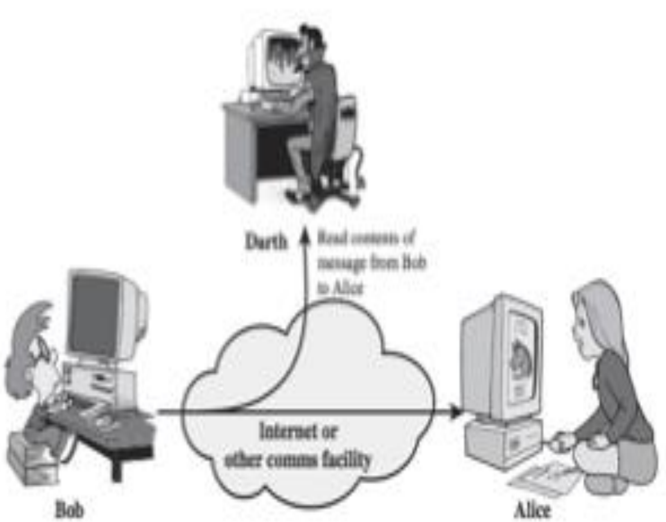


Figure 1.3 Release of Message Contents

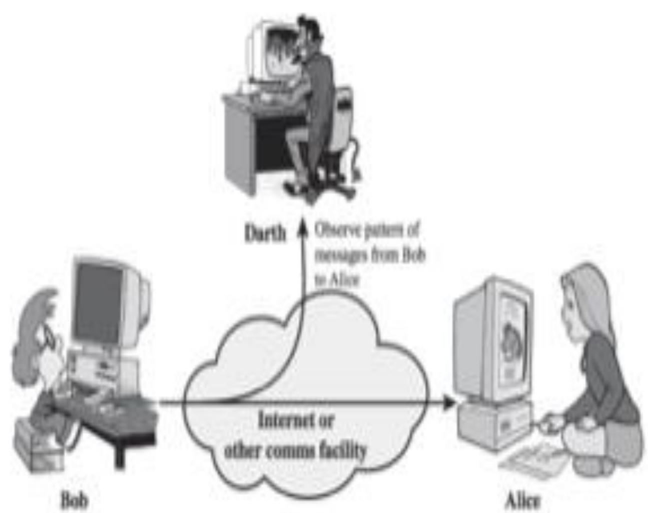


Figure 1.3 Traffic Analysis

Threat

- A threat is a possible danger that might exploit a vulnerability to breach security.

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Network and System Attacks

- Information Gathering
- Buffer Overflow Attacks
- Format String Attacks
- SQL Injection Attacks
- Spoofing Attacks
- Phishing Attacks
- DoS Attacks
- Virus, Worms, Trojan Horse
- Session Hijacking
- Snooping and Sniffing
- OS and Unix System Security
- Botnets
- Spamming

Defense Mechanisms

- Antivirus
- Authentication
- Proxy Servers
- IDS
- Firewall
- Email Security
- Cryptography
- PGP
- Digital Signatures
- Kerberos
- IPsec
- Web Security

Types of Attackers

- Attacker – Someone who can find an exploitable bug in a computer system.
- Cracker – An attacker who exploit a system illegally.
- Script kiddies – Uses tools available publicly.
- White hacker- People who discover vulnerabilities but does not exploit.
  - They help to fix it.
- Black hacker – Bad people who want to exploit systems after discovery.
- Cyber terrorists – Often have religious and fundamentalist mindset.
- Cyber army – State sponsored attackers.
  - Work for nation's strategic security.

Who Are Vulnerable to Attacks ?

- Financial institutions
- Defense organizations
- Government agencies
- Pharmaceutical companies
- IT companies
- Intellectual property management companies
- Academic institutions
- Everyone connected to internet

CIA Principles of Security

Information security is defined by an *acronym* CIA

- Confidentiality: Avoiding unauthorized disclosure of information.
- Integrity: *An* assurance that information is not altered midway of transmission.
- Availability: *An* assurance of information access and modification in a reasonable timeframe.

AAA Principles of Security

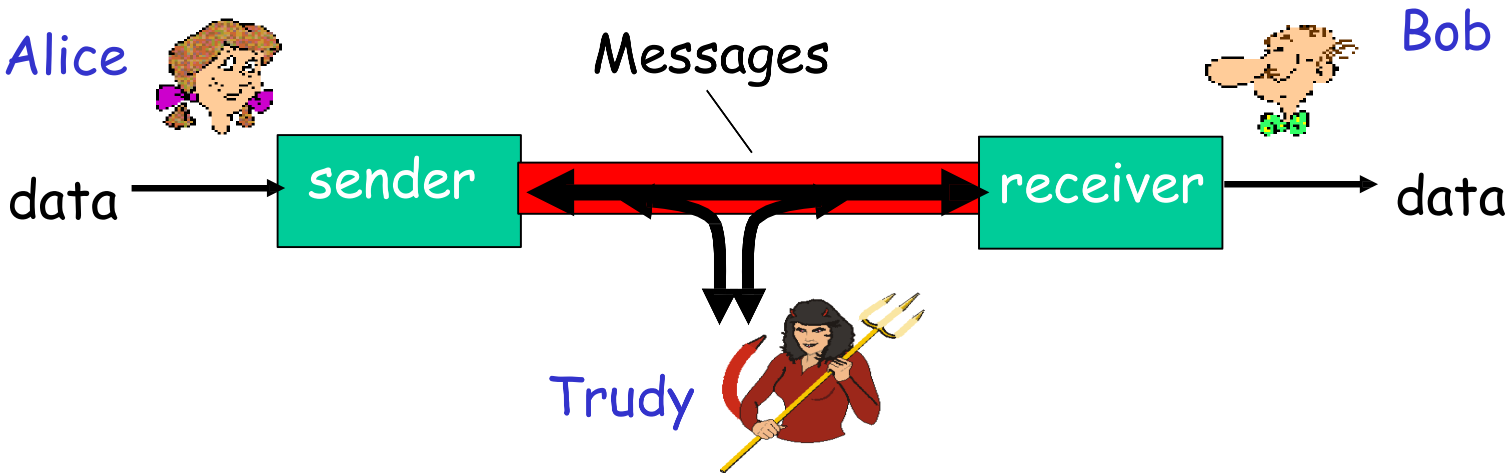
- AAA stand for Assurance, Authenticity and Anonymity
  - Assurance asks for guarantee.
  - Authenticity asks to tell you “who are you”.
  - Anonymity asks not to reveal identity.

Bob, Alice want to communicate "securely"

- Trudy is an enemy (intruder): "bad" guy

Q: what should Bob & Alice be concerned about?

- *eavesdrop:* messages are intercepted — confidentiality
- *change:* messages are modified — integrity
- *impersonation:* entire communication is hijacked by replacing sender or receiver by himself — authentication
- *denial of service*: prevent services (e.g., by overloading resources) — availability



Who might Bob, Alice be?

… well, *real-life* Bobs and Alices!

- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates

What is network security?

Goals of network security:

Confidentiality: Only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

Authentication: Sender and receiver want to confirm identity of each other.

Integrity: Sender and receiver want to ensure message not altered (in transit, or afterwards) without detection.

Availability: Services must be accessible and available to users.

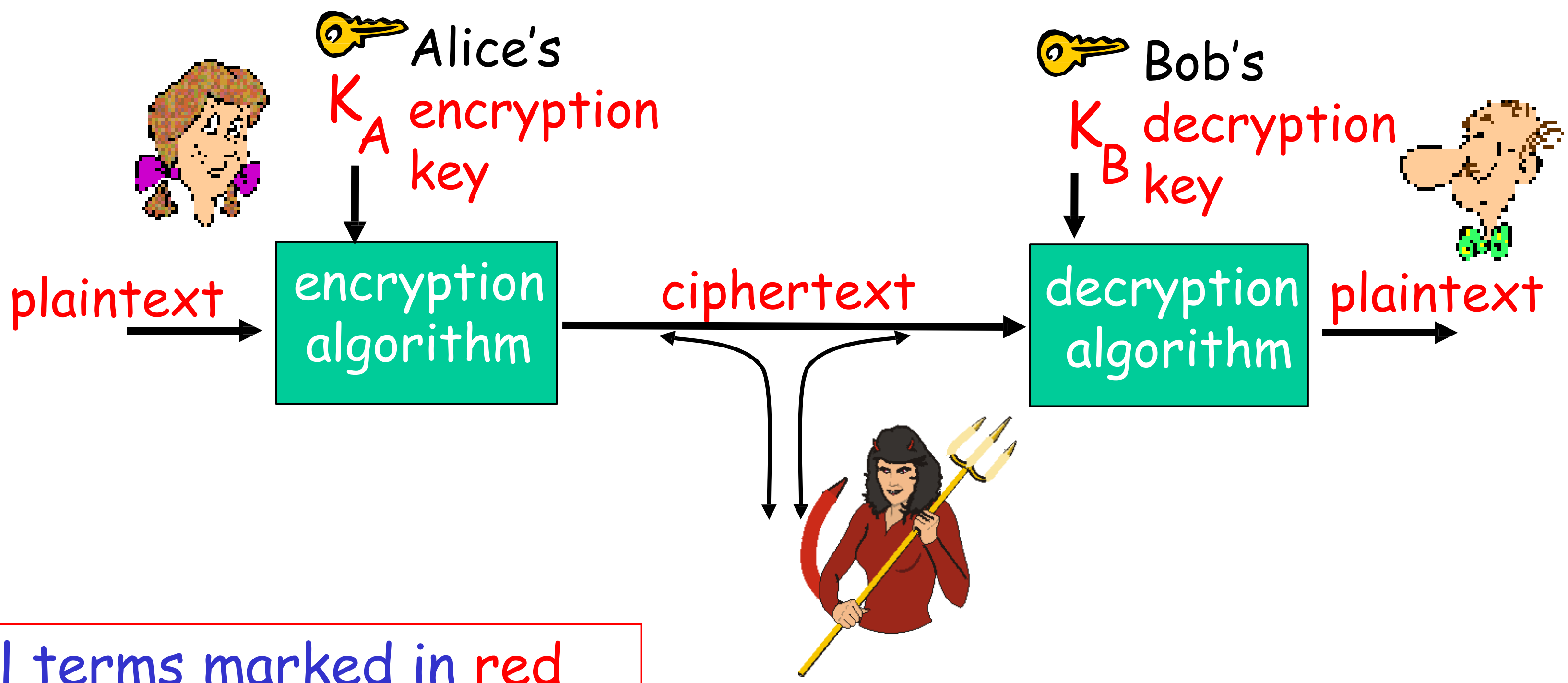
Roadmap

- Principles of cryptography
- Message integrity

Cryptography

- Cryptography allows a sender to disguise a message so that an intruder can't gain information from it.

"confidentiality"



All terms marked in red are crypto terminology

Types of cryptography

Symmetric key

- Both sender and receiver use *identical key*

e.g., Sender A encrypts with the key

Receiver B decrypts with same key

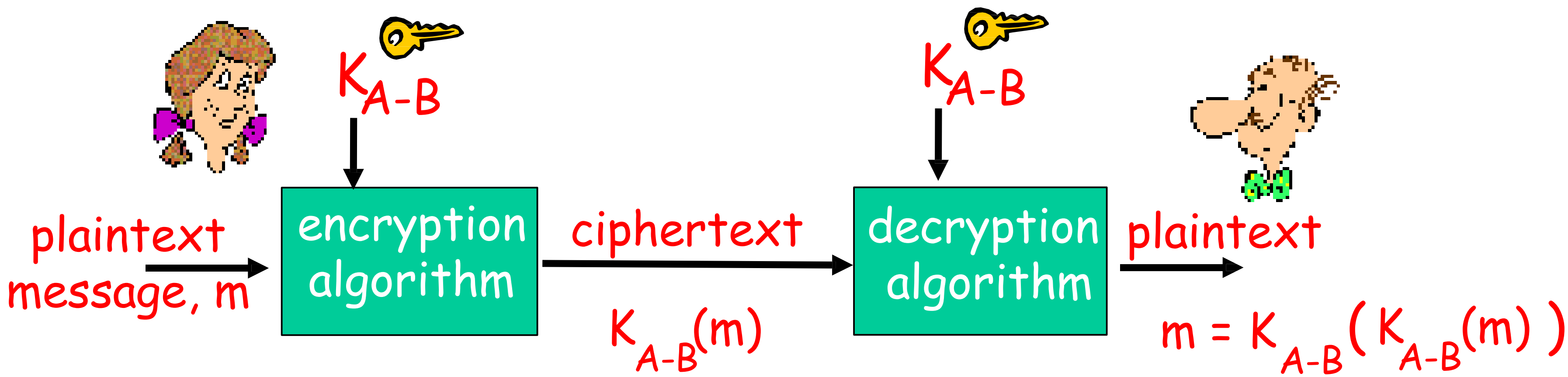
Public/private keys

- Two keys (public and private) are to be used

e.g., Sender A encrypts with B's public key

Receiver B decrypts with its Private key

Symmetric key cryptography



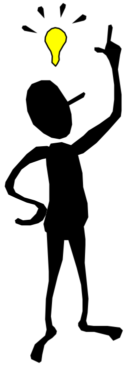
Symmetric key crypto: Bob and Alice share/know same (symmetric) key: K_{A-B}

- **Q:** How do Bob and Alice agree on key value?

Public key cryptography

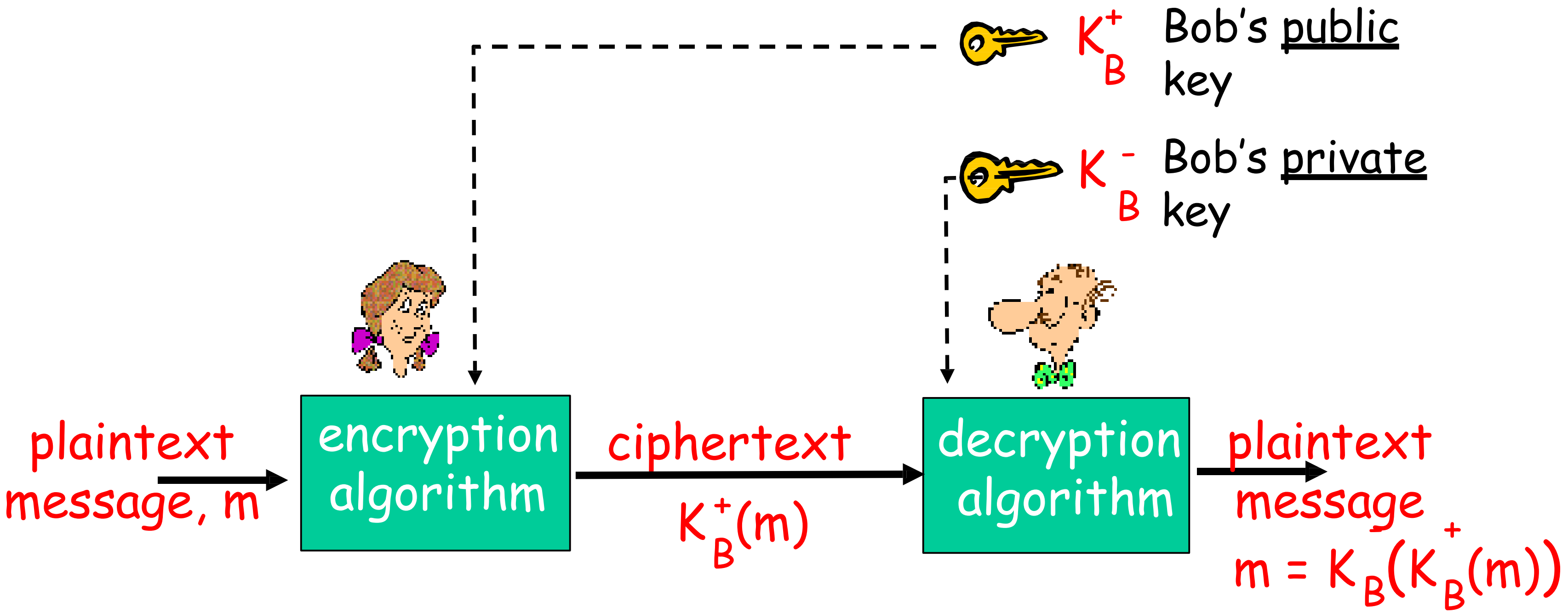
Symmetric key crypto

- Requires sender, receiver know shared secret key
- Q: How to agree on key in first place (particularly if never "met")?



- *Public key cryptography*
- Radically different approach
- Two keys
  - *Public key:* encryp. key
    - known to *all*
  - *Private key:* decryp. key known only to receiver
- Sender uses public key only to encryp
- Reciever uses both keys to decryp.

Public key cryptography



- Note: Only Bob is able to understand (decrypt) message m. Because only Bob has Bob's private key.
- This assures "confidentiality".

Public key encryption algorithms

Requirements:

1 Need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

2 Given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adleman algorithm

Roadmap

- Principles of cryptography
- Message integrity

Message Integrity/Authentication

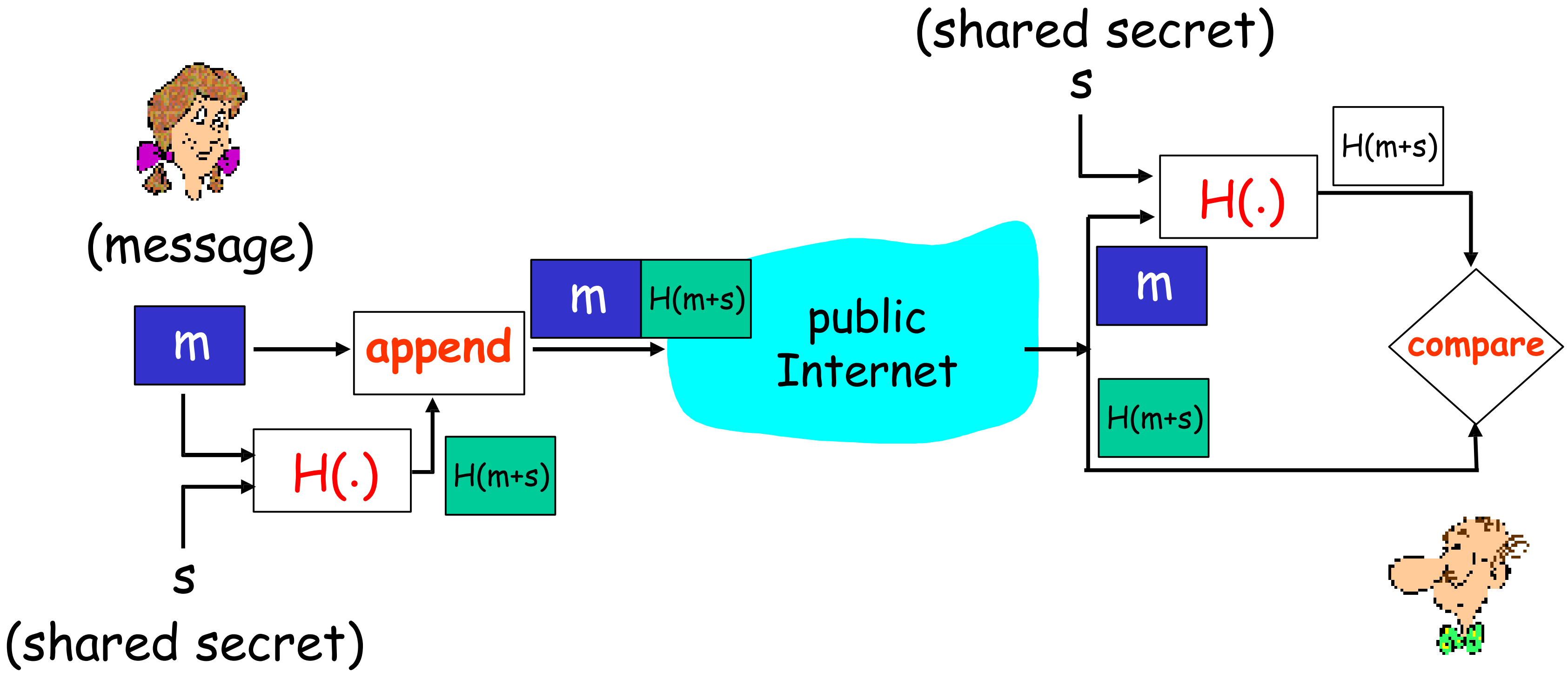
Bob receives msg from Alice, wants to ensure:

- Authentication: message originally came from Alice
- Integrity: message not changed since sent by Alice

Cryptographic Hashing:

- What:
  - Takes input m and produces fixed length value H(m).
    e.g., as in Internet checksum
- Properties of H:
  - Given m = H(x), (x unknown), it is computationally infeasible to determine x.
  - Difficult to find x and y such that H(x) = H(y)
  - Note: Internet checksum *fails* this requirement!
- Examples
  - Widely used hash functions: MD5, SHA

MAC: Message Authentication Code



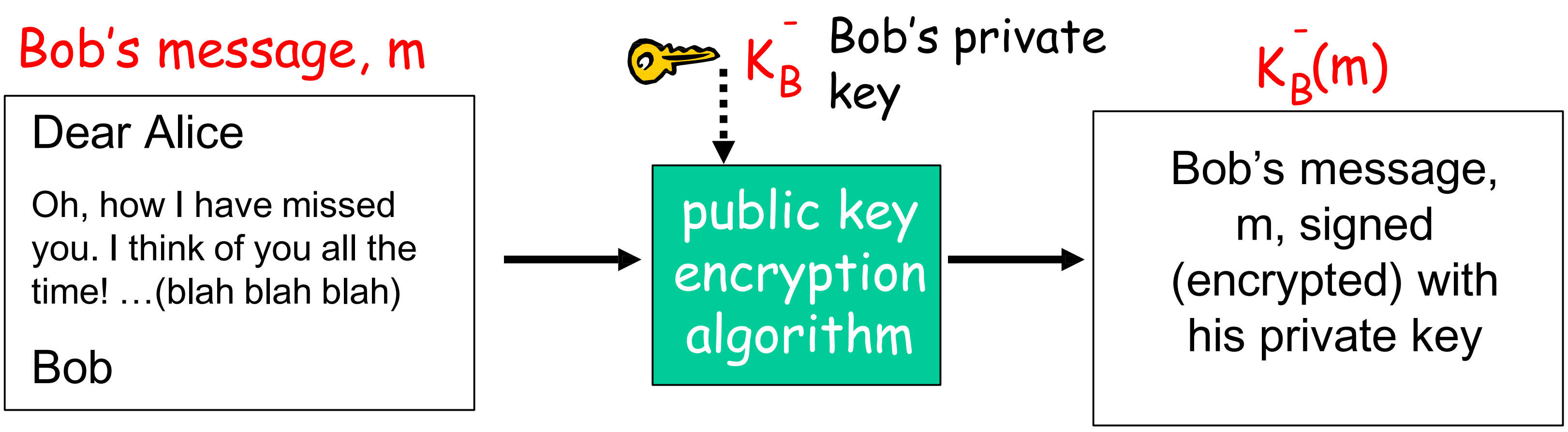
- Does MAC solve
  - Integrity ?? How ??
    via Hashing
  - Authentication ?? How ??
    via secret key

- Any problem ??
  - Secret key distribution ??
- So we can't really authenticate via MAC alone.

Digital Signatures via Public Key Crypto

Simple digital signature for message m:

- Bob "signs" m by encrypting with his private key K_B^-, creating "signed" message, $K_B^-(m)$



Digital Signatures via Public Key Crypto (more)

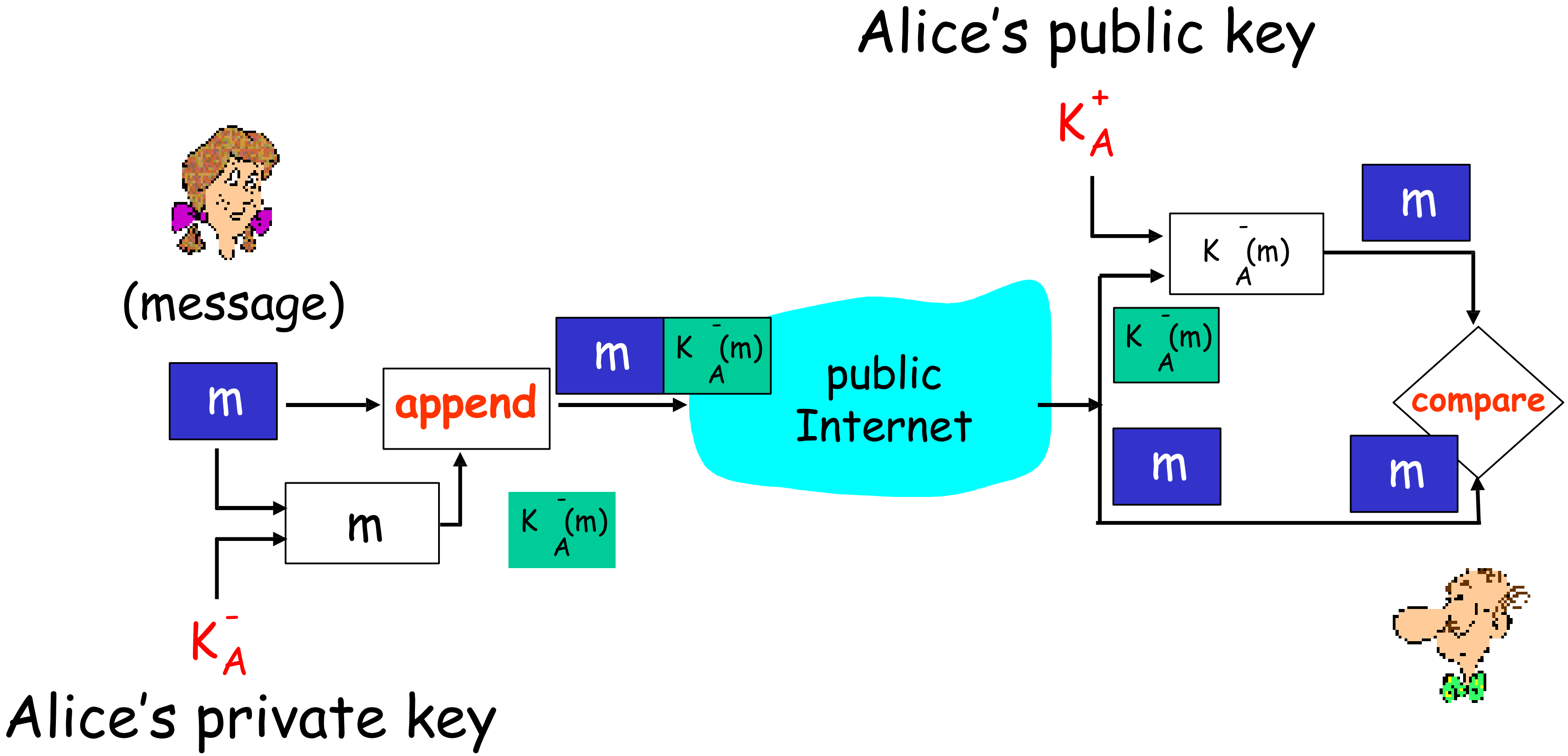
- Suppose Alice receives msg m, digital signature $K_B^-(m)$
- Alice verifies m signed by Bob by applying Bob's public key K_B^+ to $K_B^-(m)$ then checks $K_B^+(K_B^-(m)) = m$.
- if $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob's private key.

Alice thus verifies that:

- ✓ Bob signed m.
- ✓ No one else signed m.
- ✓ Bob signed m and not m'.

-

MAC via private/public keys



- Note: Only Alice would have had her private key
- This assures "authentication".

Digital Signatures via Public Key Crypto (more)

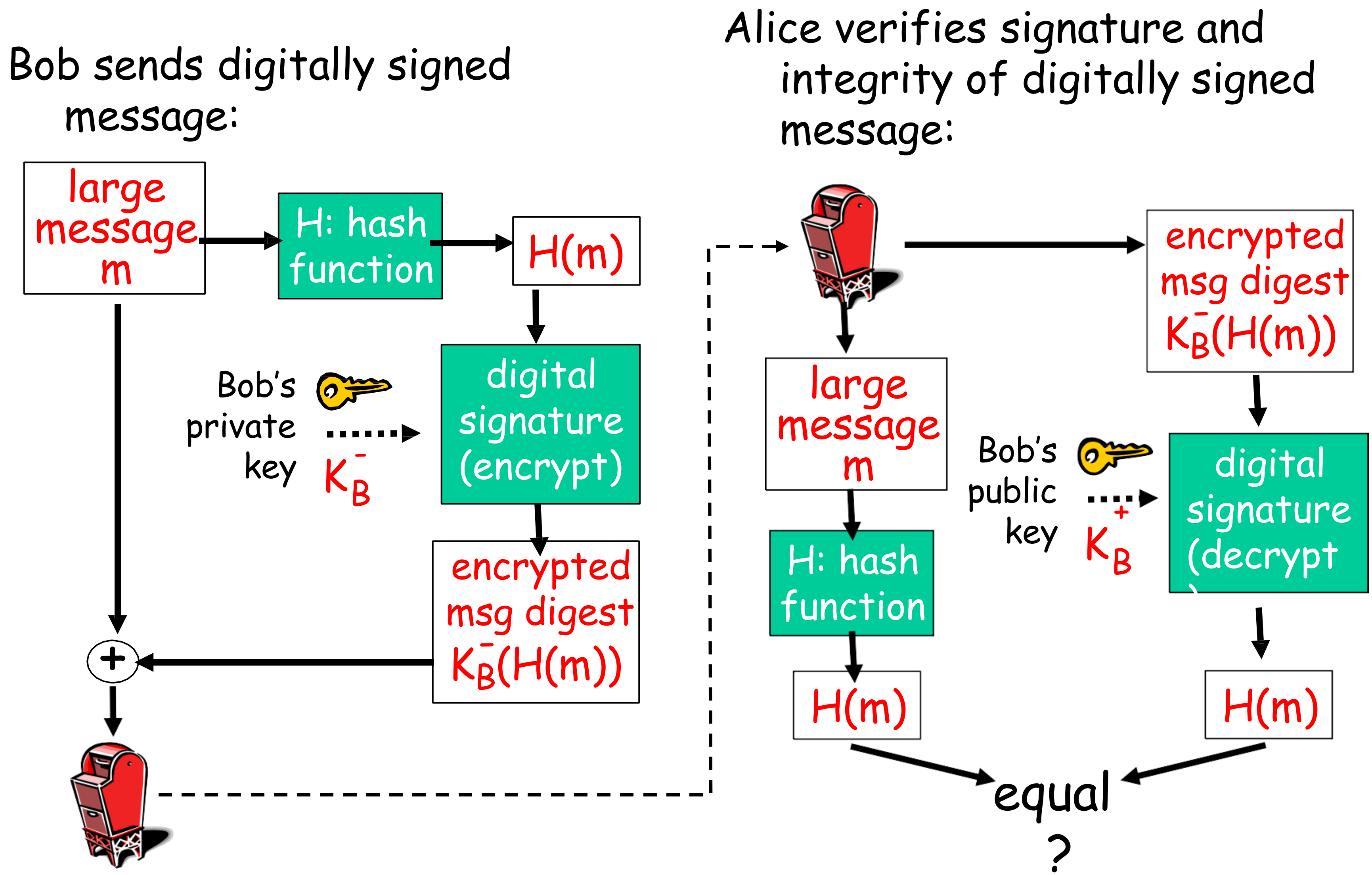
Problem

- Signing data by encryption and decryption is computationally expensive.
- Imagine encrypting (signing) huge files of data !!!

Solution

- Sign hashed output of original msg (sign H(m) only).
- Recall hash algorithms turn large msgs into small, fixed length msg.
- … signed MAC is the solution

Digital signature = signed MAC
= authentication + integrity



Public Key Certification

- Problem with public key:
  - When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she *know* it is Bob's public key, not Trudy's?
- Solution:
  - Trusted certification authority (CA)

Recap

So far:

- Cryptography & confidentiality
  - Symmetric key
  - Public key: A wants to send msg m to B. What does A send?

    A sends $K_B^+(m)$; hence, ONLY B understands m by applying $K_B^-(K_B^+(m))$

    => confidentiality

Note: Sender applies receiver's public key

- Authentication & integrity
  - MAC (Msg Authen. Code): requires symmetric key
  - Signed MAC: A -> B

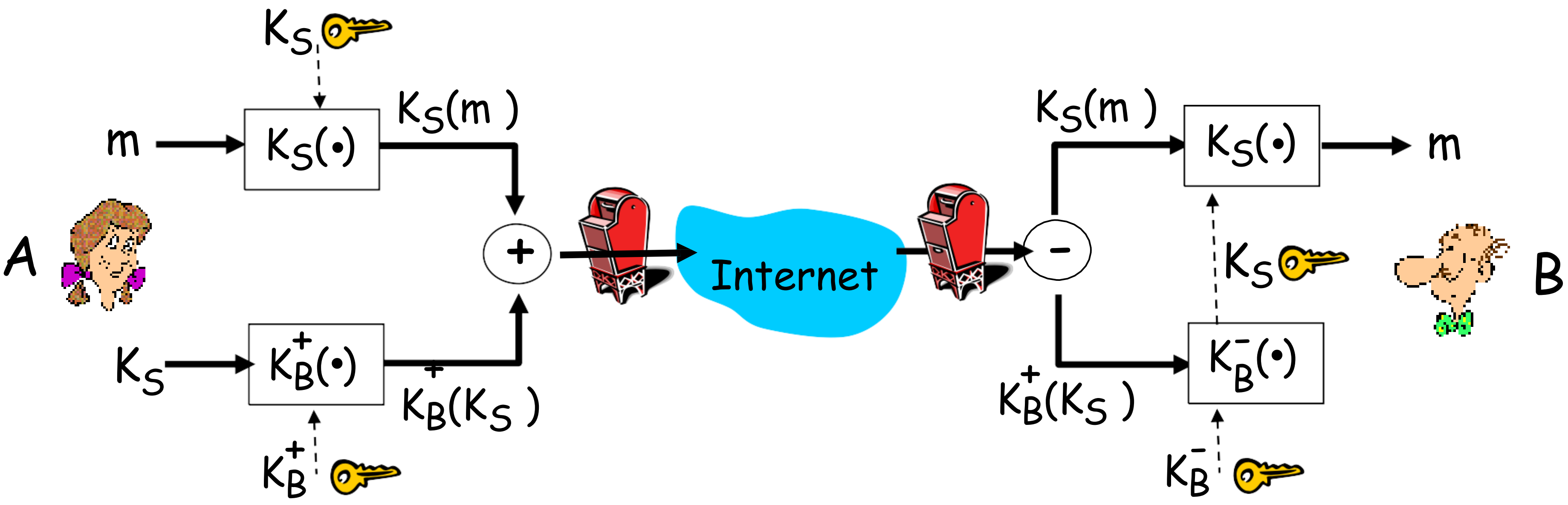
    A sends $(m, K_A^-(m))$ to B,
    Hence, All get m by applying $K_A^+(K_A^-(m))$;

    Comparison => authen. + integrity, but NOT confidentiality

Note: Sender applies its private key

Secure e-mail (confidentiality)

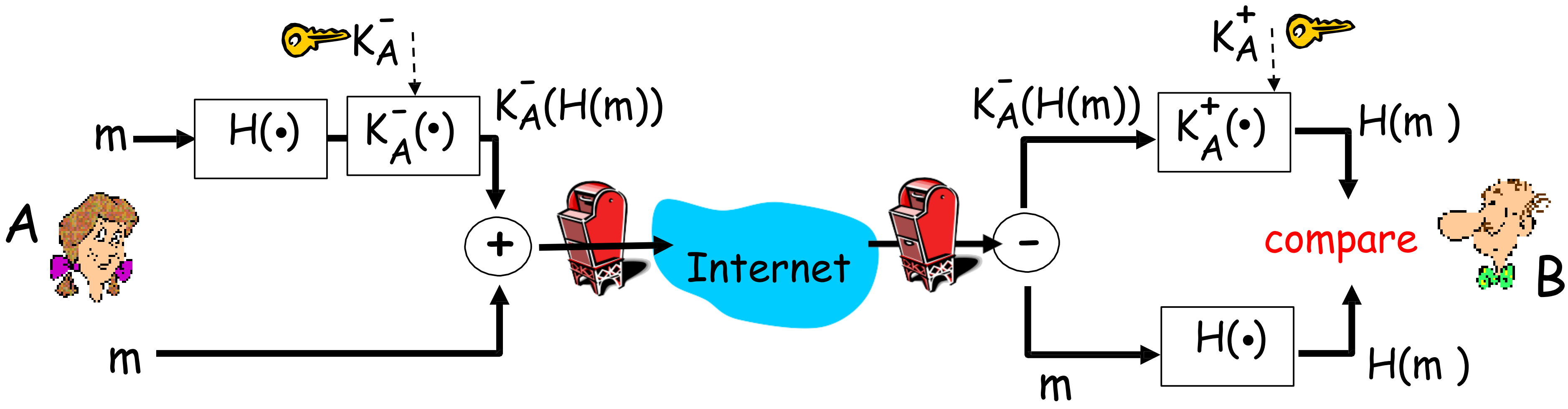
- Alice wants to send confidential e-mail, m, to Bob.



Alice generates random *symmetric* private key, K_S.

Secure e-mail (authen. + integrity)

- Alice wants to provide sender authentication/integrity.

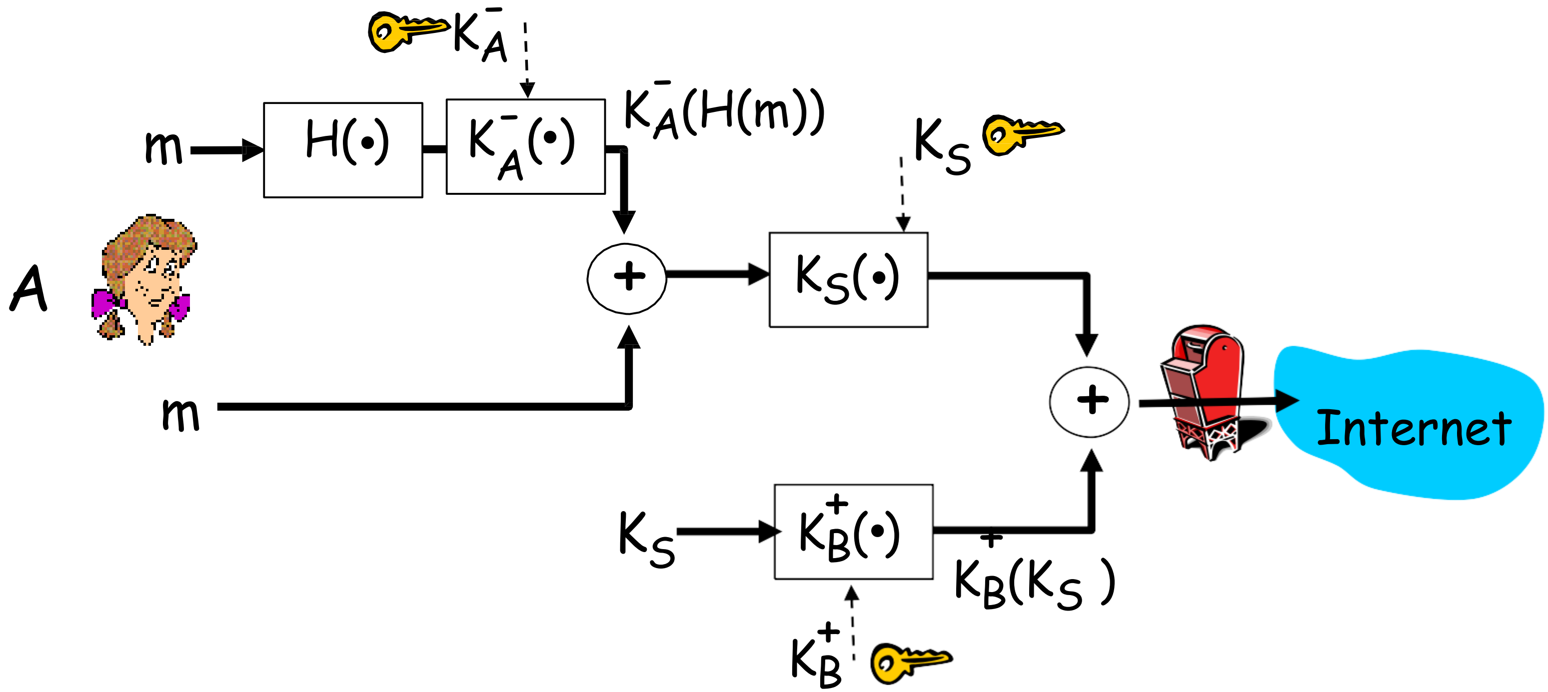


- Alice digitally signs message.
- sends both message (in the clear) and digital signature.

Again note that to provide authenticate/integrity, sender encrypts with its <u>private</u> (all can understand msg)

Secure e-mail (all: confid. + auth. + integrity)

- Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, and newly created symmetric key.

The end of class!