Computer Network

Ch8. Network Security

17011599 / Ahn Jeong Yeon

17011588 / Noh Ha Yoon

1.What is network security?

Confidentiality

only sender, intended receiver should “understand” message contents

Authentication

sender, receiver want to confirm identity of each other

Message Intergrity

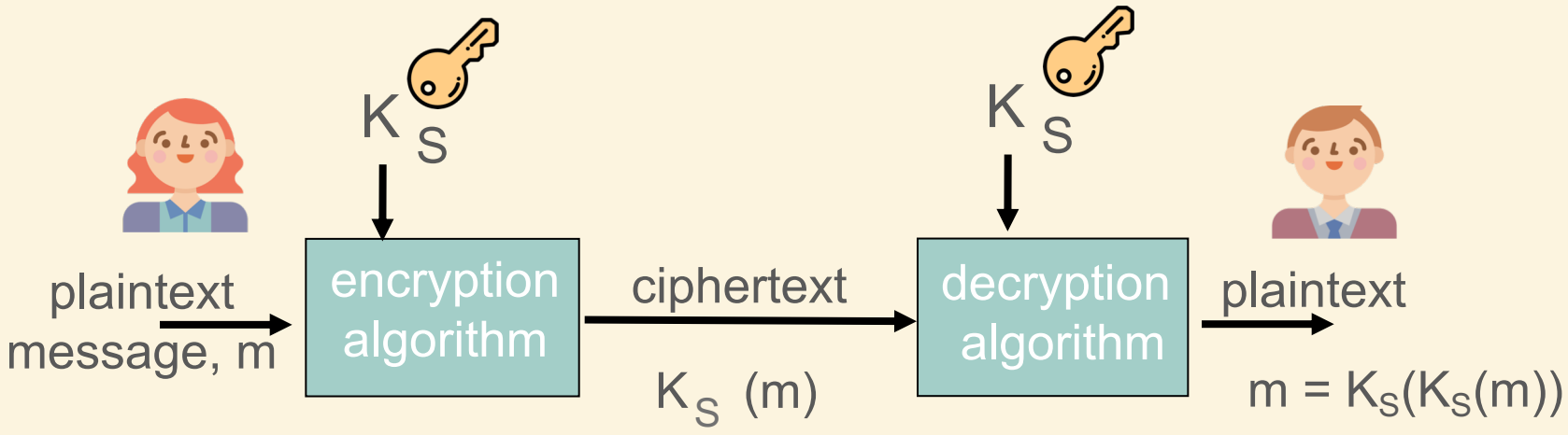
sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and Availability

services must be accessible and available to users

2. Principle of cryptography

Symmetric key cryptography

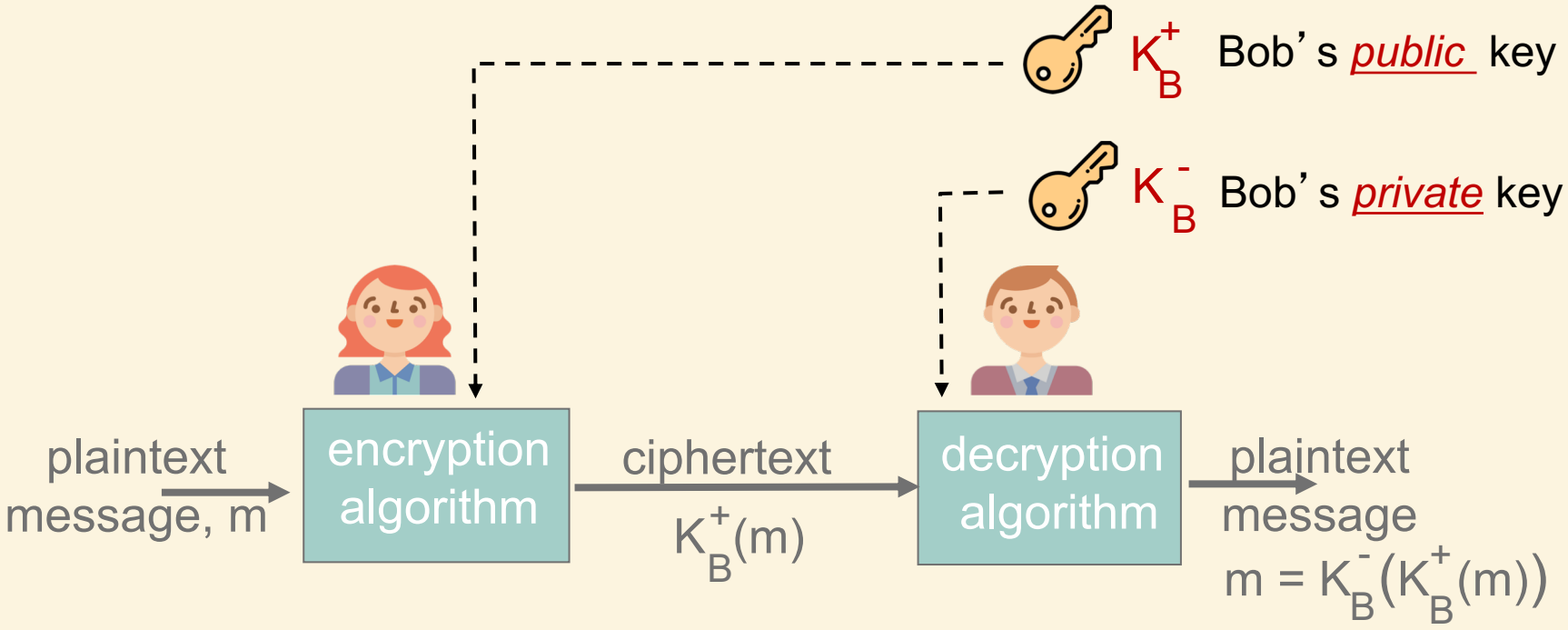


symmetric key crypto: Bob and Alice share same (symmetric) key: K_S

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

2. Principle of cryptography

Public key cryptography



- sender, receiver do not share secret key
- public encryption key known to all
- private decryption key known only to receiver

3. Message integrity, authentication

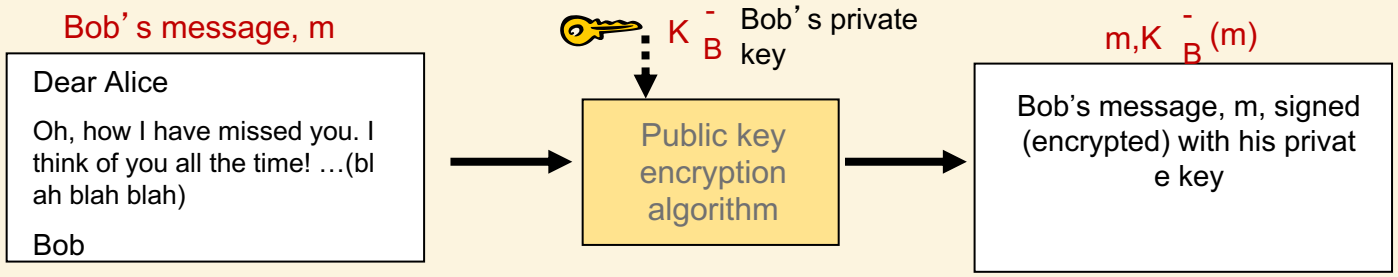
Digital signiture

cryptographic technique analogous to hand-written signatures:

- sender(Bob) digitally signs document, establishing he is document owner/creator.
- verifiable, nonforgeable: recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document

simple digital signature for message m:

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



3. Message integrity, authentication

Authentication

Protocol ap1.0

Alice says “I am Alice”

Protocol ap2.0

Alice says “I am Alice” in an IP packet containing her source IP address

Protocol ap3.0

Alice says “I am Alice” and sends her secret password to “prove” it.

Protocol ap4.0

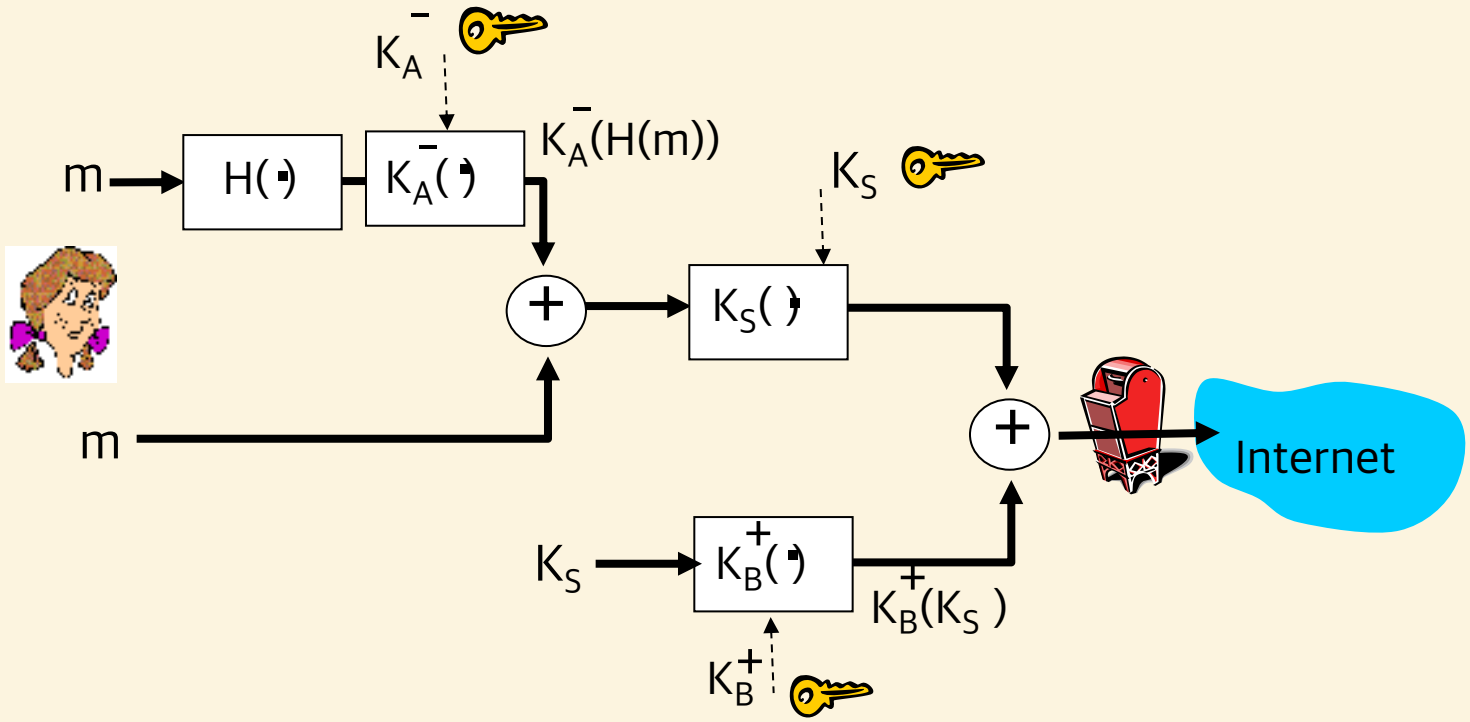
to prove Alice “live”, Bob sends Alice *nonce*, R.
Alice must return R, encrypted with shared secret key

Protocol ap5.0

use nonce, public key cryptography

4. Securing e-mail

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



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

5. Securing TCP connections: SSL

SSL: Secure Sockets Layer

widely deployed security protocol

- supported by almost all browsers, web servers
- https
- billions $/year over SSL

mechanisms: [Woo 1994],

implementation: Netscape

variation -TLS:

transport layer security, RFC 2246

provides

- confidentiality
- integrity
- authentication

Original goals:

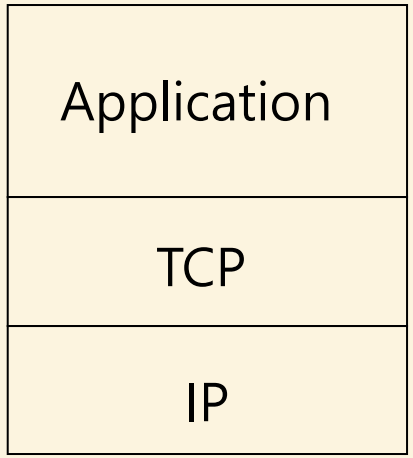
- Web e-commerce transactions
- encryption (especially credit-card numbers)
- Web-server authentication
- optional client authentication
- minimum hassle in doing business with new merchant

available to all TCP applications

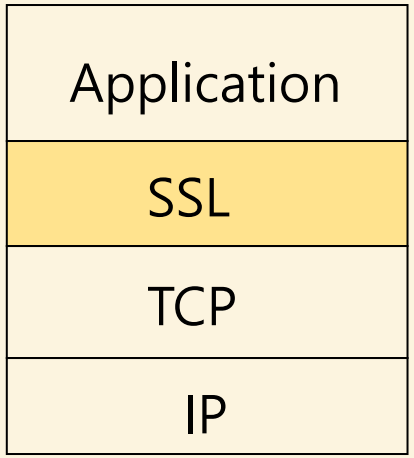
secure socket interface

5. Securing TCP connections: SSL

SSL and TCP/IP



normal application



application with SSL

- SSL provides application programming interface (API) to applications
- C and Java SSL libraries/classes readily available

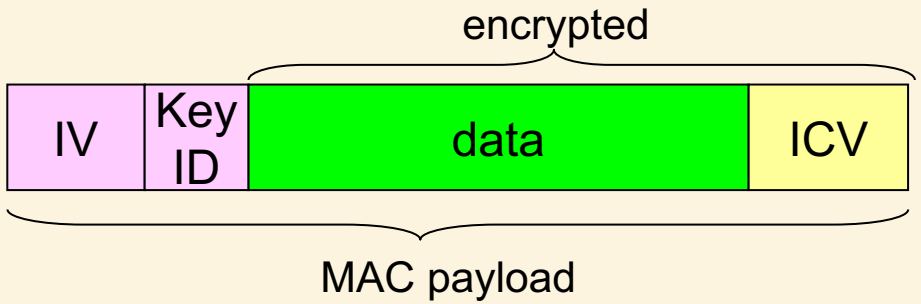
6. Network layer security: IPsec

IPsec

- IKE message exchange for algorithms, secret keys, SPI numbers
- either AH or ESP protocol (or both)
  - AH provides integrity, source authentication
  - ESP protocol (with AH) additionally provides encryption
- IPsec peers can be two end systems, two routers/firewalls, or a router/firewall and an end system

7. Securing wireless LANs

WEP



encryption

- sender calculates Integrity Check Value (ICV, four-byte hash/CRC over data
- each side has 104-bit shared key
- sender creates 24-bit initialization vector (IV), appends to key: gives 128-bit key
- sender also appends keyID (in 8-bit field)
- 128-bit key inputted into pseudo random number generator to get keystream
- data in frame + ICV is encrypted with RC4

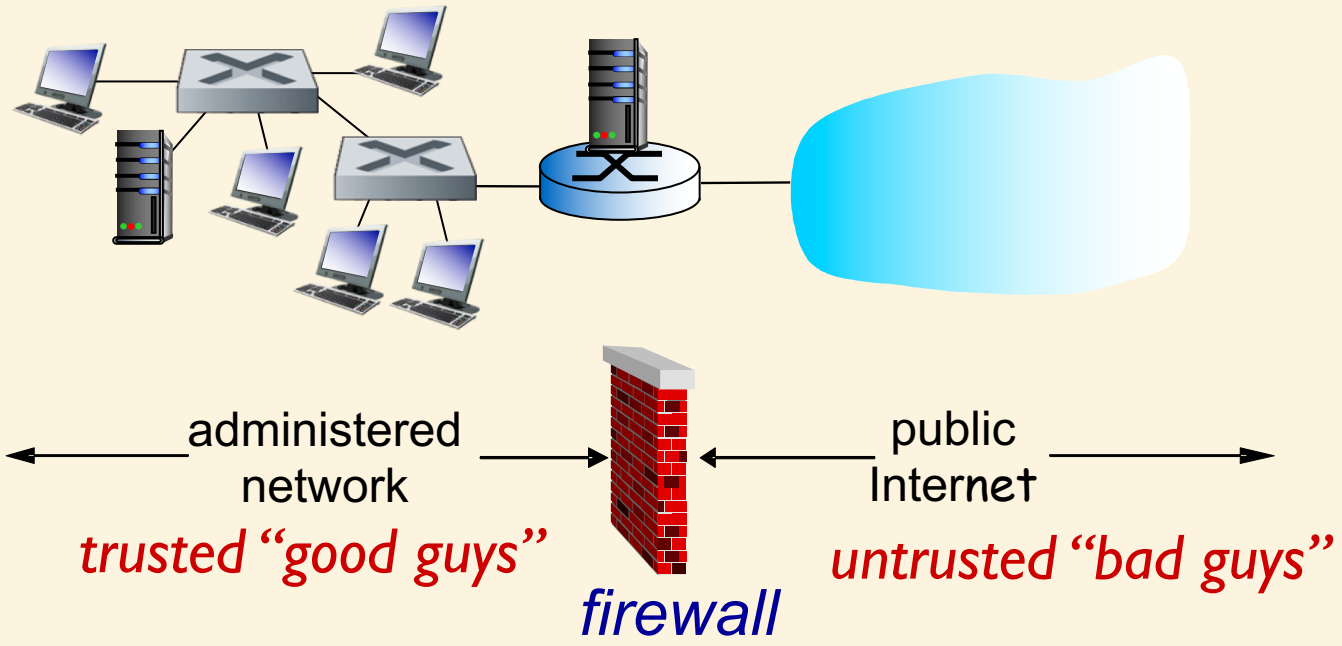
decryption

- receiver extracts IV
- inputs IV, shared secret key into pseudo random generator, gets keystream
- XORs keystream with encrypted data to decrypt data + ICV
- verifies integrity of data with ICV

8. Operational security: firewalls and IDS

Firewalls

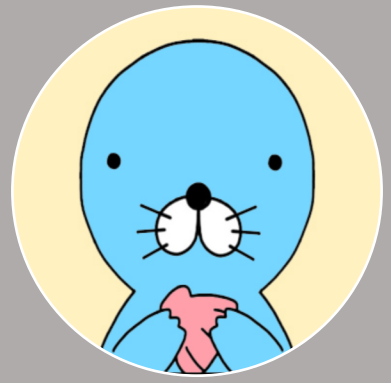
isolates organization’s internal net from larger Internet, allo wing some packets to pass, blocking others



8. Operational security: firewalls and IDS

IDS: intrusion detection system

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- IDS: intrusion detection system
  - deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack



THANK YOU