“Access Denied….”: Encryption and Security

Part C of Seminar on Current Issues and Technologies for the Internet

Dr. Junaid Ahmed Zubairi

Visiting Associate Professor

CIT, Agriculture University, Rawalpindi

August17th, 2002 6:30PM

Seminar Outline

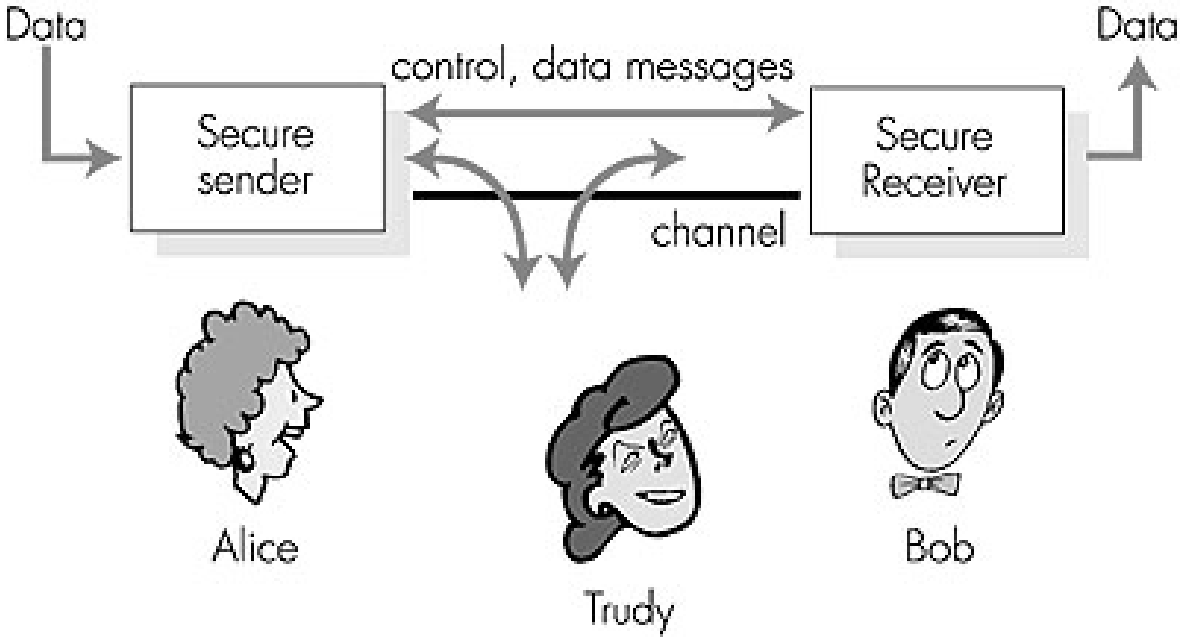
Foundations:

- what is security?
- cryptography
- authentication
- message integrity

Security in practice:

- application layer: secure e-mail
- transport layer: Internet commerce, SSL,
- Reference: Computer Networking by James F. Kurose and Keith W. Ross, 1st Edition, Addison Wesley 2001

Friends and enemies: Alice, Bob, Trudy



- well-known in network security world
- Bob, Alice want to communicate “securely”
- Trudy, the “intruder” may intercept, delete, add messages

Who are Bob and Alice?

- Maybe they are two routers that wish to securely exchange routing tables
- Or two computers that wish to establish a secure transport connection
- Or two email applications trying to exchange secure email
- Or an e-commerce client communicating with a vendor

What is network security?

Secrecy: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

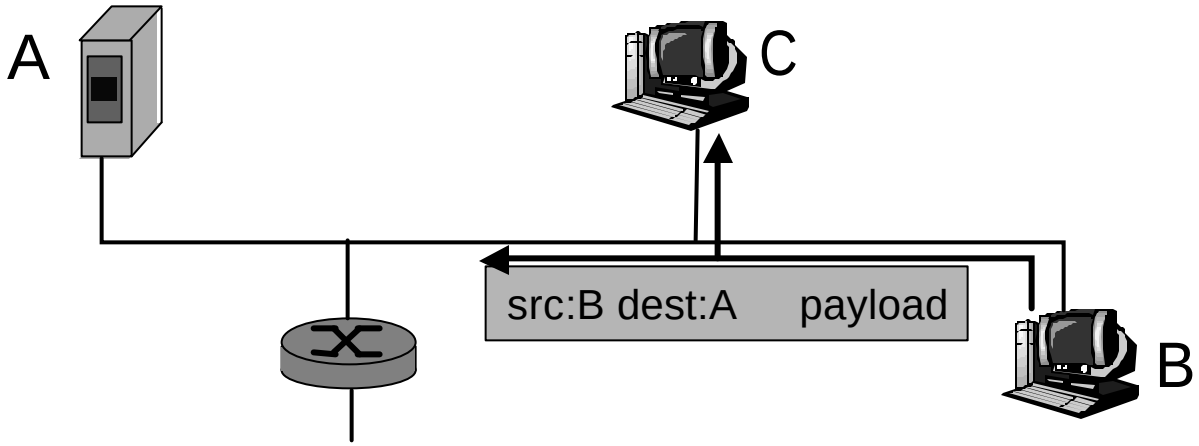
Authentication: sender, receiver want to confirm identity of each other

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

Internet security threats

Packet sniffing:

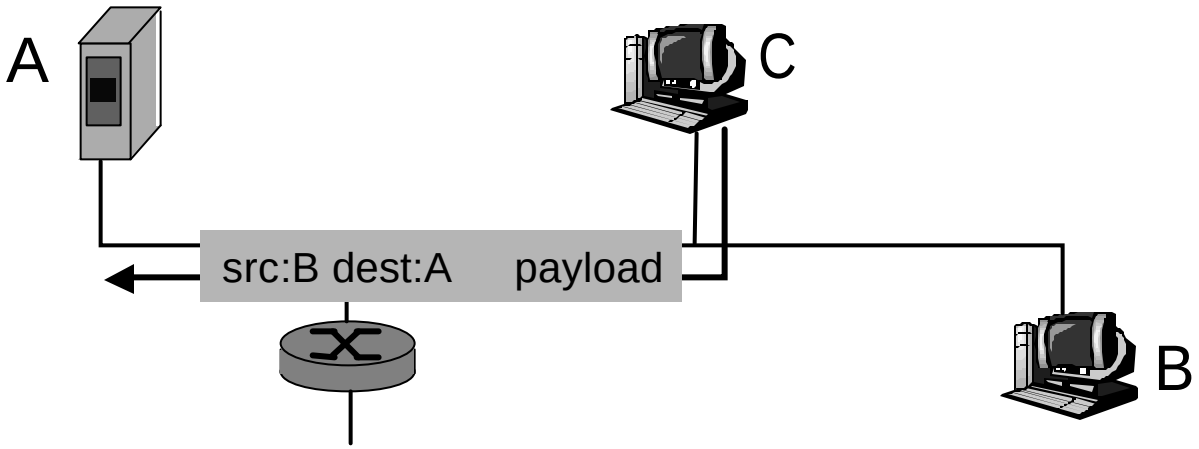
- broadcast media
- promiscuous NIC reads all packets passing by
- can read all unencrypted data (e.g. passwords)
- e.g.: C sniffs B's packets



Internet security threats

IP Spoofing:

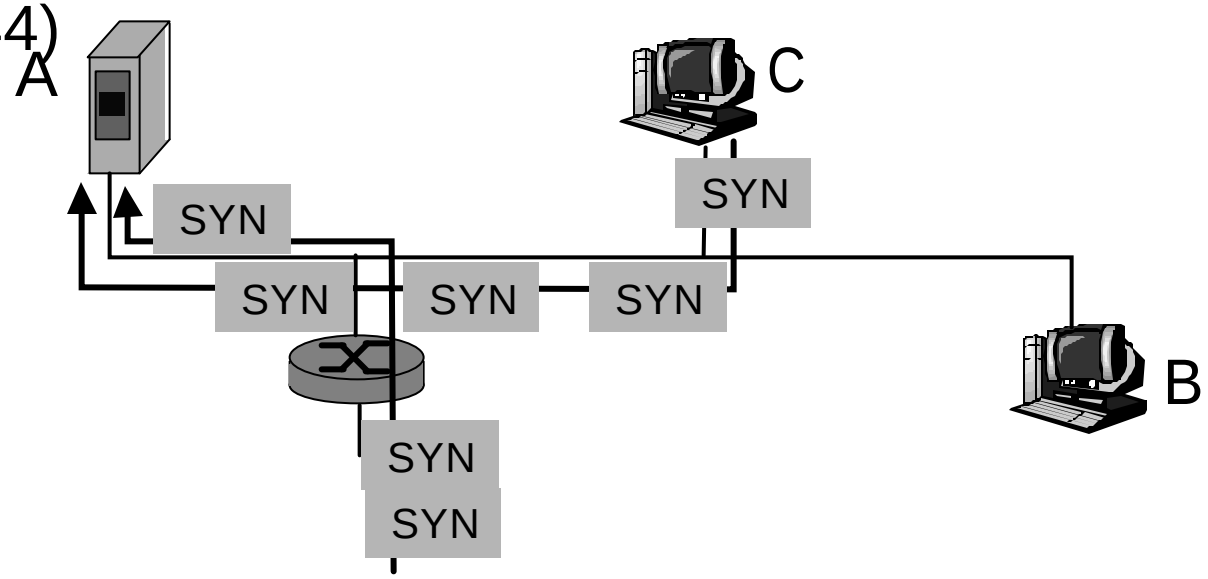
- can generate “raw” IP packets directly from application, putting any value into IP source address field
- receiver can’t tell if source is spoofed
- e.g.: C pretends to be B



Internet security threats

Denial of service (DOS):

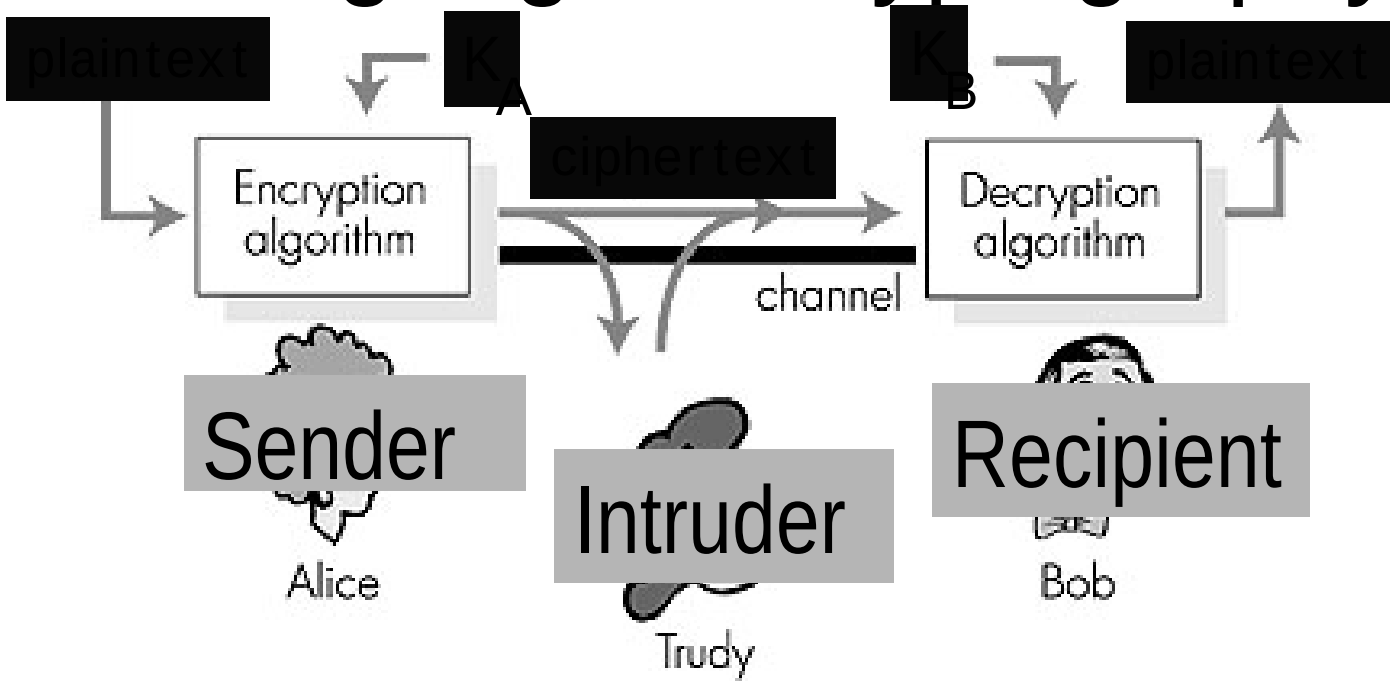
- flood of maliciously generated packets “swamp” receiver
- Distributed DOS (DDOS): multiple coordinated sources swamp receiver
- e.g., C and remote host SYN-attack A; A rendered unusable by genuine users (solution: RFC2267 & 2644)



Encryption and Data Security

- For ensuring secrecy, we must ensure that the sensitive data has been encrypted and secured
- Encryption transforms the data using a “key” into a value that is meaningless in its normal form
- This encrypted value can only be decrypted by authorized agency and/or intended person

The language of cryptography



symmetric key crypto: sender, receiver keys identical ($K_A = K_B$)

public-key crypto: encrypt key *public*, decrypt key *secret*

Symmetric key cryptography

substitution cipher: substituting one thing for another e.g. monoalphabetic cipher: substitute one letter for another

E.g.: **Plaintext: bob. Transfer money now**

ciphertext: nkn uomjikco hkjvw jkr

Q: How hard to break this simple cipher?:

- brute force (how hard?) well known frequencies
- other? Vigenere polyalphabetic with mutliple keys

Symmetric Key Cryptography

- In modern symmetric key schemes, XOR is the fundamental logical operation involved in encrypting a message
- For example, consider a byte to be sent out: It is 1011 0111 (Decimal 183)
- We select a secret 4-bit key 1100 and perform XOR of this key with the original data
- 1011 0111
- 1100 1100
- ----------
- 0111 1011(Decimal 123)

Symmetric Key Cryptography

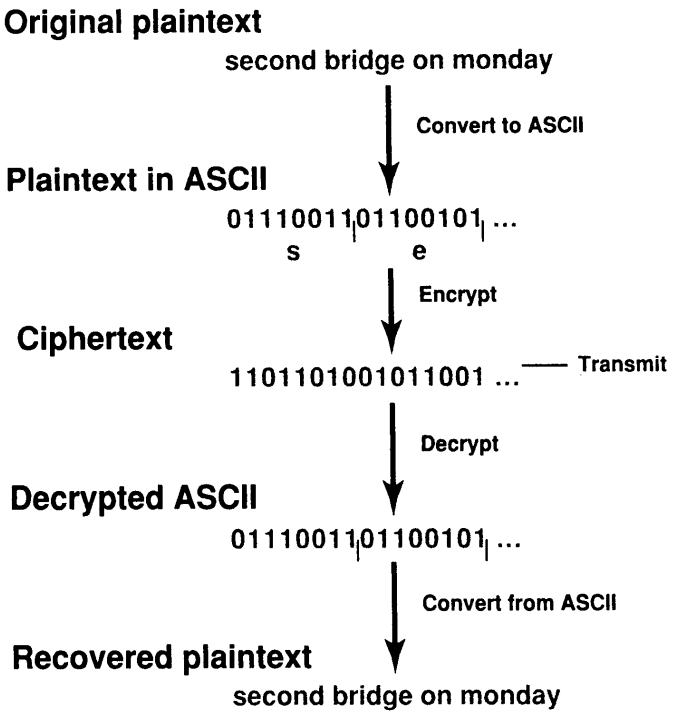
- Now the recipient receives this message and decrypts it by using the same key with XOR operation
- received data is 0111 1011
- The key is 1100
- 0111 1011
- 1100 1100
- ----------
- 1011 0111 (original data)
- Key delivery problem??

Another Example

- As an example of using encryption for plaintext messages, consider this diagram

Symmetric Cipher

FIGURE 16.12
The figure shows the process of converting a plaintext message to an ASCII string, which can be interpreted as a numeric value. Encryption keys are then used to covert this value to another number representing the ciphertext. The message receiver uses decryption keys to convert the received value back to the original number and the decodes this as an ASCII string.



Adapted for academic use from “Exploring The Digital Domain” by Abernethy Allen, ITP 1999

Symmetric Cipher

- In symmetric secret key cipher, the key must be sent to recipient, otherwise the message cannot be decrypted
- Sending the key on public network is like putting your house key in locksmith’s shop and allowing everyone to duplicate it
- KDC (Key distribution center) can securely send a one time symmetric key to two registered users who wish to communicate

Symmetric key crypto: DES

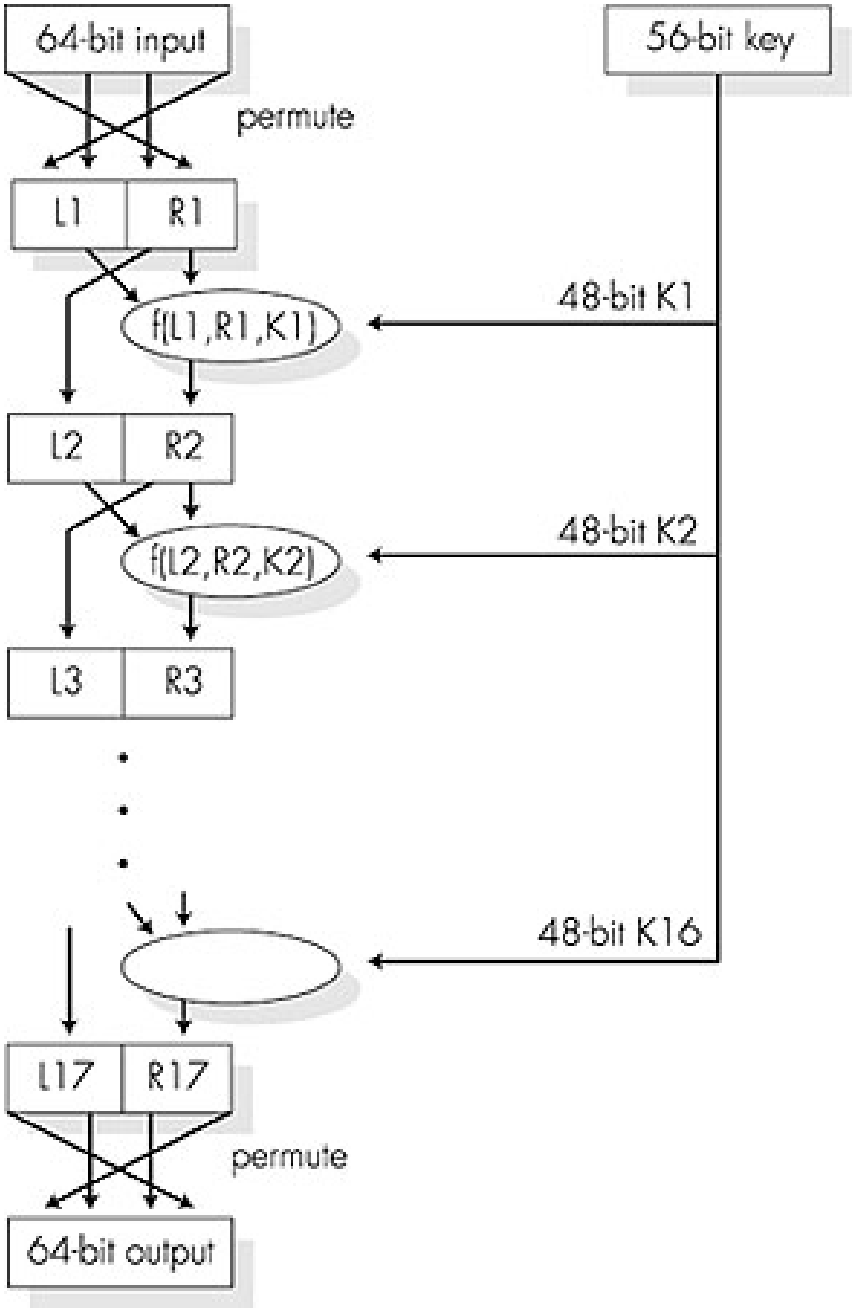
DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64 bit plaintext input
- How secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase (“Strong cryptography makes the world a safer place”) decrypted (brute force) in 4 months
  - no known “backdoor” decryption approach
- making DES more secure
  - use three keys sequentially (3-DES) on each datum
  - use cipher-block chaining to prevent data intrusion

Symmetric key crypto: DES

DES operation

- initial permutation
- 16 identical "rounds" of function application, each using different 48 bits of key
- final permutation



Asymmetric or Public Keys

- Asymmetric keys solve the key distribution problem
- The RSA algorithm works as follows:
  - Sender gets the public key of recipient (available to everyone)and uses it to encrypt the message
  - Receiver uses private key (only known to receiver) to decrypt the message

Asymmetric Keys

- In some apartment complexes, the laundry room is locked
- Every tenant gets a key to the laundry room. This is like a “public” key
- If the management wants to enforce operating hours (for example, 8am to 10pm), they would install an additional lock
- The key of this lock is not duplicated. It stays with the management

Asymmetric Keys

- In a similar way, a site creates its own public and private key pair, related to each other in “strange” ways
- It lets everyone download the public key but it will keep the private key secret
- Suppose that John wants to buy something from www.crazybuyers.com
- John will go to the the above website and obtain their public key

Asymmetric Keys

- John will encrypt the message using the public key of Crazybuyers.
- The message will be transmitted over the Internet
- Anyone who gets this message and tries to open it using the public key of Crazybuyers will fail (why? Remember laundry room after 10pm?)

RSA: Choosing keys

1. Choose two large prime numbers *p, q.* (e.g., product 1024 bits long)

2. Compute $n = pq$, $z = (p-1)(q-1)$

3. Choose e (with $e<n$) that has no common factors with z. (e, z are "relatively prime").

4. Choose d such that $ed-1$ is exactly divisible by z. (in other words: $ed \bmod z = 1$).

5. *Public* key is (n,e). *Private* key is (n,d).

RSA: Encryption, decryption

0. Given (n,e) and (n,d) as computed above

1. To encrypt bit pattern, m, compute

   $c = m^e \bmod n$ (i.e., remainder when m^e is divided by n)

2. To decrypt received bit pattern, c, compute

   $m = c^d \bmod n$ (i.e., remainder when c^d is divided by n)

Bang $m = (m^e \bmod n)^d \bmod n$

Session Keys

- RSA is much slower than DES because it involves large number arithmetic
- Sometimes RSA can be combined with DES to accelerate data transfer
- Sender can generate a symmetric session key (DES key) and send it to recipient encrypted with RSA
- The actual data transfer takes place with DES encryption

Digital Signatures

- Authentication is a core issue in e-commerce
- Authentication is to verify the source of a document
- Authentication of paper documents is done with watermarks, stamps, signatures and seals
- How to authenticate the electronic documents?

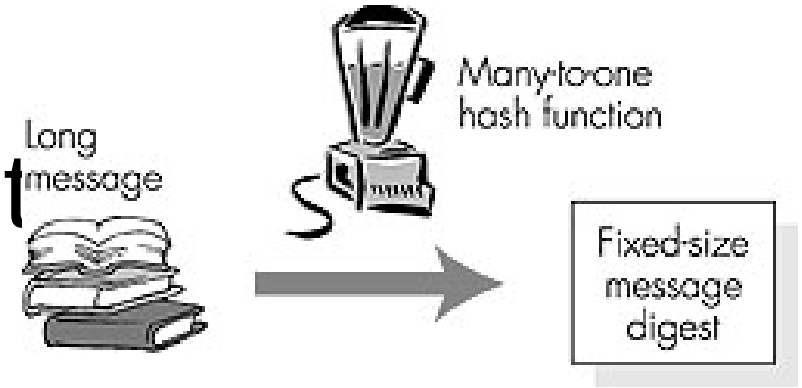
Authentication

- With little effort, the public-private keys can be applied in reverse to perform verification of e-documents
- For example, consider this e-conversation between two persons on the internet

Authentication

- Zain--> Zaki AoA, Zain here
- Zaki-->Zain Prove you are Zain
- Zain-->Zaki Send me a random message, I will return a digital signature (message digest encrypted using my private key)
- Zaki-->Zain Random message
- Zain-->Zaki digital signature
- Zaki decrypts the message using Zain’s public key and matches it to message digest

Message Digest



Computationally expensive to public-key-encrypt long messages

Goal: fixed-length,easy to compute digital signature, “fingerprint”

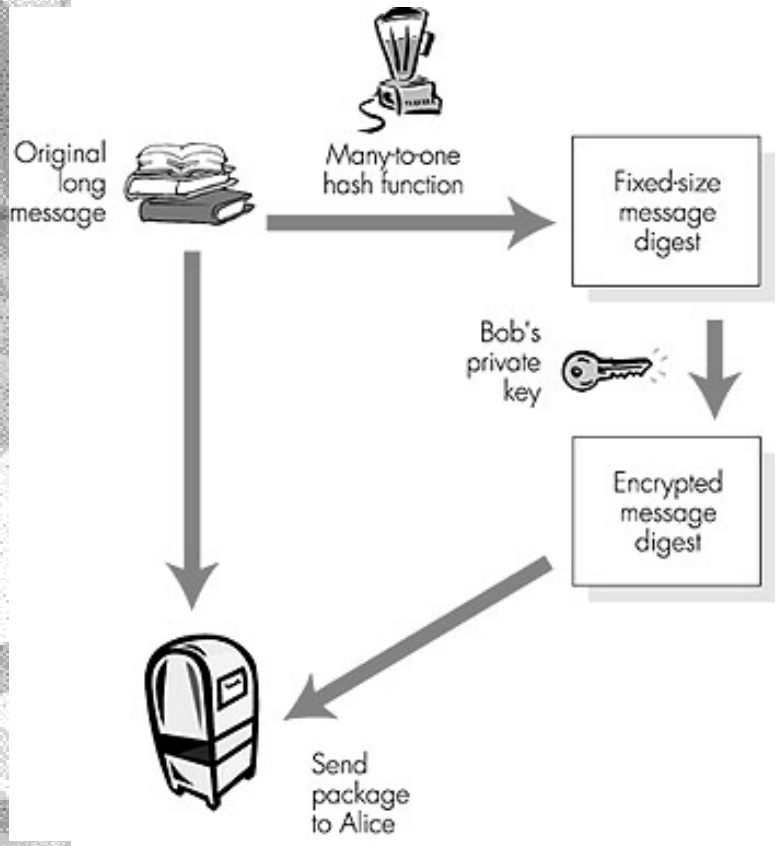
- apply hash function H to *m*, get fixed size message digest, *H(m).*

Hash function properties:

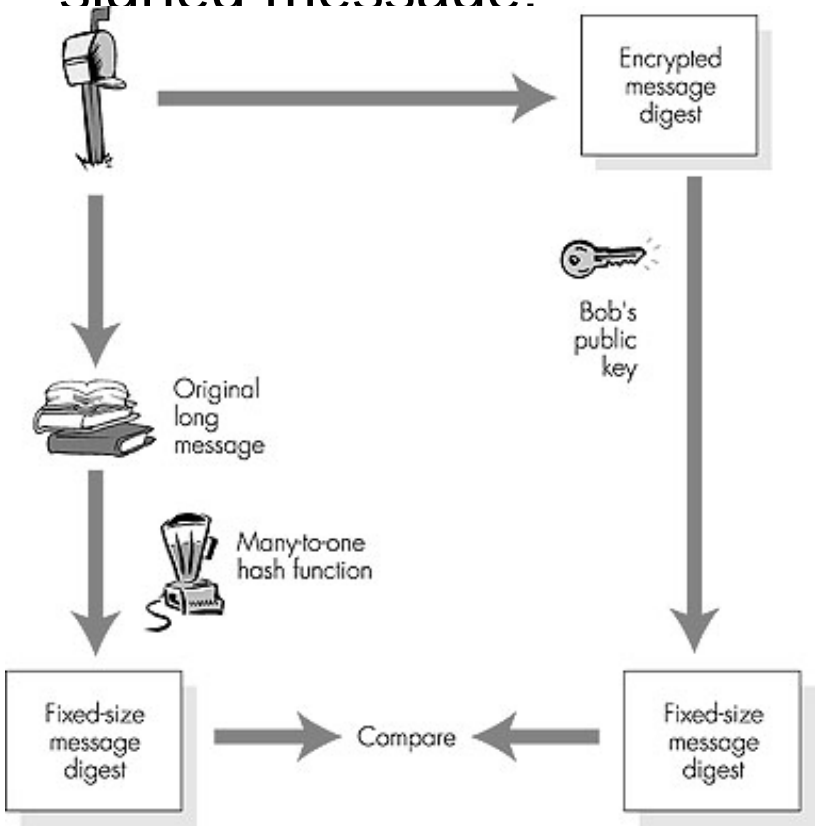
- Many-to-1
- Produces fixed-size msg digest (fingerprint)
- Given message digest x, computationally infeasible to find m such that x = H(m)
- computationally infeasible to find any two messages m and m’ such that H(m) = H(m’).

Digital signature = Signed message digest

Bob sends digitally signed message:



Alice verifies signature and integrity of digitally signed message:



Message Digests

- Message can go in clear text and the message digest can be attached to it encrypted with sender's private key
- Any changes in the clear text would produce a different message digest
- MD5 (RFC1321) and SHA-1 are in use, with SHA-1 as US Federal standard

Key Distribution

- Symmetric keys can be distributed through a KDC (Key distribution center)
- Kerberos (RFC1510) is an example of a KDC. Kerberos was designed for users of a campus server
- A CA (Certification Authority) knows which public key belongs to which organization so that no one can masquerade as another person or organization

Kerberos Example

- A registered user contacts Kerberos AS (Authentication Server) using encryption, requesting to use a service on one of the campus servers (S1)
- AS verifies access rights, then generates a ticket (containing user's name, one-time session key R1 and an expiration time before year 9999). This ticket is sent to the user using S1's secret key. User CANNOT read this ticket. However user can read the one-time session key R1 that is also sent separately

Kerberos Example

- User sends the ticket to S1, alongwith a timestamp encrypted using R1
- Server S1 decrypts the ticket using its secret key and extracts R1 from the ticket.
- Server S1 then decrypts the timestamp using R1, then encrypts it again with R1 and sends it back to the user, showing the knowledge of R1 as well as the proof that S1 is alive and well

At What Layer?

- Security can be provided at any layer of the protocol stack
- At the application layer, we can use PGP for secure email
- At transport layer, we can use SSL to encrypt all transport sessions
- At the network layer, we can encrypt all datagrams using IPSec

Secure Email

- Secure email should provide
- Secrecy
- Sender authentication
- Message Integrity
- Receiver Authentication

Pretty good privacy (PGP)

- Internet e-mail encryption scheme, a de-facto standard.
- Uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described.
- Provides secrecy, sender authentication, integrity.
- Inventor, Phil Zimmerman, was target of 3-year federal investigation.

A PGP signed message:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:The money that I
  requested has not arrived
  yet. Check with the bank

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3
  mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Secure sockets layer (SSL)

- PGP provides security for a specific network application
- SSL works above transport layer & below app layer. Provides security to any TCP-based app using SSL services.
- SSL: used between WWW browsers, servers for E-commerce (https).
- SSL security services:
  - server authentication
  - Server authentication:
    - SSL-enabled browser includes public keys for trusted CAs.
    - Browser requests server certificate, issued by trusted CA.
    - Browser uses CA's public key to extract server's public key from certificate.
  - Visit your browser's security menu to see its trusted CAs.

SSL (continued)

Encrypted SSL session:

- Browser generates symmetric session key, encrypts it with server's public key, sends encrypted key to server.
- Using its private key, server decrypts session key.
- Browser, server agree that future messages will be encrypted.
- All data sent into TCP socket (by client or server) is encrypted with

- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.

Network Layer Security

- IPSec is a whole suite of protocols with several RFC's
- Providing encryption at the network layer encrypts all applications
- Targets for IPSec are integrity, source authentication and secrecy
- IPSec has AH and ESP protocols

SA (Security Agreement)

- The source and the destination enter into an agreement before starting secure transmission
- SA denotes a simplex connection
- SA has:
  - AH or ESP identifier
  - Source IP address
  - 32-bit SPI (Security Parameter Index) i.e. connection identifier

AH Protocol

- AH (Authentication Header) protocol provides source authentication and integrity but no secrecy
- After establishing SA, source starts sending AH datagrams showing upper layer protocol as 51
- AH datagrams have AH header after the normal IP header

AH Header

- AH Header includes several fields:
  - Next Header field: Identifying the upper protocol e.g. TCP, UDP etc.
  - SPI field: indicating connection number
  - Sequence Number field: A 32 bit field containing sequence number of every AH datagram
  - Authentication field: containing encrypted message digest (digital signature) for this datagram. Encryption is with symmetric keys

ESP Protocol

- ESP (Encapsulation Security Payload) provides authentication and secrecy
- ESP datagrams are identified by protocol field value of 50 in the IP header
- Upper layer segment is sandwiched between ESP header and trailer
- ESP Auth field follows the trailer

ESP Protocol

- The original upper layer segment and the ESP trailer are encrypted with a type of DES encryption
- ESP trailer contains the upper layer protocol identifier
- ESP header has SPI and sequence number
- ESP Auth contains digital signature for authentication
- IKE (Internet Key Exchange) algorithm is the default key distribution protocol for IPSec

Firewalls

- A firewall is a piece of hardware and software that isolates an organization's internal network from the Internet
- The firewall then allows some traffic and blocks other traffic
- Firewalls try to prevent intruders from crashing the organization's servers, reading secret information and modifying the same

Packet Filtering Firewalls

- An organization's gateway router can be configured to filter out some packets
- For example, discard all IP datagrams whose upper protocol field is 17 (UDP) thus blocking audio/video streaming
- Block all segments whose port number is 23 (Telnet)

Firewall in action

- Block all IP datagrams whose source IP address is internal but they have arrived from outside (IP Spoofing)
- Block all incoming TCP segments with ACK=0 (external clients trying to connect to internal servers)

Application Gateways

- If we wish to allow only few users to connect to outside world, we need application gateways in addition to packet filters
- For example, a telnet app gateway would verify if a user is authorized to telnet outside. If yes, telnet is allowed else blocked

Network Security (summary)

Basic techniques……

- cryptography (symmetric and public)
- authentication
- message integrity

…. used in many different security scenarios

- secure email
- secure transport (SSL)
- IPSec