Computer networks 503442-3

Assignments:network security

Question 1: Complete the following sentences

1) **confidentiality** *means that* only sender, intended receiver should "understand" message contents

2) **authentication** *means that* sender, receiver want to confirm identity of each other

3) **message integrity** *means that* sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

4) **access and availability** *means that* services must be accessible and available to users

5) **firewall** isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others

6) **stateful** *packet filter:* track status of every TCP connection

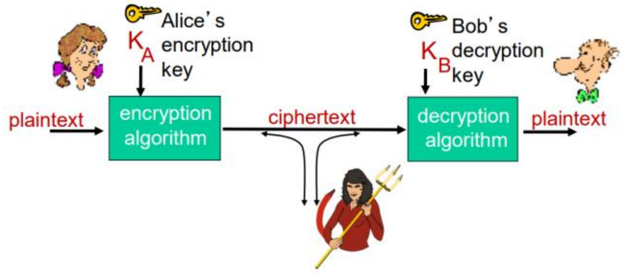
7) **deep packet inspection** look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)

8) *Question 2: answer the following questions*

1) What can a "bad guy" do?

- eavesdrop: intercept messages
- actively insert messages into connection
- impersonation: can fake (spoof) source address in packet (or any field in packet)
- hijacking: "take over" ongoing connection by removing sender or receiver, inserting himself in place
- denial of service: prevent service from being used by others

2) Briefly explain with the aid of drawing the principles of cryptography.



m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

3) What is the main difference between symmetric key cryptography and public key cryptography?

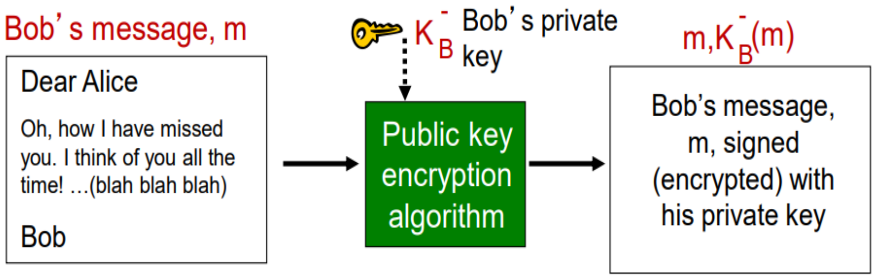
- **symmetric key crypto**

  requires sender, receiver know shared secret key

- **public key crypto**

  sender, receiver do not share secret key

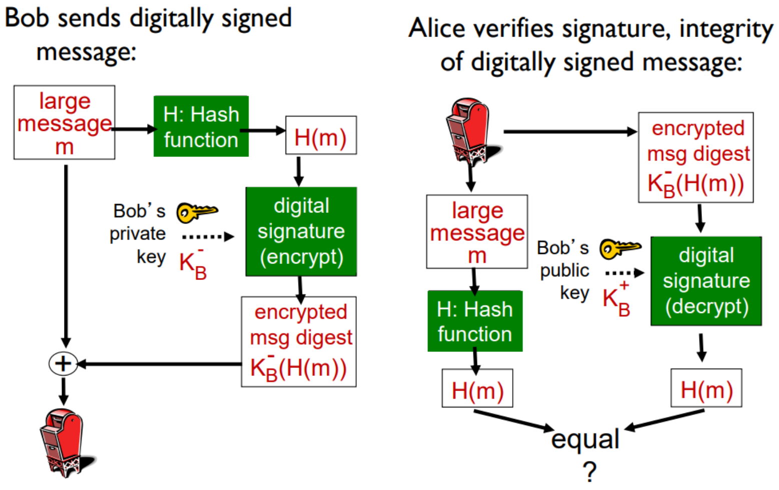
4) Briefly explain with the aid of drawing the principles of Digital signatures using public key cryptography


Bob's message, m
Dear Alice
Oh, how I have missed you. I think of you all the time! …(blah blah blah)
Bob
K_B^- Bob's private key
Public key encryption algorithm
$m,K_B^-(m)$
Bob's message, m, signed (encrypted) with his private key

5) What are the goals of Message digests?

- **fixed-length, easy- to compute digital "fingerprint"**

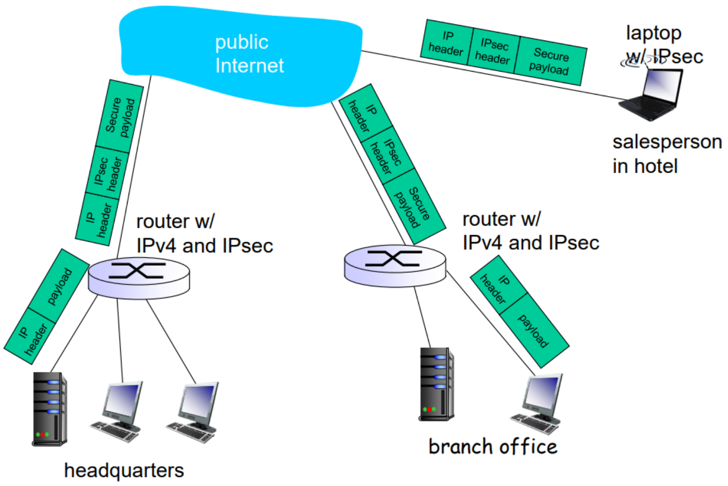
6) Briefly explain with the aid of drawing the principles of Digital signatures using public key cryptography and Message digests.



7) What are the original goals of Secure Sockets Layer)SSL(?

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

8) Describe with the aid of drawing the principles of Virtual Private Networks (VPNs)



9) What are the objectives of Firewalls?

❖ stateless packet filters ❖ stateful packet filters ❖ application gateways

10) What is the basis of the packet forwarding/dropping in stateless packet filtering in firewalls?

▪ source IP address, destination IP address

▪ TCP/UDP source and destination port numbers

▪ ICMP message type ▪ TCP SYN and ACK bits

11) Briefly explain the Stateful packet filtering in firewalls

▪ track status of every TCP connection

▪ track connection setup (SYN), teardown (FIN): determine whether incoming, outgoing packets "makes sense"

▪ timeout inactive connections at firewall: no longer admit packets

12) What are the functions of intrusion detection system (IDS)?

▪ 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

Best Wishes Prof. Mohammed Abd-Elnaby