CS 54001-1: Large-Scale Networked Systems

Professor: Ian Foster

TAs: Xuehai Zhang, Yong Zhao

Lecture 4

www.classes.cs.uchicago.edu/classes/archive/2003/winter/54001-1

Week 1: Internet Design Principles & Protocols

- An introduction to the mail system
- An introduction to the Internet
- Internet design principles and layering
- Brief history of the Internet
- Packet switching and circuit switching
- Protocols
- Addressing and routing
- Performance metrics
- A detailed FTP example

Week 2: Routing and Transport

- Routing techniques
  - Flooding
  - Distributed Bellman Ford Algorithm
  - Dijkstra’s Shortest Path First Algorithm
- Routing in the Internet
  - Hierarchy and Autonomous Systems
  - Interior Routing Protocols: RIP, OSPF
  - Exterior Routing Protocol: BGP
- Transport: achieving reliability
- Transport: achieving fair sharing of links

Week 3:
Measurement & Characterization

- What does the Internet look like?
- What does Internet traffic look like?
- How do I measure such things?
- How do such characteristics evolve?
- What Internet characteristics are shared with other networks?
- Are all those Faloutsos' related?

Week 4: Security

- Context: Attacks, services, & mechanisms
- Message encryption
- Public key cryptography
- Authentication protocols
- Message integrity
- Public key infrastructure
- Firewalls

Attacks, Services and Mechanisms

- Security Attack: Any action that compromises the security of information.
- Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.
- Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Attacks

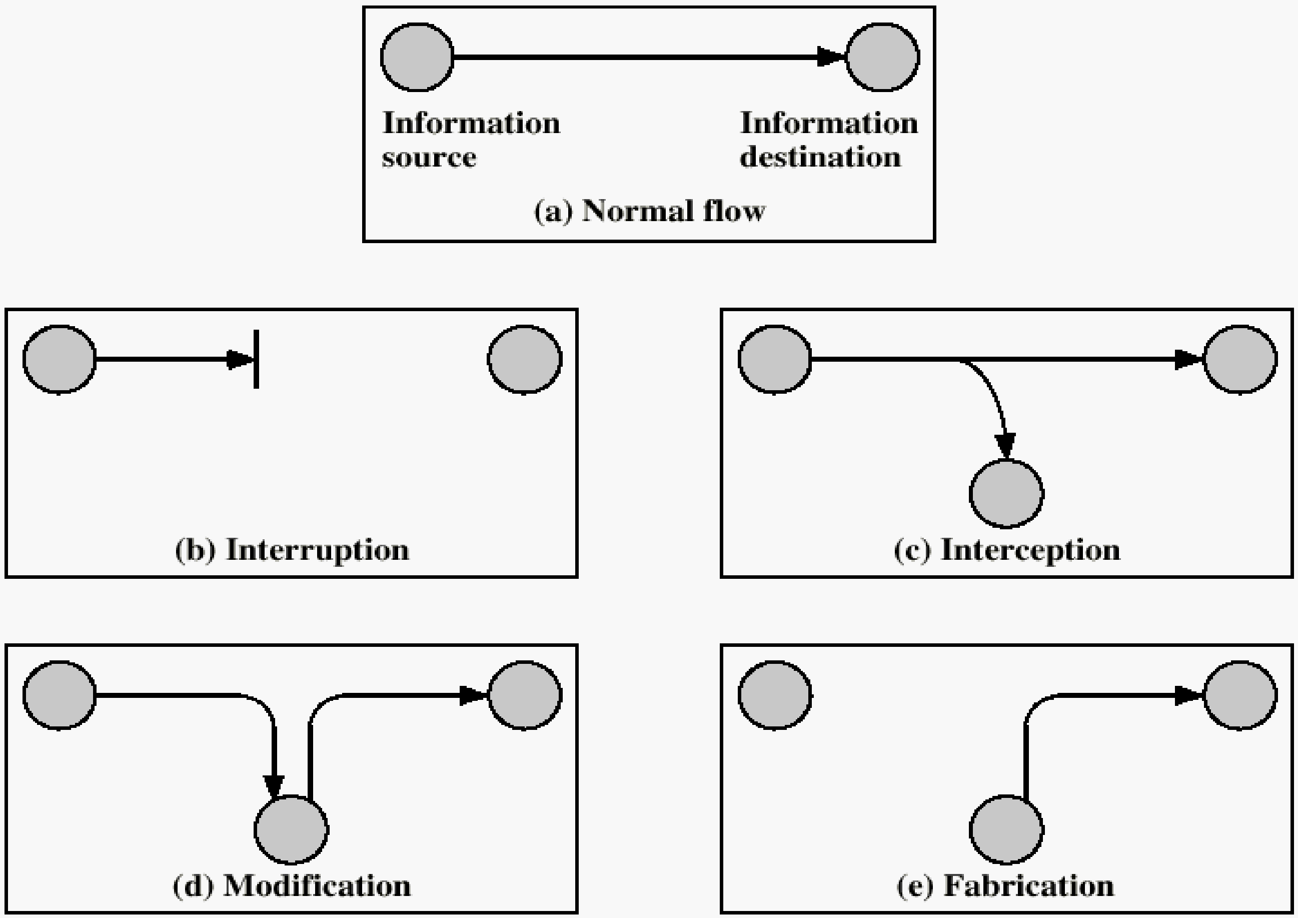


Figure 1.1 Security Threats

Security Attacks

- Interruption: This is an attack on availability
- Interception: This is an attack on confidentiality
- Modification: This is an attack on integrity
- Fabrication: This is an attack on authenticity

Active and Passive Threats

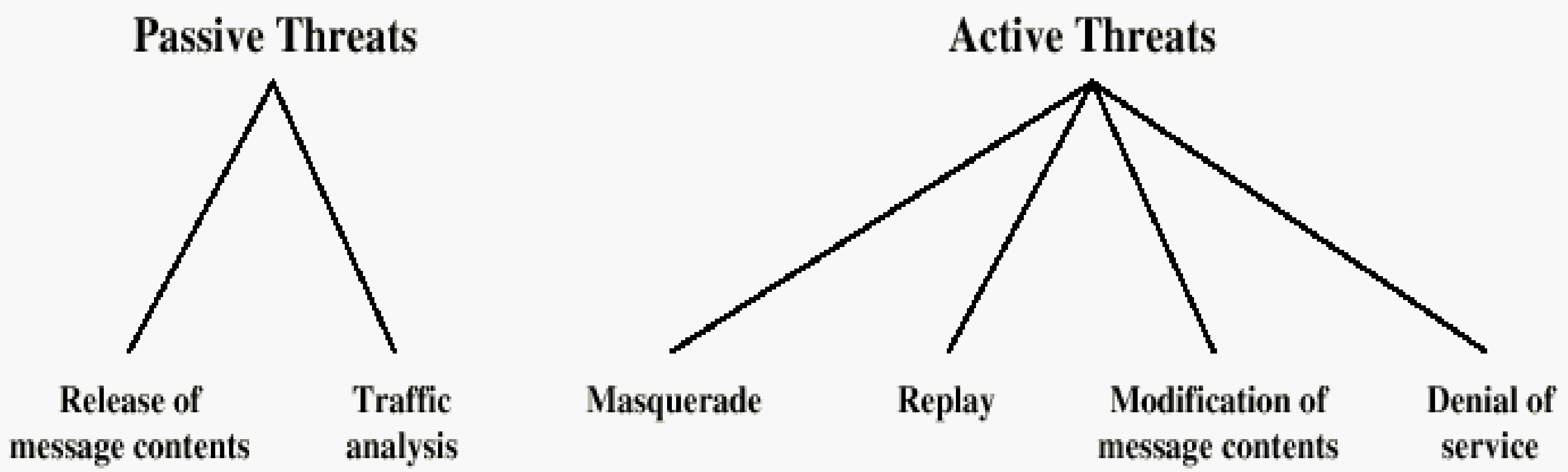
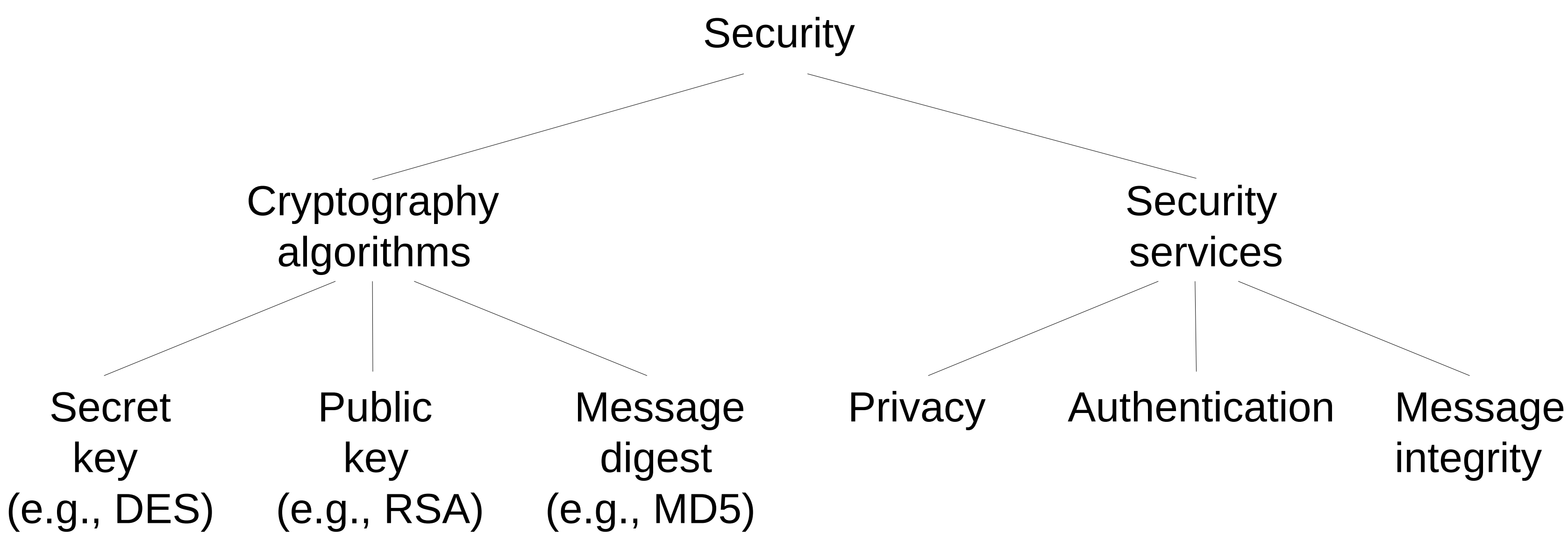


Figure 1.2 Active and Passive Security Threats

Methods of Defense

- Encryption
- Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Hardware Controls (smartcard)
- Policies (frequent changes of passwords)
- Physical Controls

Security Algorithms & Services



Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

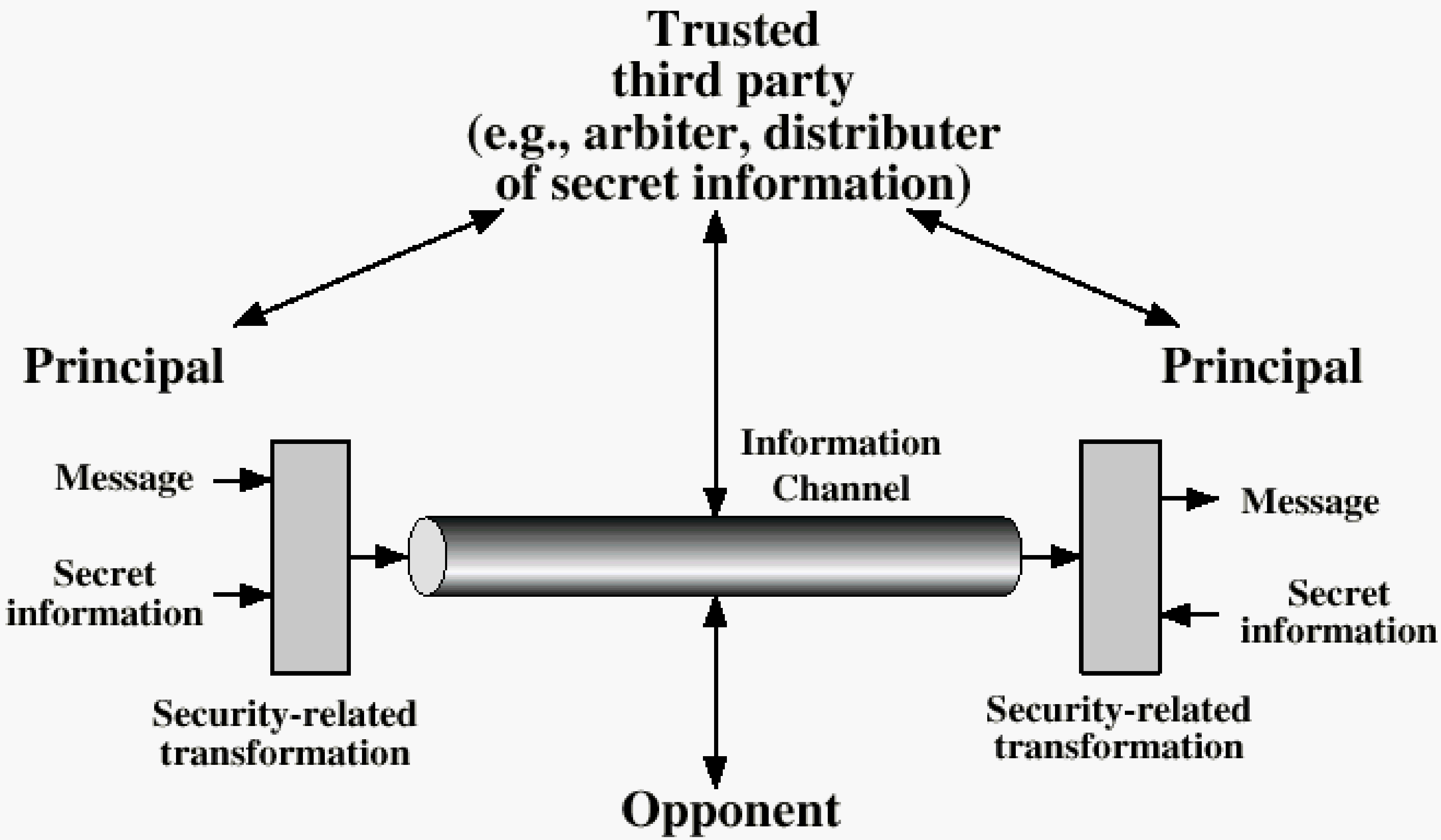


Figure 1.3 Model for Network Security

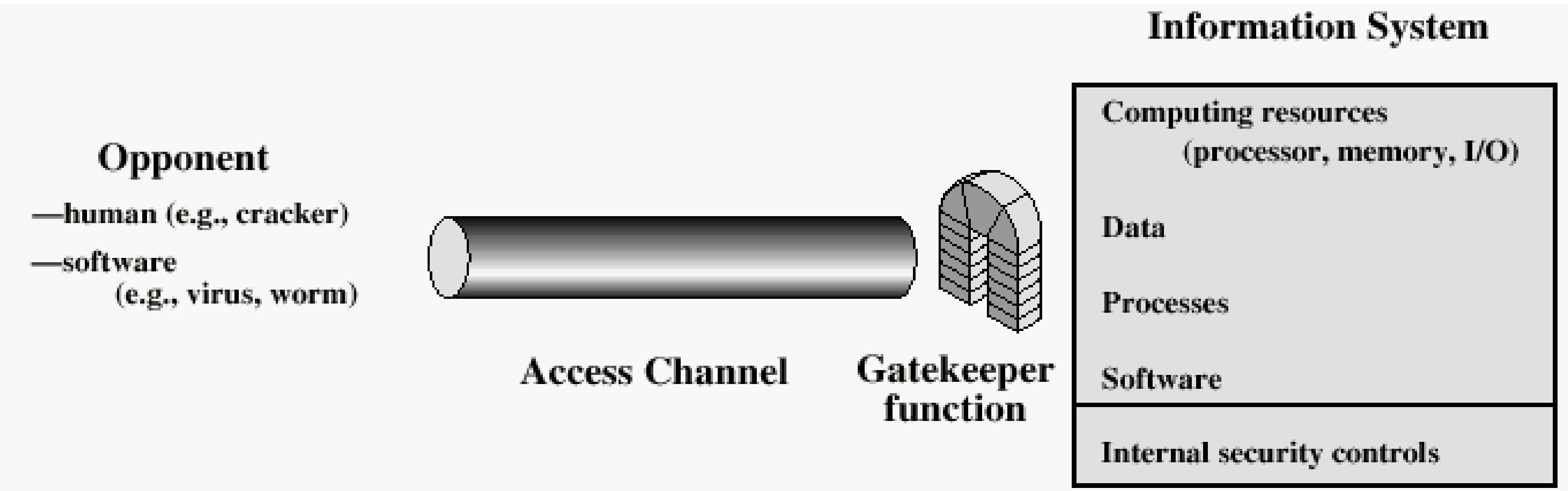


Figure 1.4 Network Access Security Model

Week 4: Security

- Context: Attacks, services, & mechanisms
- **Message encryption**
- Public key cryptography
- Authentication protocols
- Message integrity
- Public key infrastructure
- Firewalls

Conventional Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm

Conventional Encryption Principles

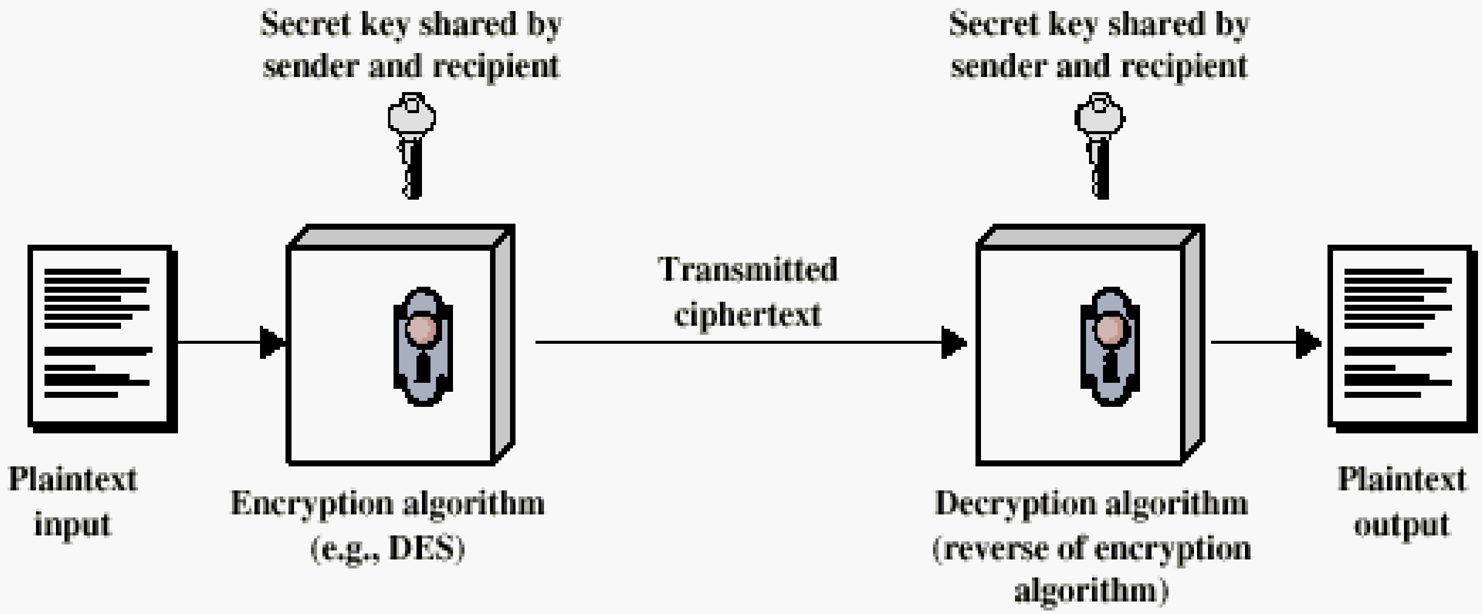


Figure 2.1 Simplified Model of Conventional Encryption

Cryptography

- Classified along three independent dimensions:
  - The type of operations used for transforming plaintext to ciphertext
  - The number of keys used
    - symmetric (single key)
    - asymmetric (two-keys, or public-key encryption)
  - The way in which the plaintext is processed

Average time required for exhaustive key search

Key Size (bits)	**Number of Alternative Keys**	**Time required at 10^6 Decryption/µs**
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Conventional Encryption Algorithms

- Data Encryption Standard (DES)
  - The most widely used encryption scheme
  - The algorithm is reffered to the Data Encryption Algorithm (DEA)
  - DES is a block cipher
  - The plaintext is processed in 64-bit blocks
  - The key is 56-bits in length

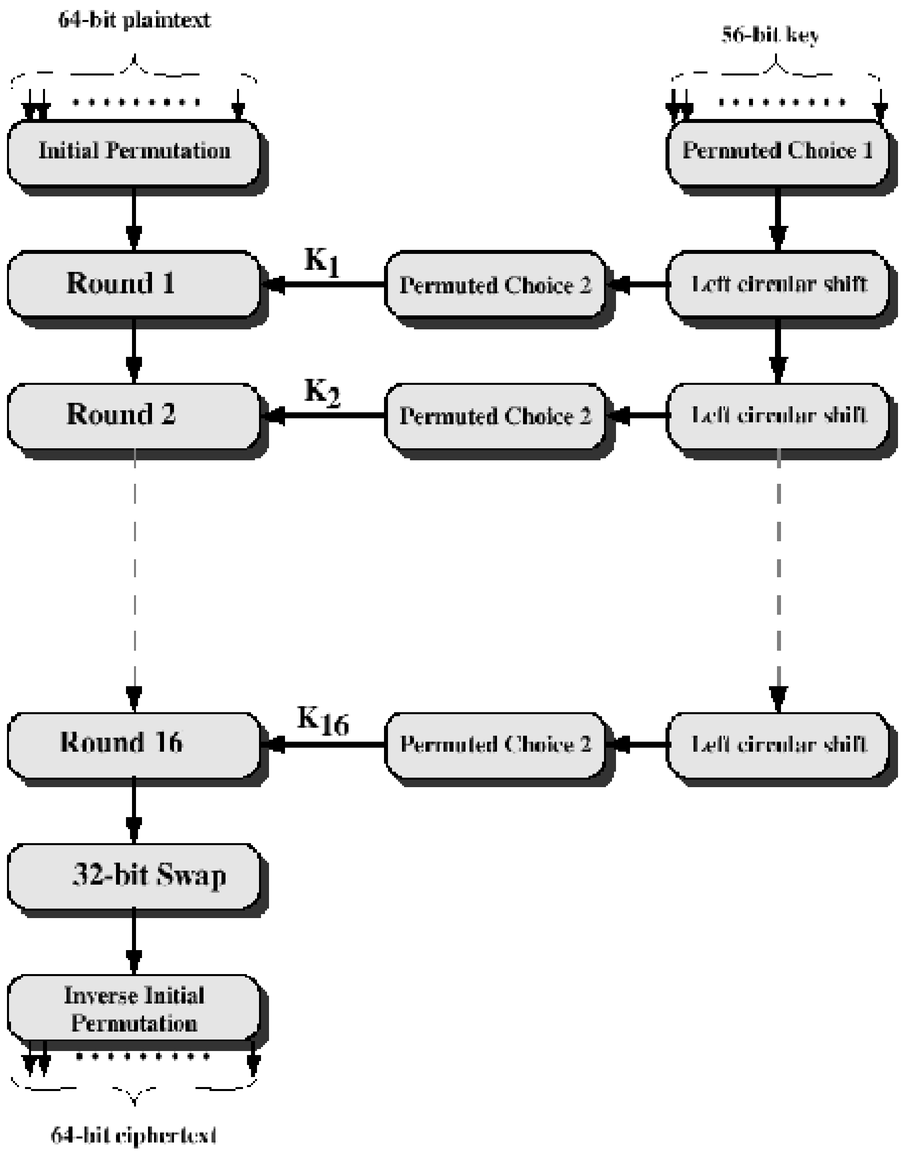


Figure 2.3 General Depiction of DES Encryption Algorithm

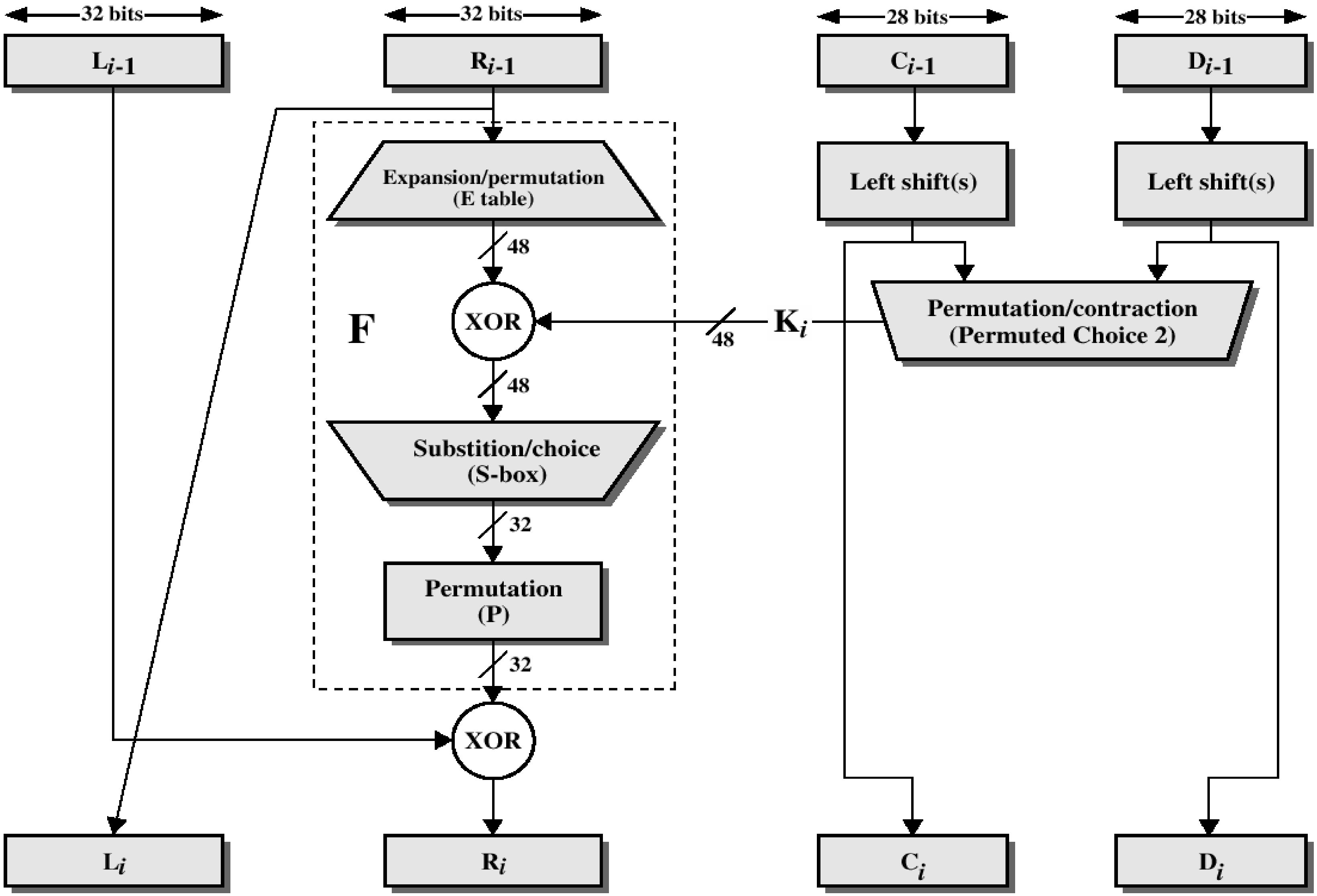
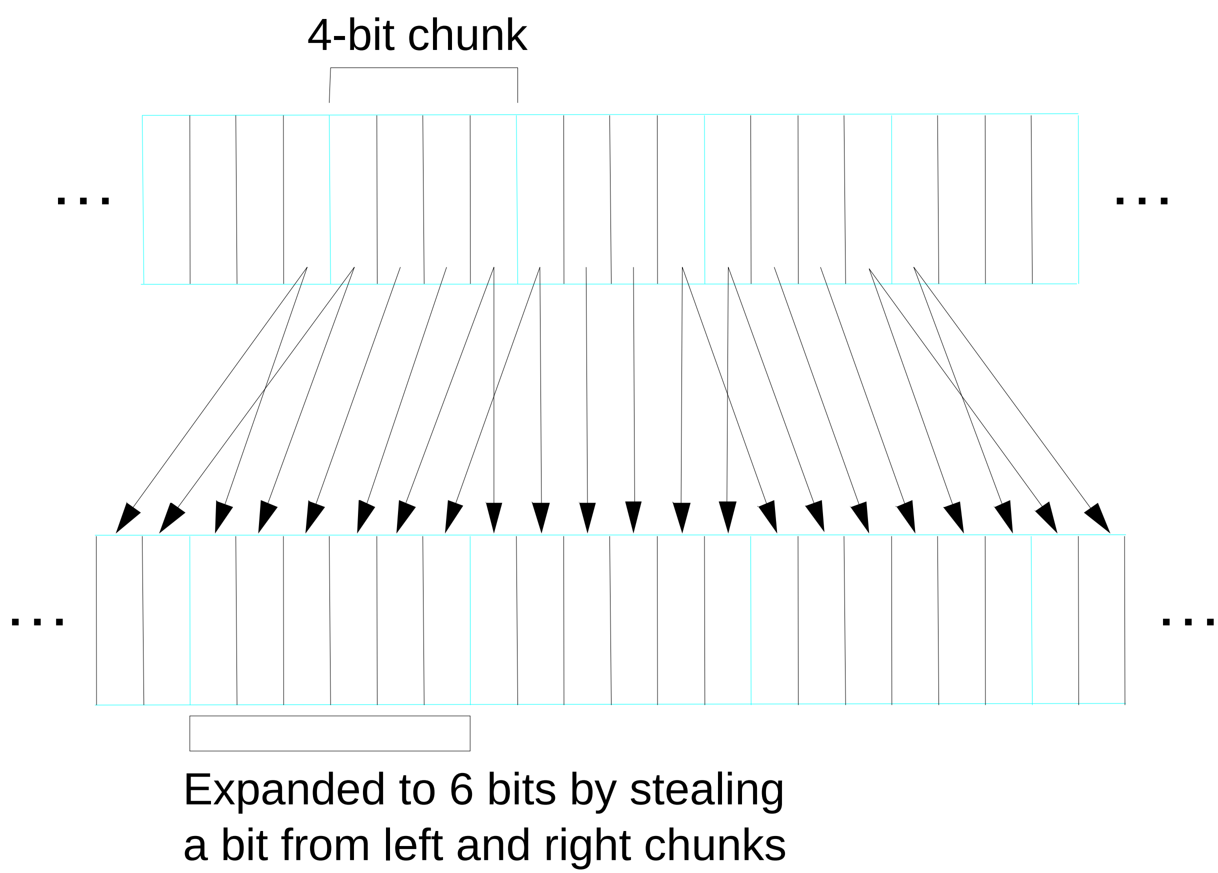
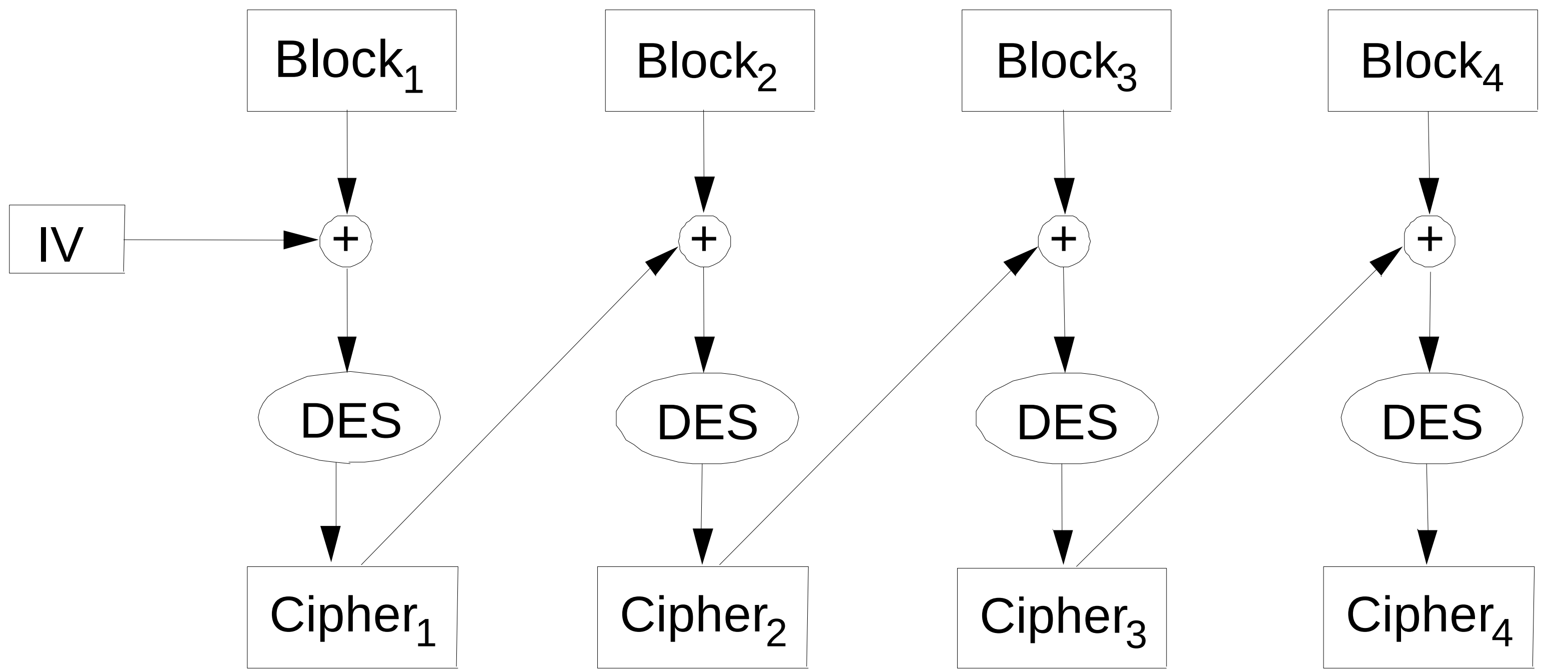


Figure 2.4 Single Round of DES Algorithm

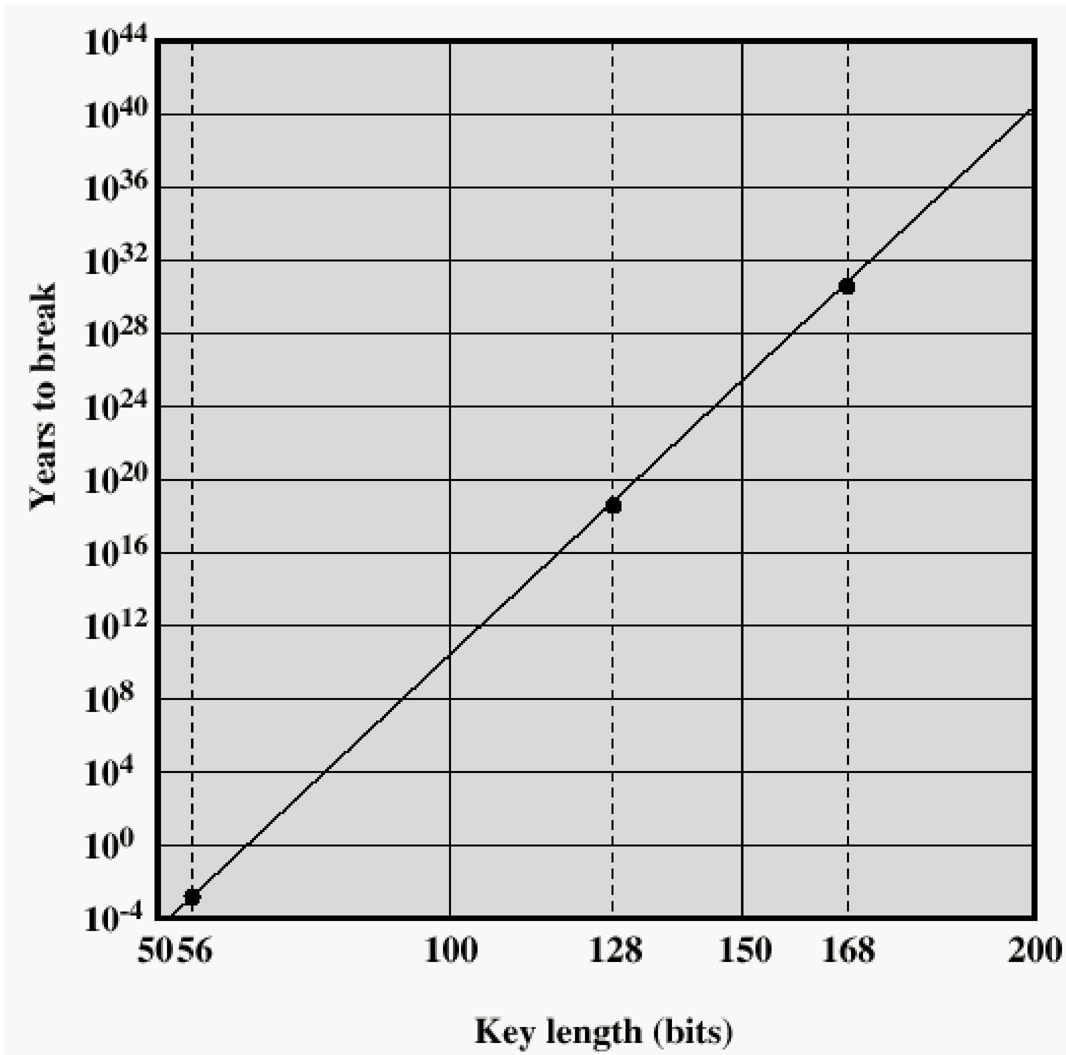
Expansion Phase of DES



Cipher Block Chaining



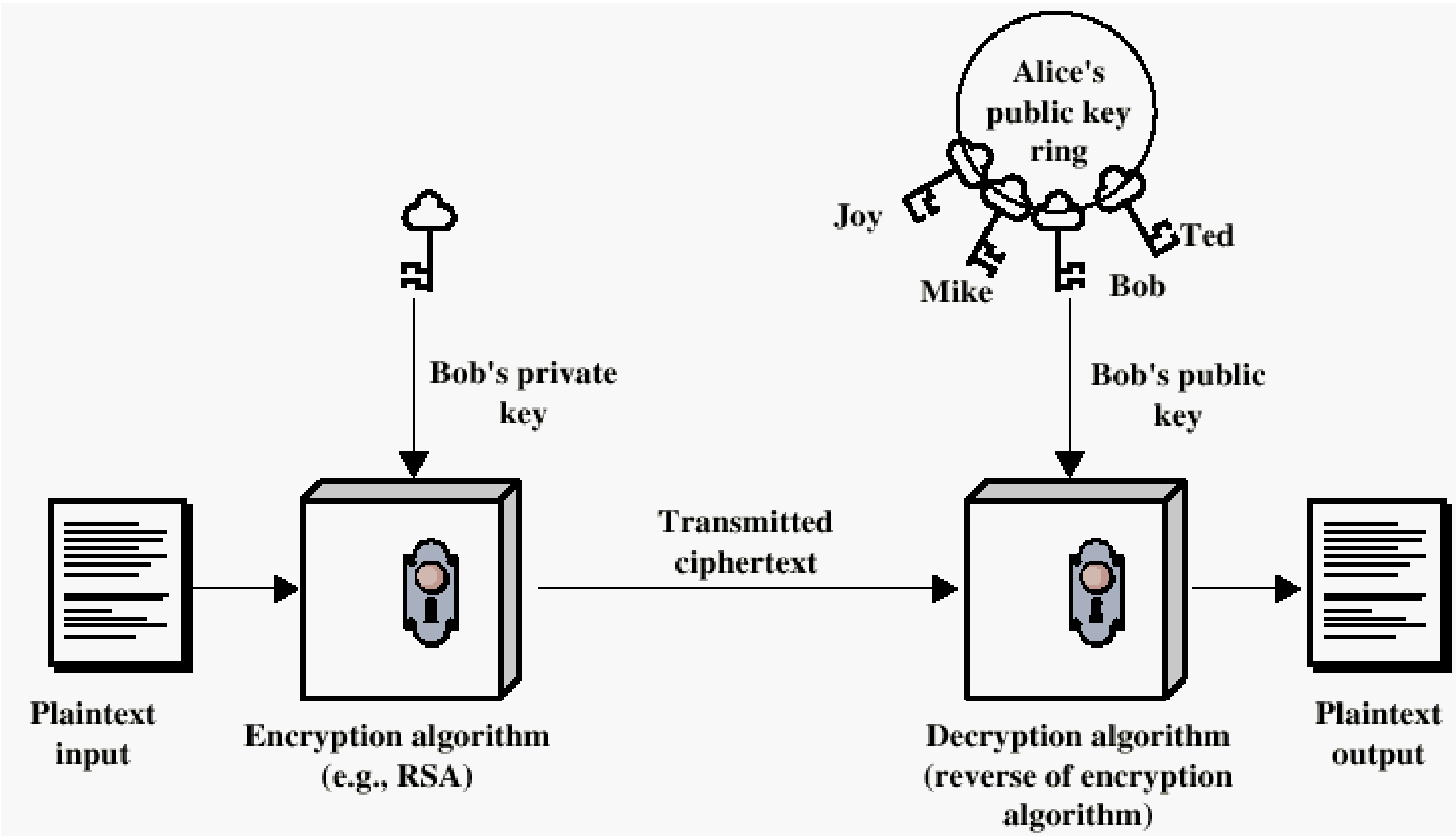
Time to break a code (10^6 decryptions/μs)



Week 4: Security

- Context: Attacks, services, & mechanisms
- Message encryption
- **Public key cryptography**
- Authentication protocols
- Message integrity
- Public key infrastructure
- Firewalls

Public-Key Cryptography



Applications for Public-Key Cryptosystems

- Three categories:
  - **Encryption/decryption:** The sender encrypts a message with the recipient's public key
  - **Digital signature:** The sender ”signs” a message with its private key
  - **Key exchange:** Two sides cooperate to exhange a session key

Requirements for Public-Key Cryptography

- Computationally easy for a party B to generate a pair (public key KUb, private key KRb)
- Easy for sender to generate ciphertext

$$C = E_{KUb}(M)$$

- Easy for the receiver to decrypt ciphertect using private key

$$M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$$

Requirements for Public-Key Cryptography

- Computationally infeasible to determine private key (KRb) knowing public key (KUb)
- Computationally infeasible to recover message M, knowing KUb and ciphertext C
- Either of the two keys can be used for encryption, with the other used for decryption

$$M = D_{KRb}[E_{KUb}(M)] = D_{KUb}[E_{KRb}(M)]$$

Public-Key Cryptographic Algorithms

- RSA and Diffie-Hellman
- RSA - Ron Rives, Adi Shamir and Len Adleman at MIT, in 1977.
  - RSA is a block cipher
  - The most widely implemented
- Diffie-Hellman
  - Exchange a secret key securely
  - Compute discrete logarithms

The RSA Algorithm – Key Generation

1. Select p,q — p and q both prime
2. Calculate $n = p \times q$
3. Calculate $\Phi(n) = (p-1)(q-1)$
4. Select integer e — $\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$
5. Calculate d — $d = e^{-1} \bmod \Phi(n)$
6. Public Key — KU = {e,n}
7. Private key — KR = {d,n}

Example of RSA Algorithm

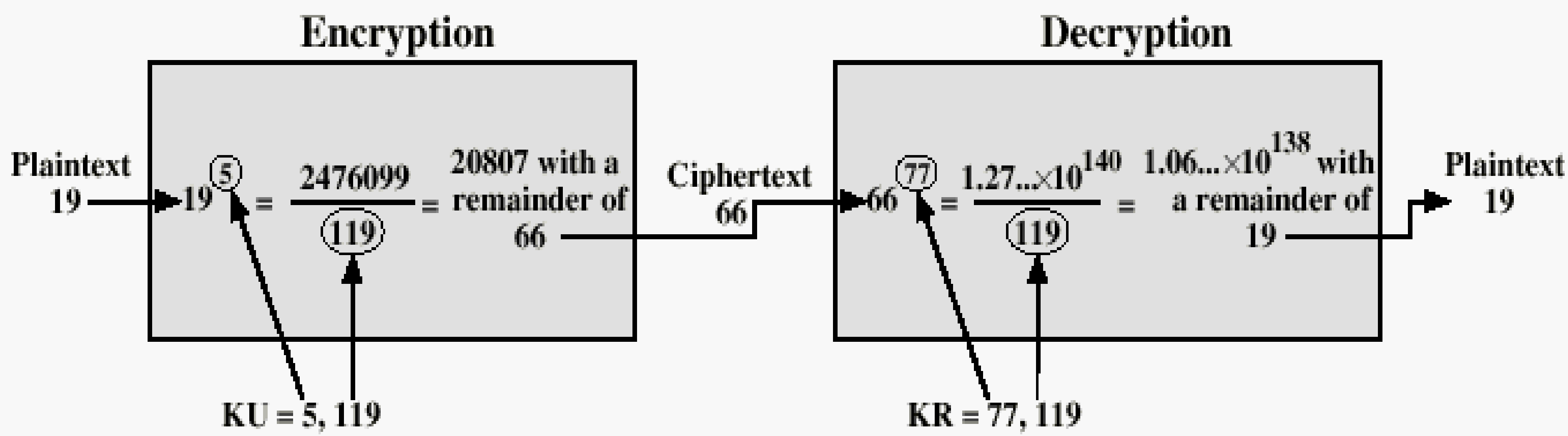


Figure 3.9 Example of RSA Algorithm

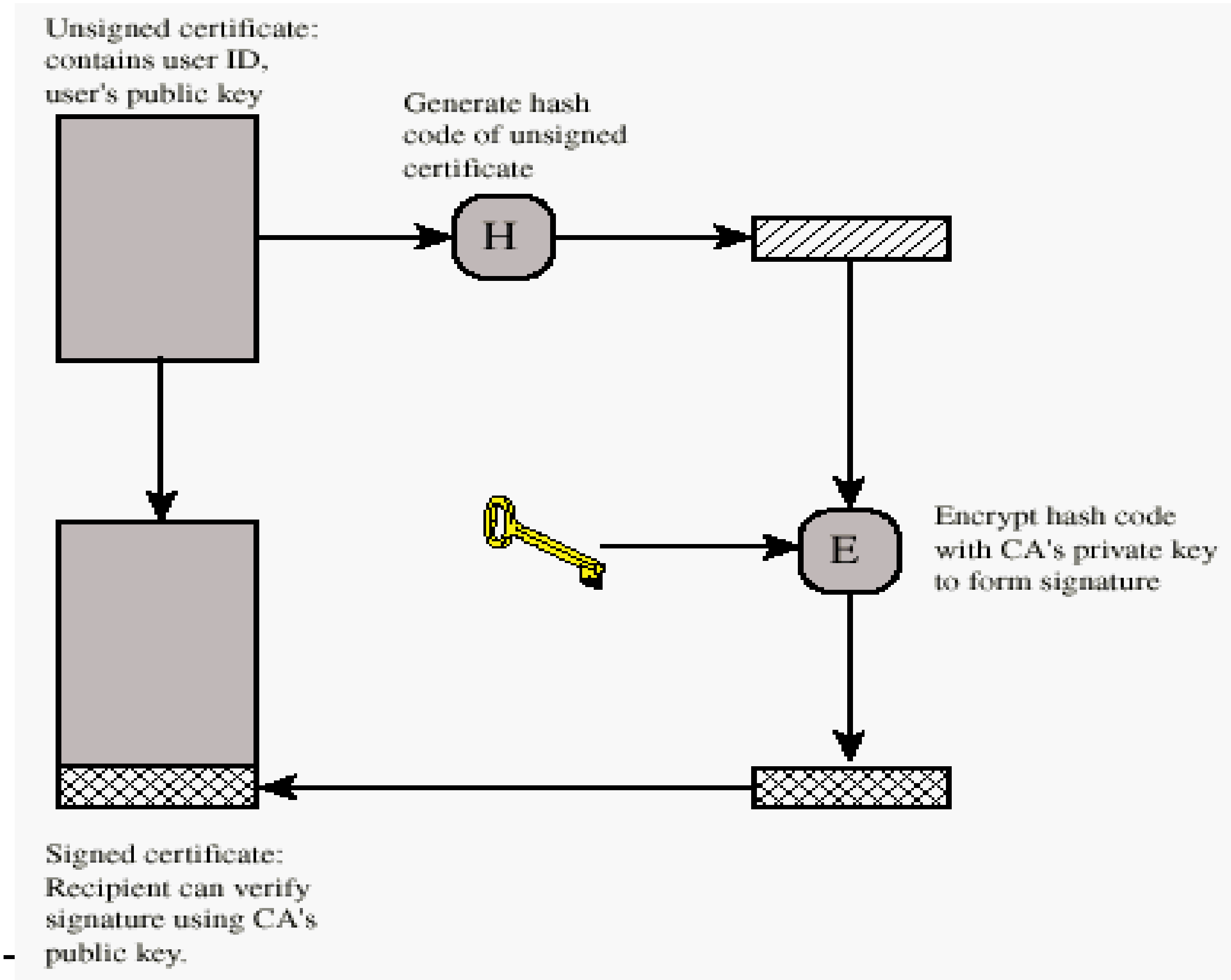
The RSA Algorithm - Encryption

- Plaintext: $M<n$
- Ciphertext: $C = M^e \pmod n$

The RSA Algorithm - Decryption

- Ciphertext: C
- Plaintext: $M = C^d \pmod{n}$

Key Management
Public-Key Certificate Use



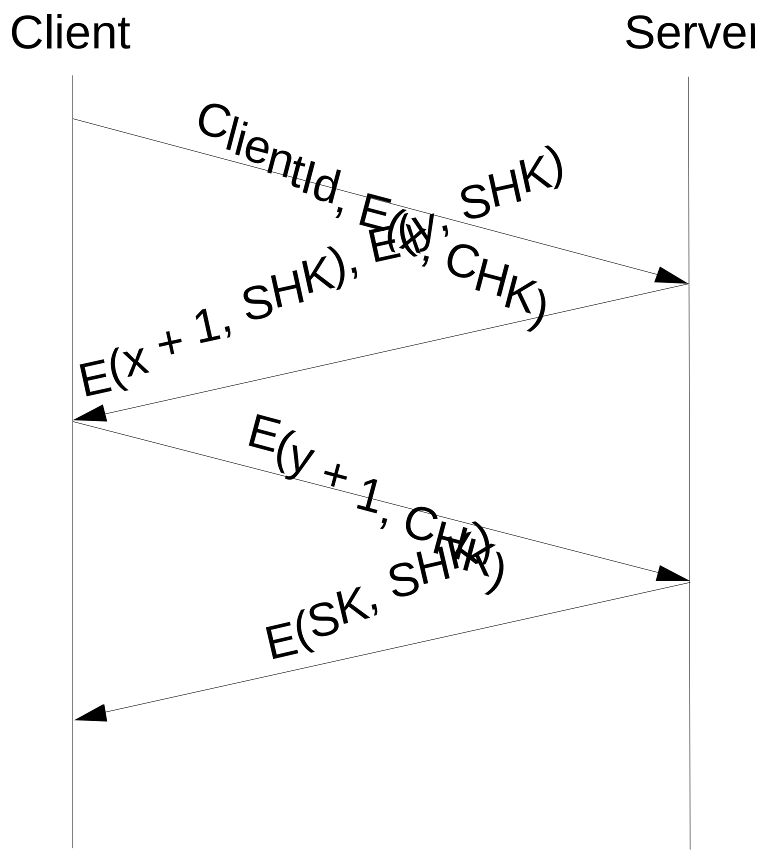
Week 4: Security

- Context: Attacks, services, & mechanisms
- Message encryption
- Public key cryptography
- **Authentication protocols**
- Message integrity
- Public key infrastructure
- Firewalls

Authentication Protocols

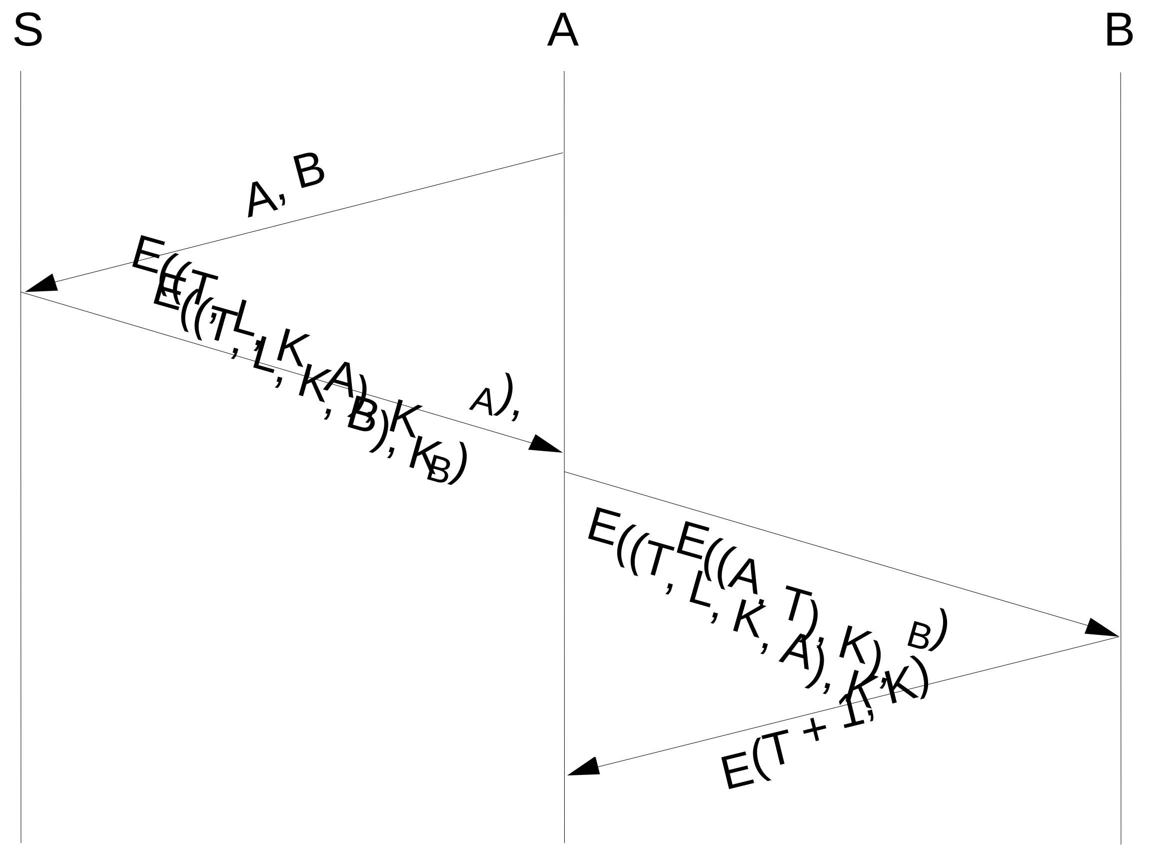
- Simple three-way handshake
  - Assume two parties share a secret key
- Trusted third party
  - E.g., Kerberos
- Public key authentication

Simple Three-Way Handshake



E(m,k) denotes encryption of message m with key k

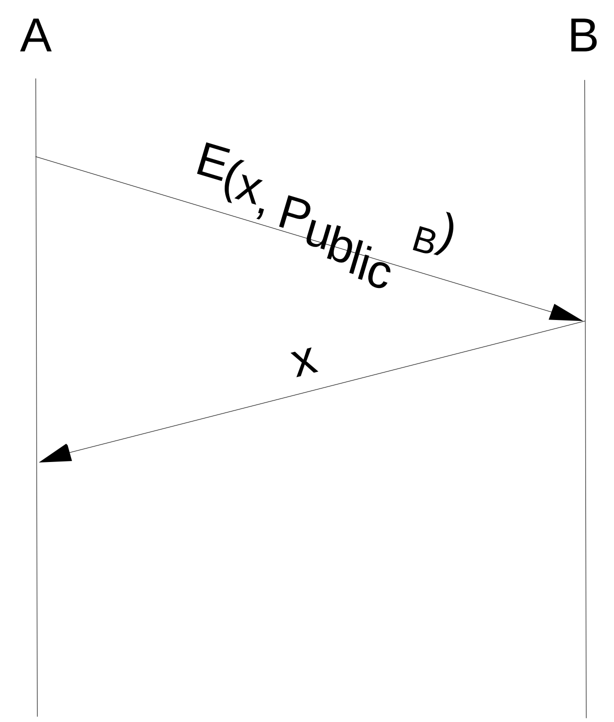
Trusted Third Party



Ka and Kb are secret keys shared with server S

T=timestamp, L=lifetime, K=session key

Public Key Cryptography



Message Integrity

- Requirements - must be able to verify that:
  - Message came from apparent source or author,
  - Contents have not been altered,
  - Sometimes, it was sent at a certain time or sequence.
- Protection against active attack (falsification of data and transactions)

Approaches to Message Integrity

- Conventional encryption
  - Only the sender and receiver should share a key
- Message integrity without message encryption
  - An authentication tag is generated and appended to each message
- Message Authentication Code
  - Calculate the MAC as a function of the message and the key. MAC = F(K, M)

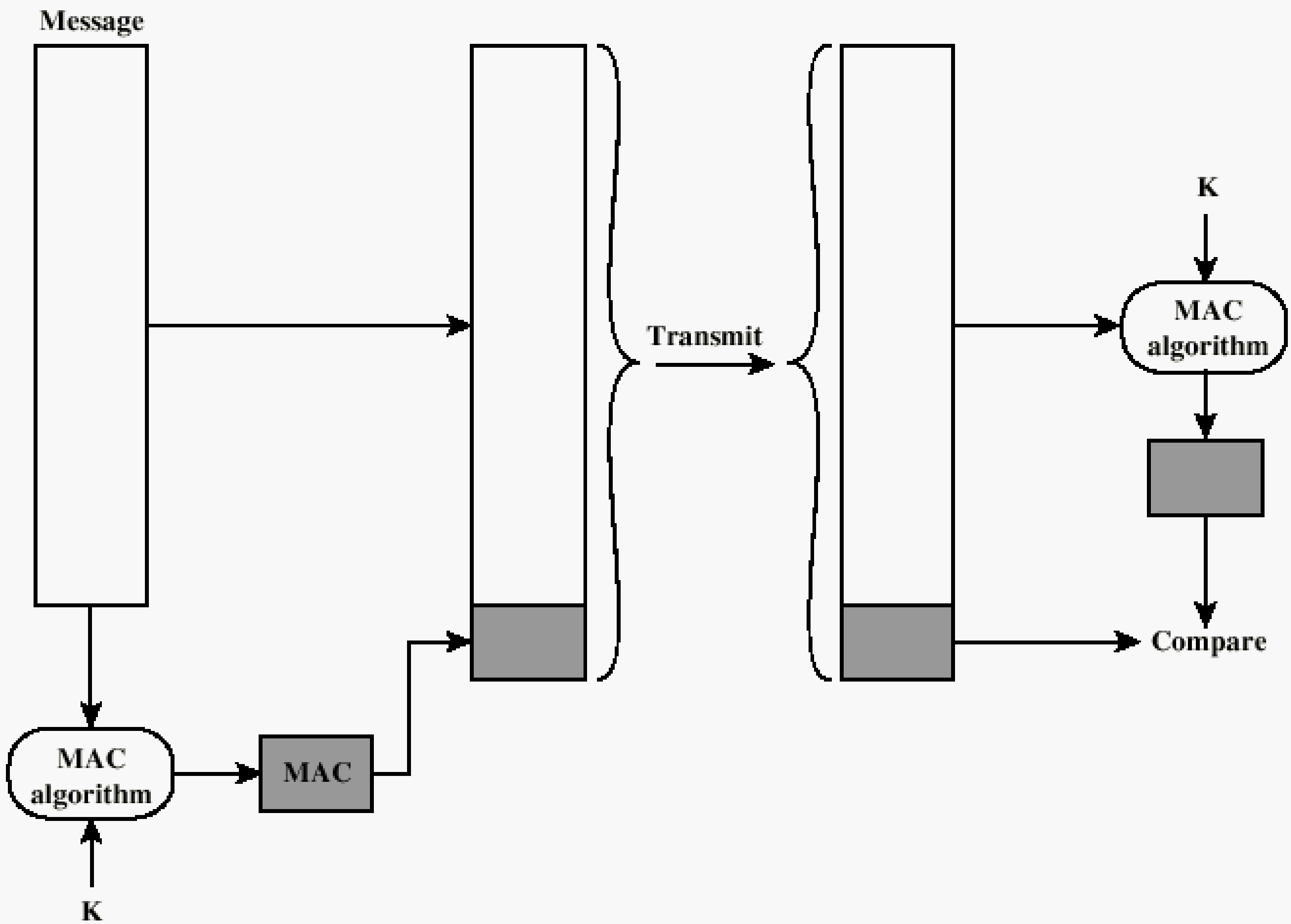
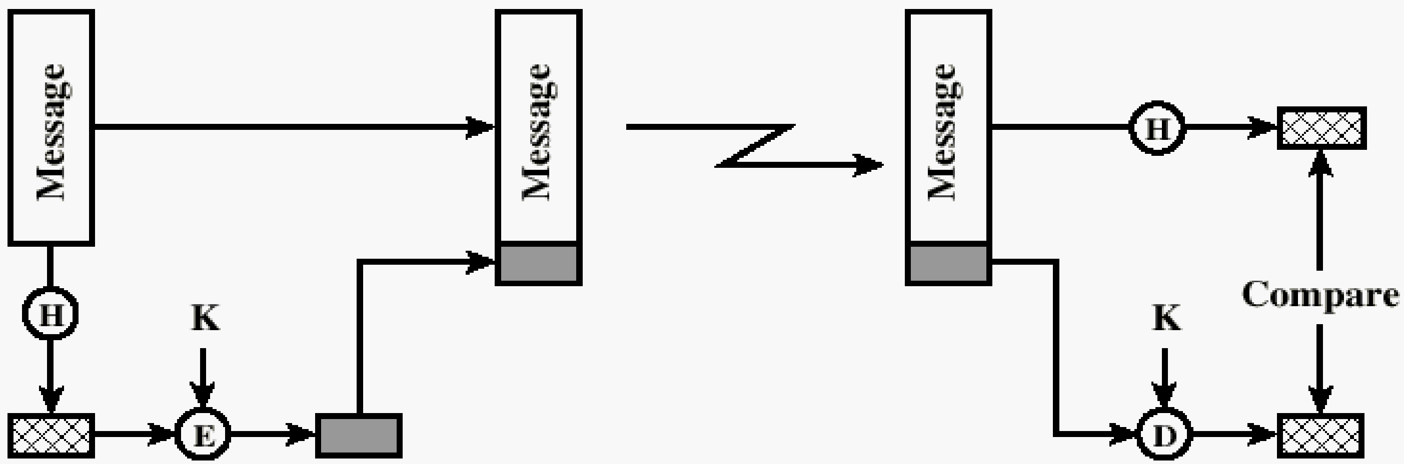
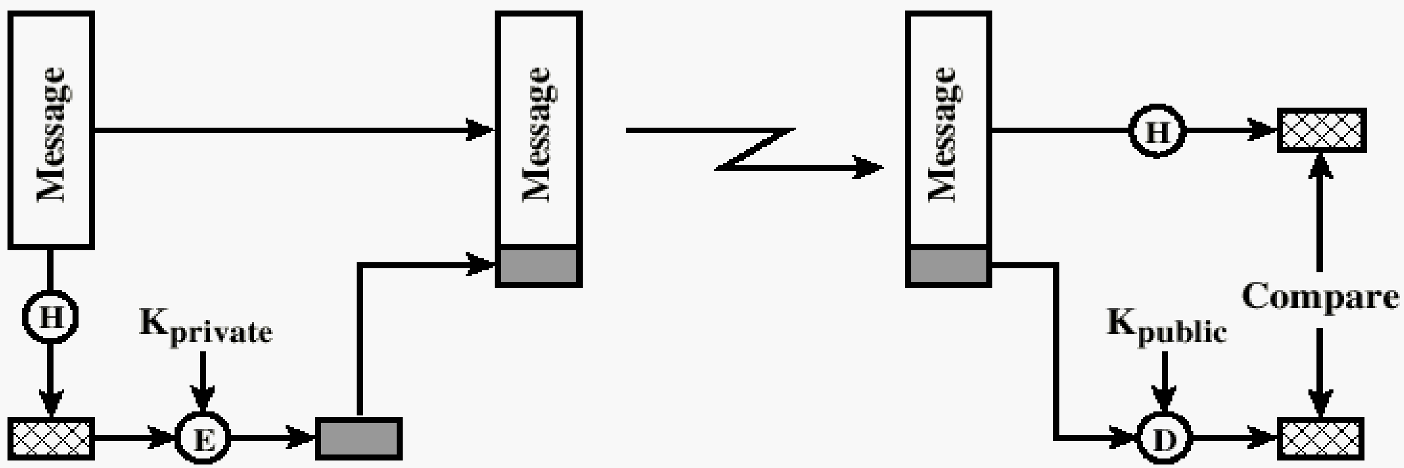


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

One-way HASH function



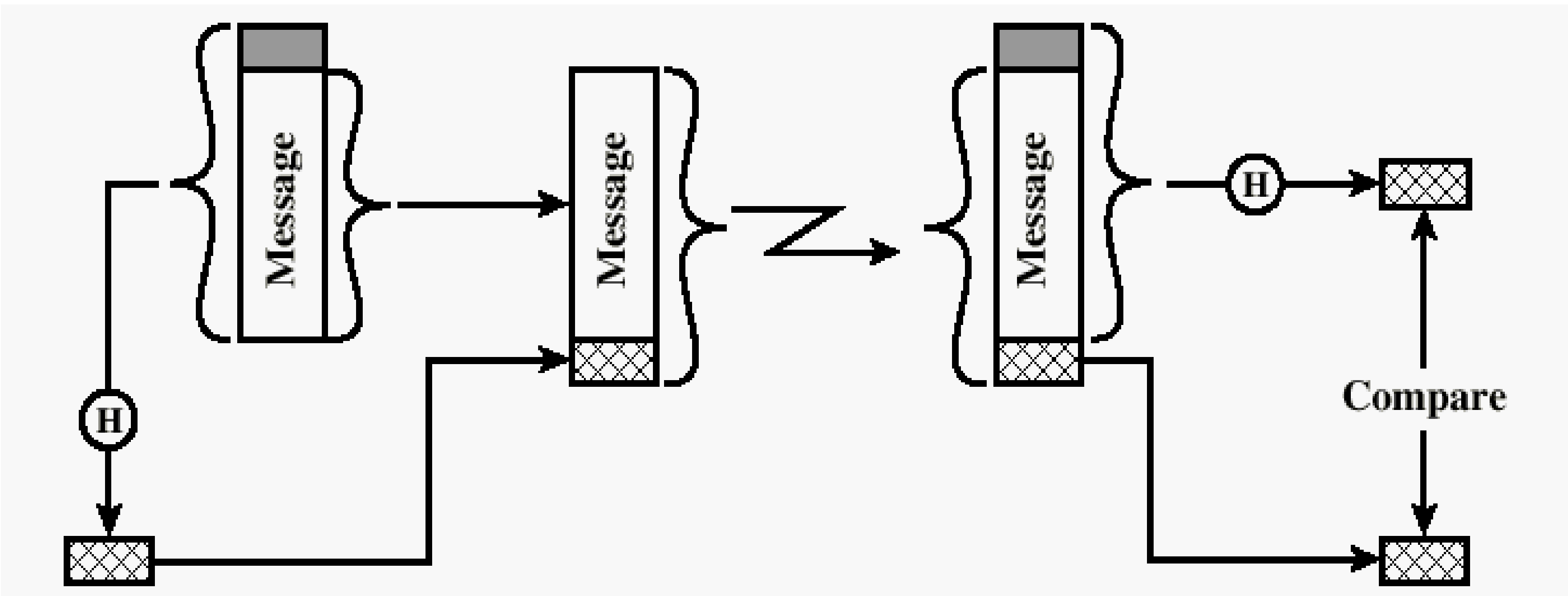
(a) Using conventional encryption



(b) Using public-key encryption

One-way HASH function

- Secret value is added before the hash and removed before transmission.



(c) Using secret value

Secure HASH Functions

- Purpose of the HASH function is to produce a ”fingerprint.
- Properties of a HASH function H :

1. H can be applied to a block of data at any size
2. H produces a fixed length output
3. H(x) is easy to compute for any given x.
4. For any given block x, it is computationally infeasible to find x such that H(x) = h
5. For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y)

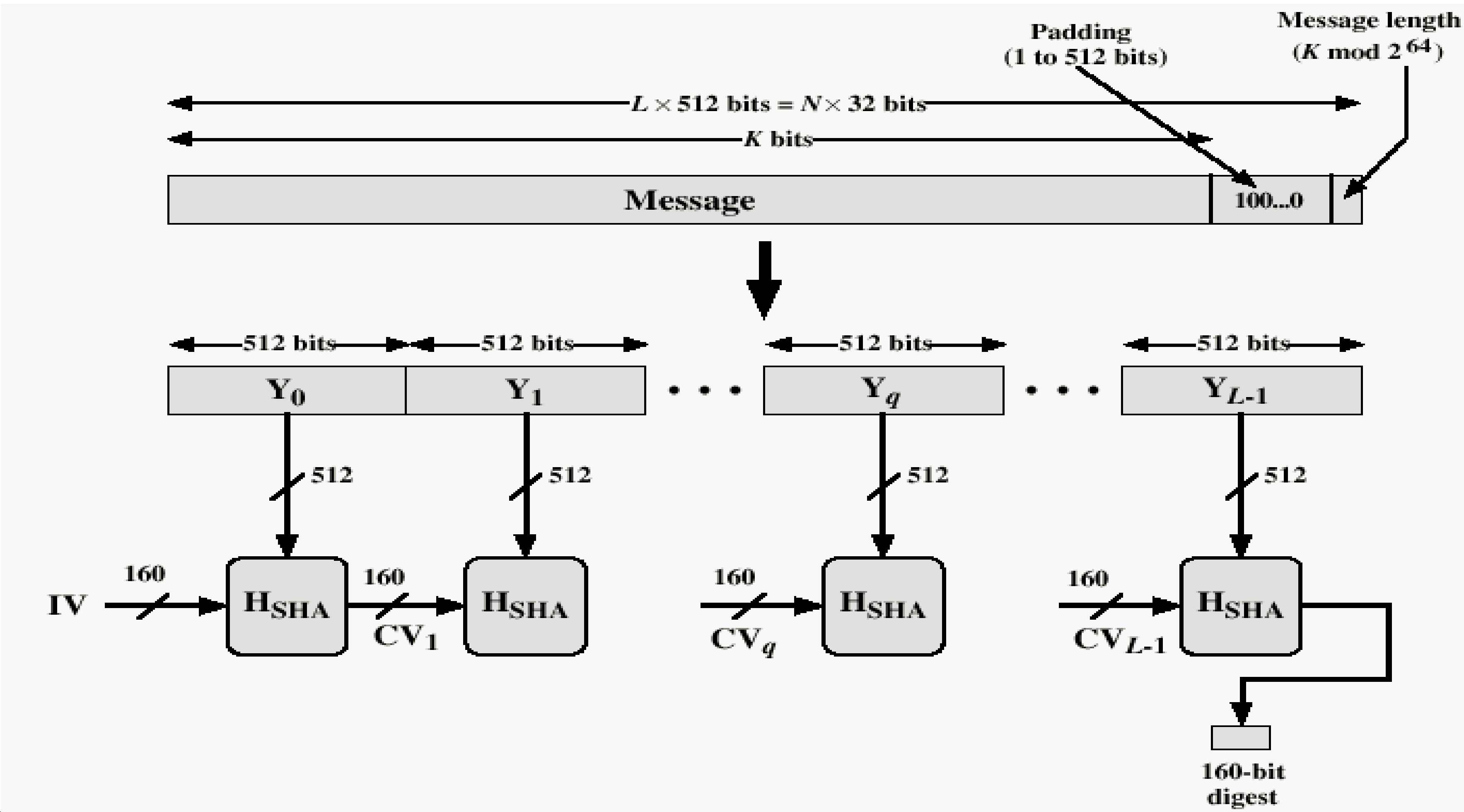
Simple Hash Function

	bit 1	bit 2	• • •	bit *n*
block 1	b_{11}	b_{21}		b_{n1}
block 2	b_{12}	b_{22}		b_{n2}
	⋮	⋮	⋮	⋮
block *m*	b_{1m}	b_{2m}		b_{nm}
hash code	C_1	C_2		C_n

Figure 3.3 Simple Hash Function Using Bitwise XOR

- One-bit circular shift on the hash value after each block is processed would improve

Message Digest Generation Using SHA-1



SHA-1 Processing of single 512-Bit Block

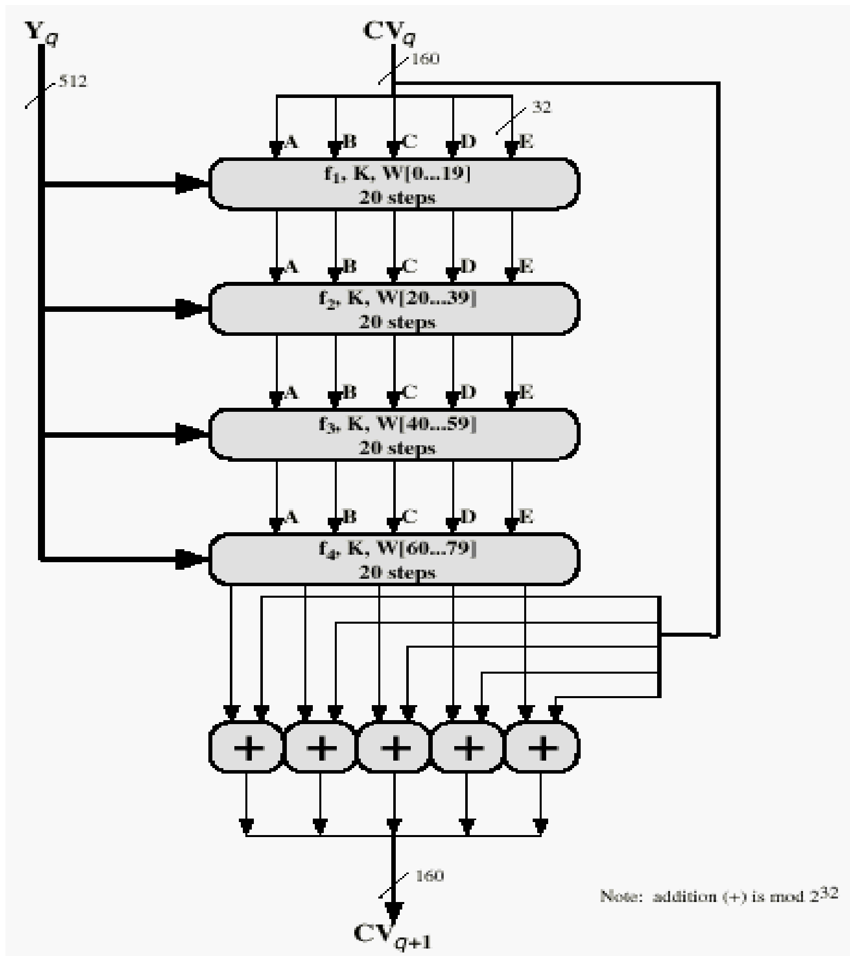
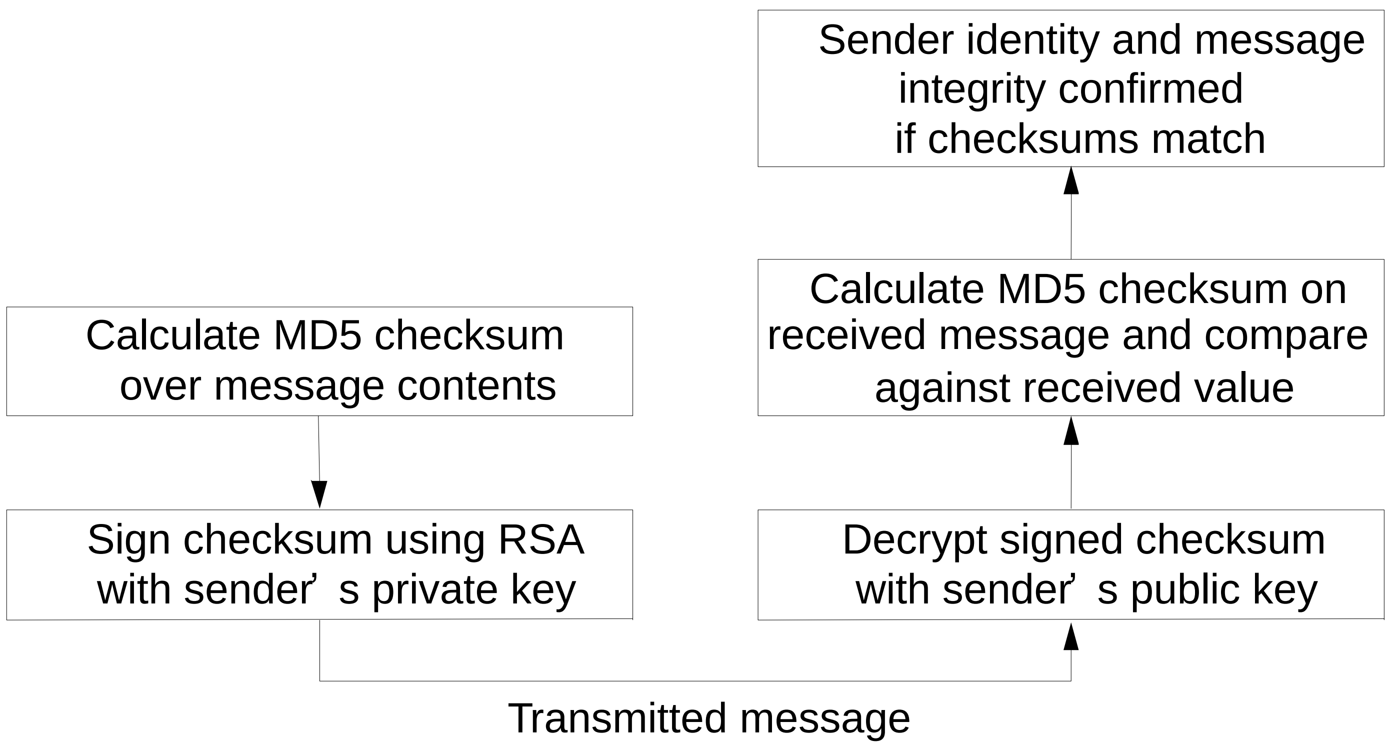
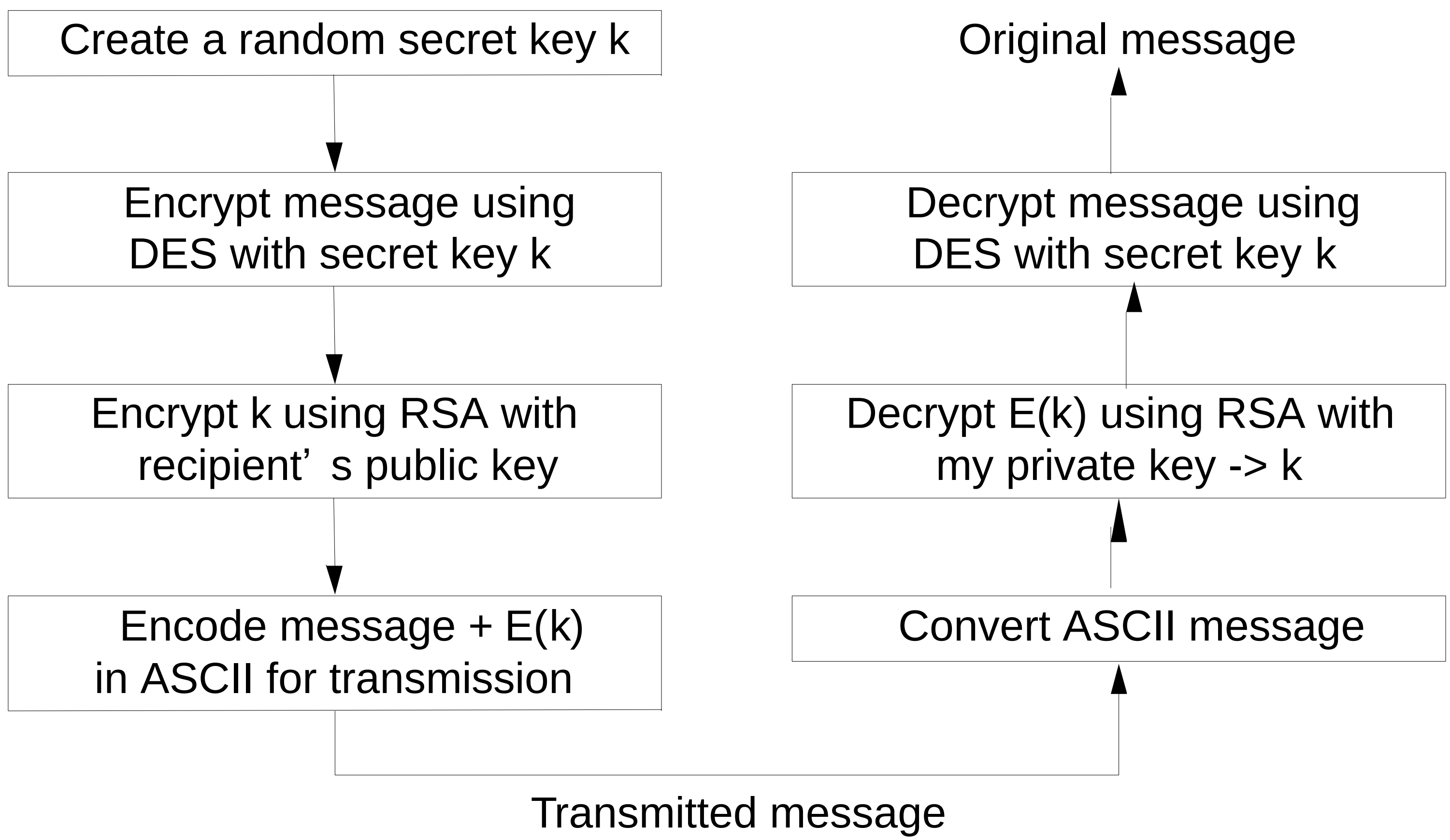


Figure 3.5 SHA-1 Processing of a Single 512-bit Block


Sender identity and message integrity confirmed if checksums match
Calculate MD5 checksum on received message and compare against received value
Calculate MD5 checksum over message contents
Sign checksum using RSA with sender’s private key
Decrypt signed checksum with sender’s public key
Transmitted message


Create a random secret key k
Encrypt message using DES with secret key k
Encrypt k using RSA with recipient’ s public key
Encode message + E(k) in ASCII for transmission
Transmitted message
Convert ASCII message
Decrypt E(k) using RSA with my private key -> k
Decrypt message using DES with secret key k
Original message

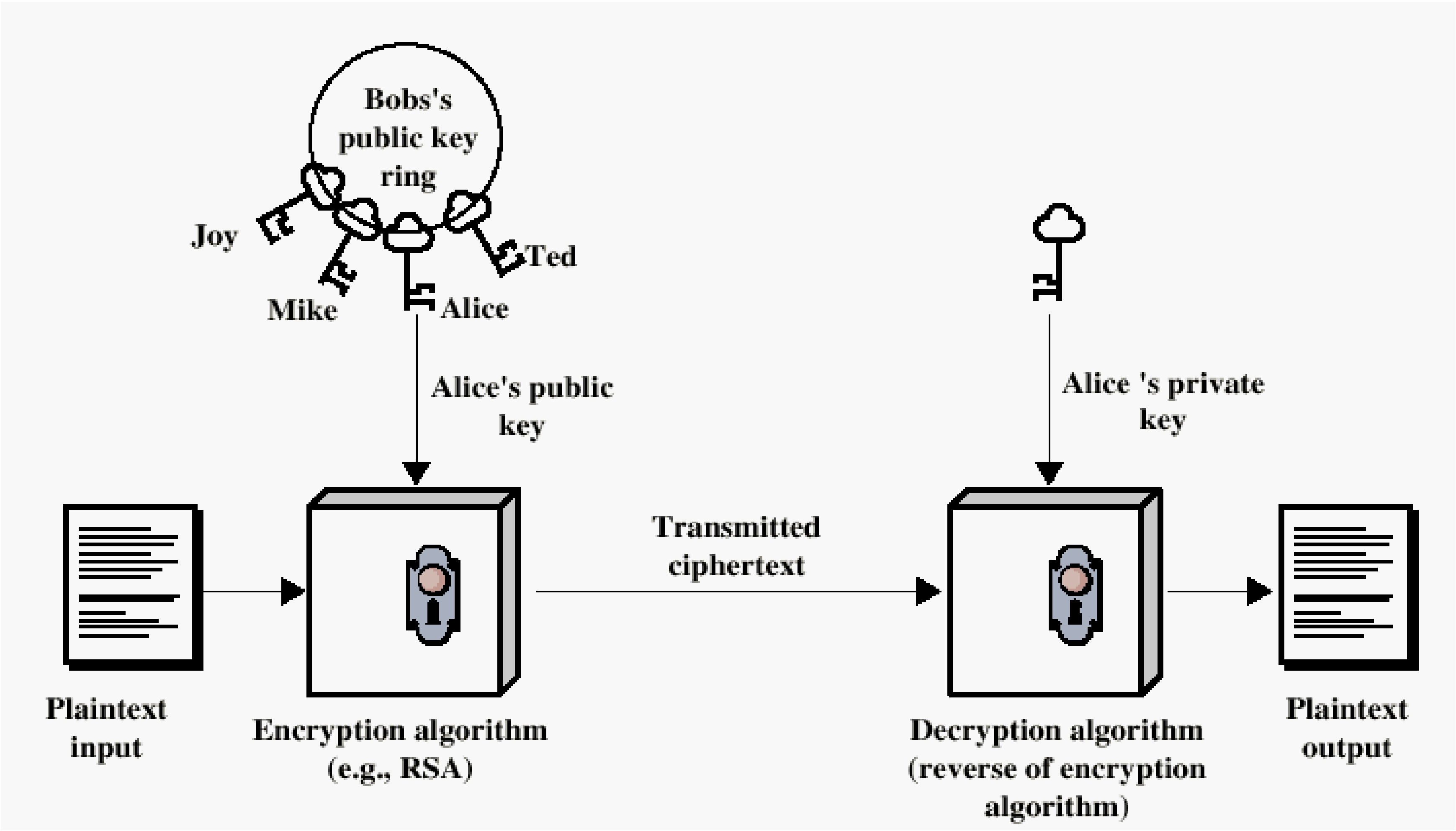
Week 4: Security

- Context: Attacks, services, & mechanisms
- Message encryption
- Public key cryptography
- Authentication protocols
- Message integrity
- **Public key infrastructure**
- Firewalls

Public-Key Cryptography Principles

- The use of two keys has consequences in: key distribution, confidentiality and authentication.
- The scheme has six ingredients
  - Plaintext
  - Encryption algorithm
  - Public and private key
  - Ciphertext
  - Decryption algorithm

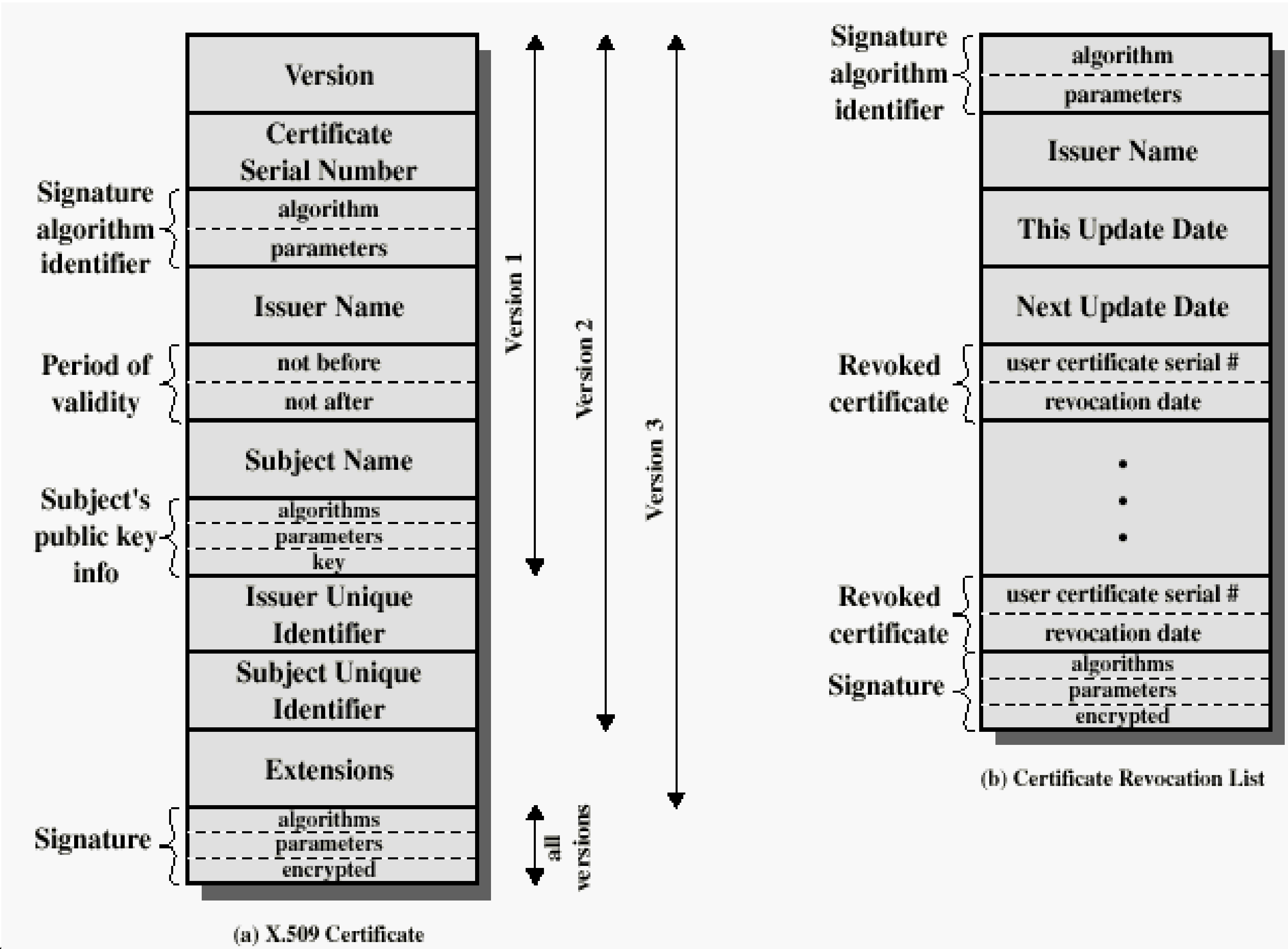
Encryption using Public-Key system



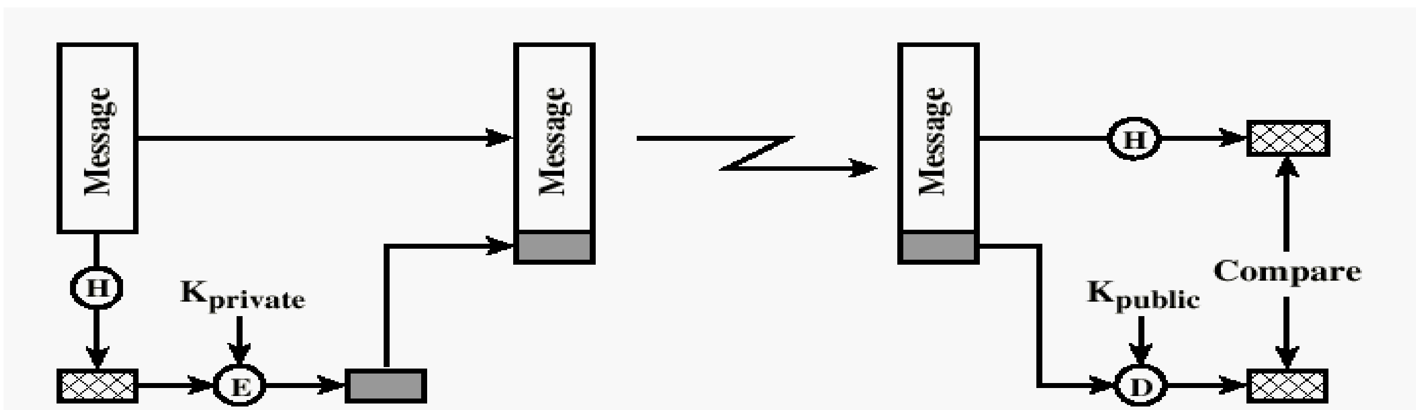
X.509 Authentication Service

- Distributed set of servers that maintains a database about users
- Each certificate contains the public key of a user and is signed with the private key of a CA
- Is used in S/MIME, IP Security, SSL/TLS and SET
- RSA is recommended

X.509 Formats



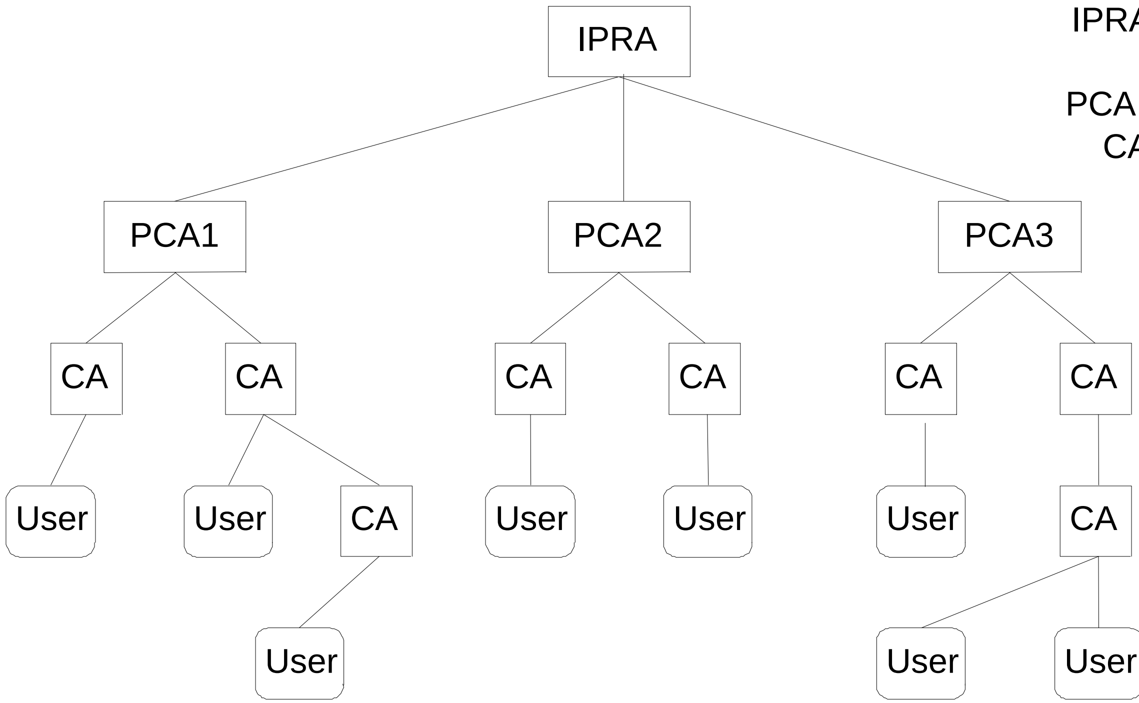
Typical Digital Signature Approach



(b) Using public-key encryption

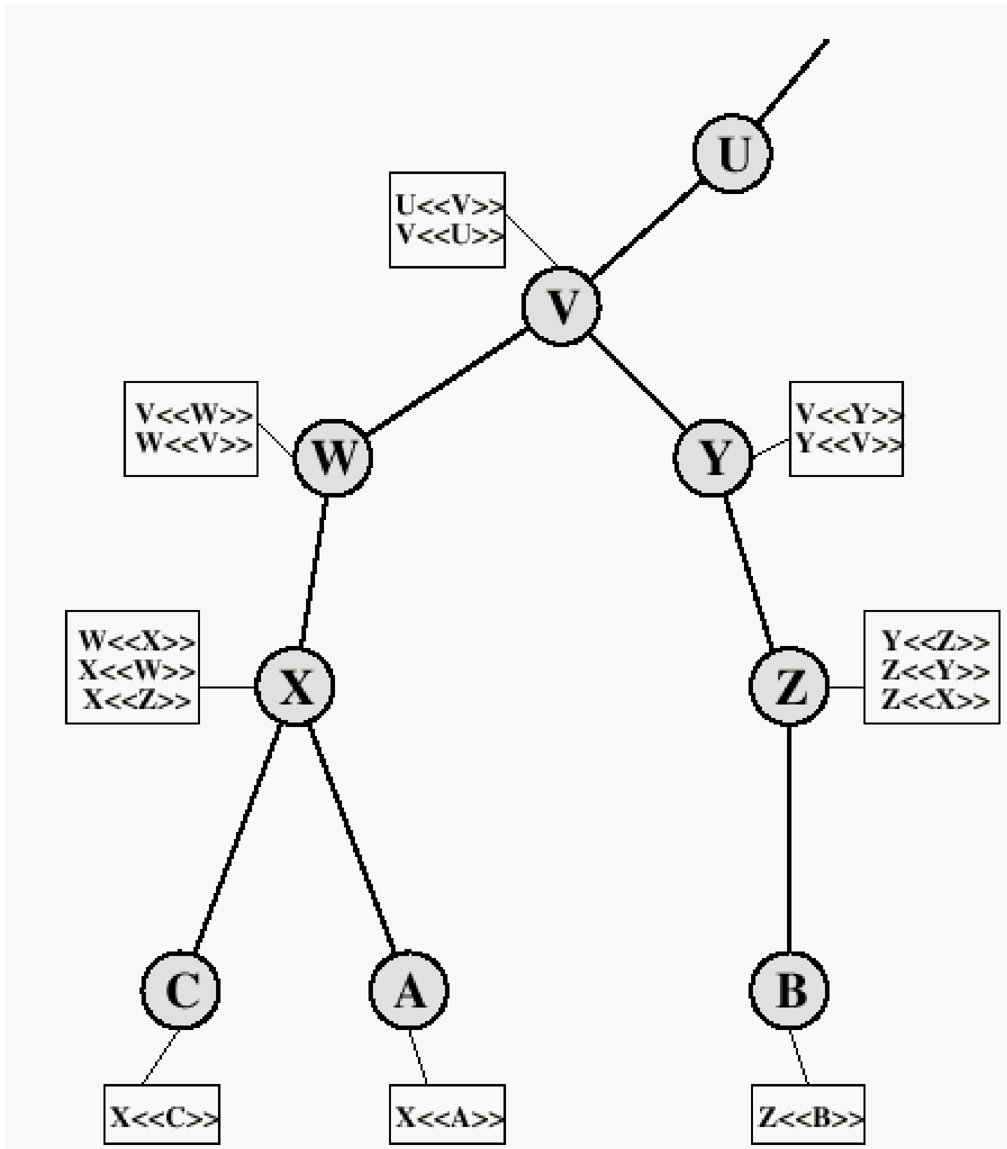
Obtaining a User's Certificate

- Characteristics of certificates generated by CA:
  - Any user with access to the public key of the CA can recover the user public key that was certified.
  - No part other than the CA can modify the certificate without this being detected.



IPRA = Internet Policy Registration Authority (root)
PCA n = policy certification authority
CA = certification authority

X.509 CA Hierarchy



Revocation of Certificates

- Reasons for revocation:
  - The users secret key is assumed to be compromised.
  - The user is no longer certified by this CA.
  - The CA's certificate is assumed to be compromised.

Week 4: Security

- Context: Attacks, services, & mechanisms
- Message encryption
- Public key cryptography
- Authentication protocols
- Message integrity
- Public key infrastructure
- **Firewalls**

Firewall Design Principles

- The firewall is inserted between the premises network and the Internet
- Aims:
  - Establish a controlled link
  - Protect the premises network from Internet-based attacks
  - Provide a single choke point

Firewall Characteristics

- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security police) will be allowed to pass
  - The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Four General Techniques

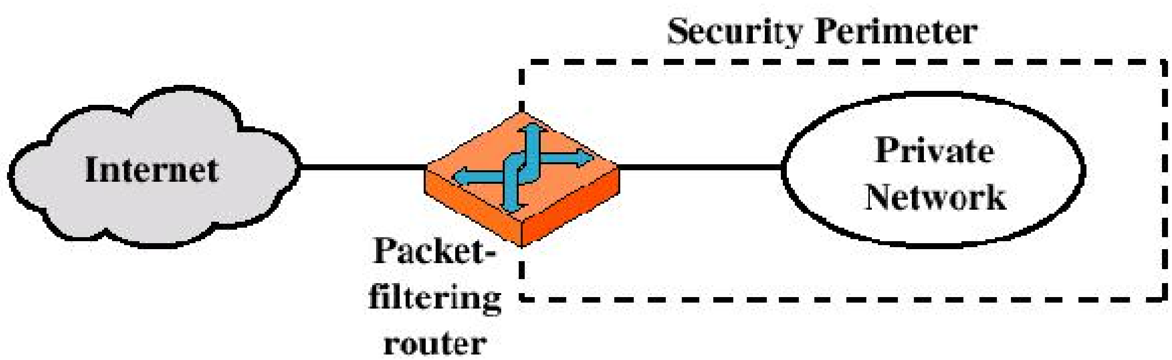
- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
- Direction control
  - Determines the direction in which particular service requests are allowed to flow
- User control
  - Controls access to a service according to which user is attempting to access it
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail)

Types of Firewalls

- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways
  - (Bastion host)

Types of Firewalls

- Packet-filtering Router



Types of Firewalls

- Packet-filtering Router
  - Applies a set of rules to each incoming IP packet and then forwards or discards the packet
  - Filter packets going in both directions
  - The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
  - Two default policies (discard or forward)

Types of Firewalls

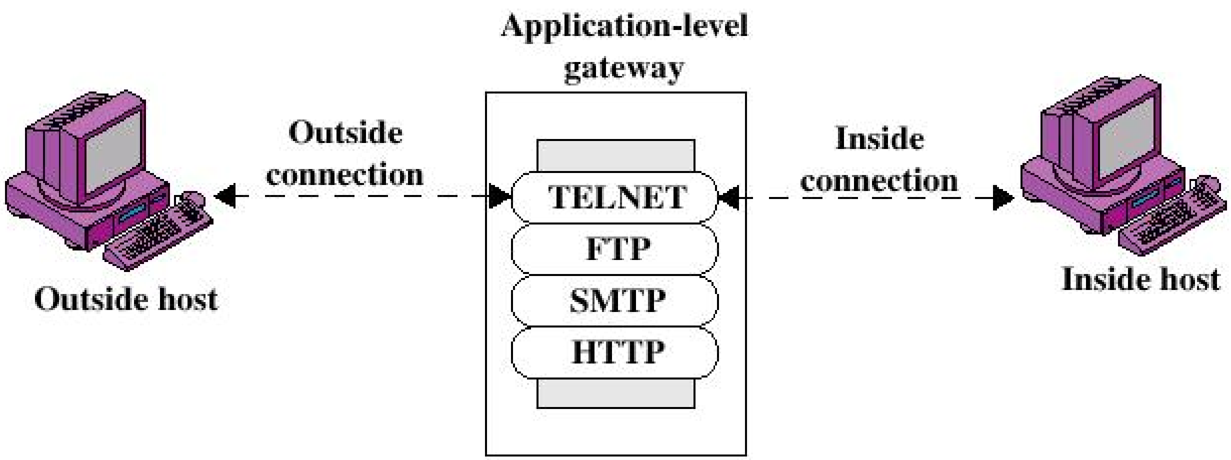
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

Types of Firewalls

- Possible attacks and appropriate countermeasures
  - IP address spoofing
  - Source routing attacks
  - Tiny fragment attacks

Types of Firewalls

- Application-level Gateway

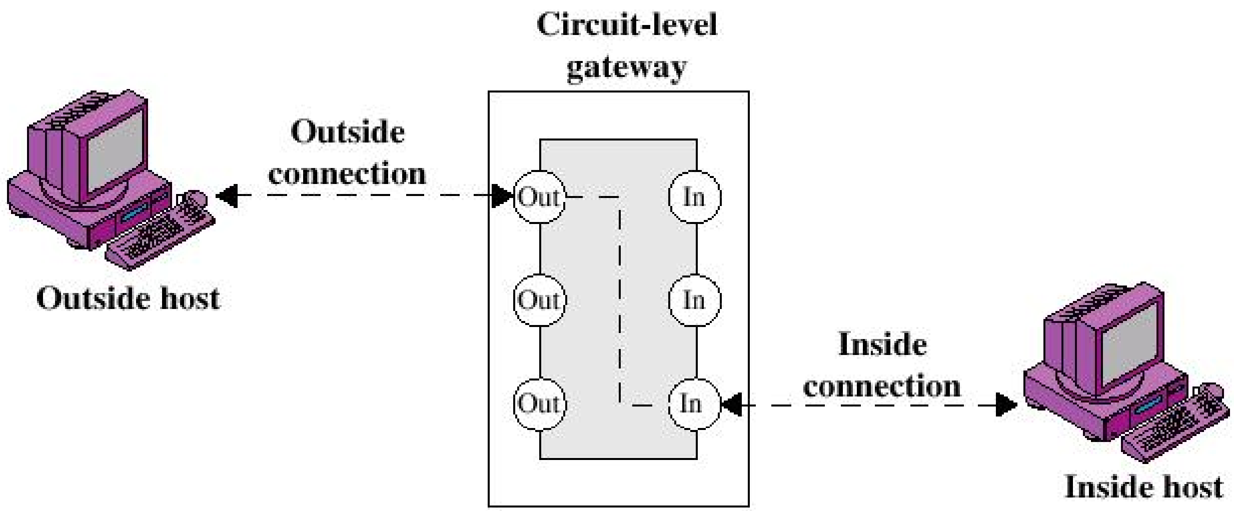


Types of Firewalls

- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic
- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

Types of Firewalls

- Circuit-level Gateway



Types of Firewalls

- Circuit-level Gateway
  - Stand-alone system or
  - Specialized function performed by an Application-level Gateway
  - Sets up two TCP connections
  - The gateway typically relays TCP segments from one connection to the other without examining the contents

Types of Firewalls

- Circuit-level Gateway
  - The security function consists of determining which connections will be allowed
  - Typically use is a situation in which the system administrator trusts the internal users
  - An example is the SOCKS package

Course Outline (Subject to Change)

1. (January 9th) Internet design principles and protocols
2. (January 16th) Internetworking, transport, routing
3. (January 23rd) Mapping the Internet and other networks
4. (January 30th) Security
5. (February 6th) P2P technologies & applications (Matei Ripeanu)
   (plus midterm)
6. (February 13th) Optical networks (Charlie Catlett)
7. *(February 20th) Web and Grid Services (Steve Tuecke)
8. (February 27th) Network operations (Greg Jackson)
9. *(March 6th) Advanced applications (with guest lecturers: Terry Disz, Mike Wilde)
10. (March 13th) Final exam

* Ian Foster is out of town.