ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA

Review
Cryptography & Network Security

MSc. NGUYEN CAO DAT

- Principles of modern ciphers
- Implement crypto library
- Network Security Applications
- System Security

Outline

- Introduction
- Basics of Cryptography
- Network Security Applications
- System Security

Introduction

- OSI Security Architecture
  - Defines a systematic way of defining and providing security requirements
  - ITU-T X.800
  - Focuses on security attacks, mechanisms and services.

Introduction

- Security Attack
  - Any action that compromises the security of information owned by an organization
  - Types of attacks
- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack.

Introduction

- Security service
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
  - The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Introduction

- Questions and Problems
  - Questions: 1.1, 1.2, 1.3
  - Problems: 1.1, 1.2

Outline

- Introduction
- Basics of Cryptography
  - Symmetric cipher
  - Public key cryptography
  - Message authentication
  - Digital signatures

Symmetric cipher

Symmetric cipher model

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = E_K(X)$

  $X = D_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Symmetric cipher

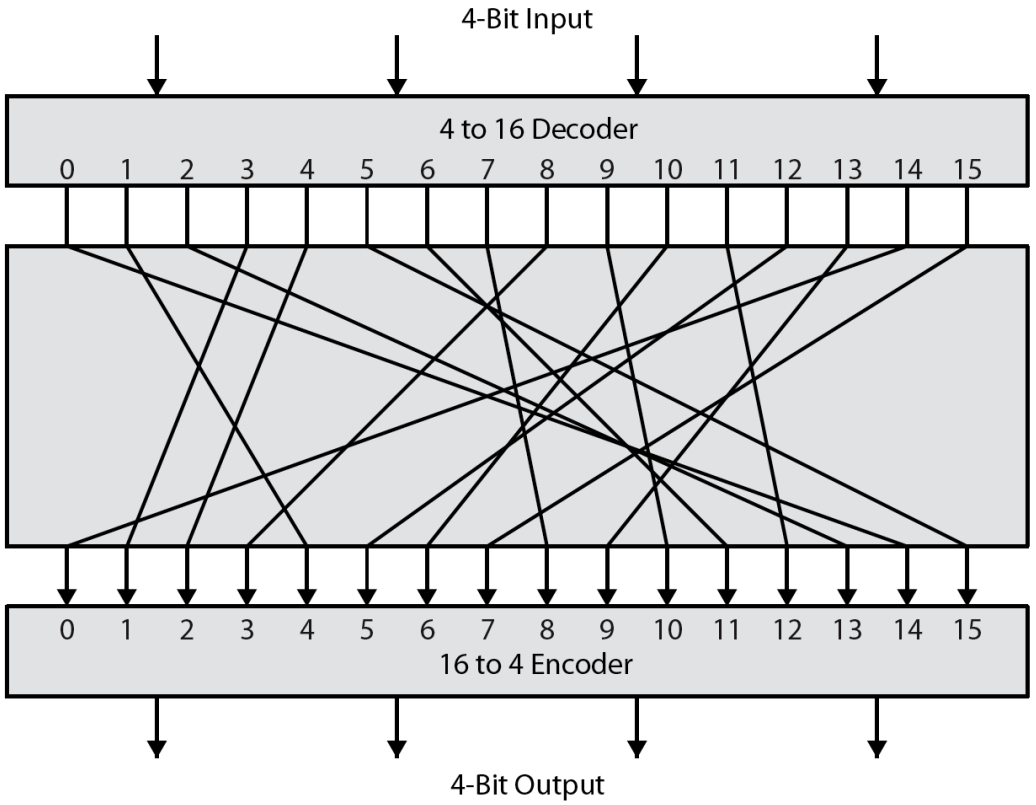
- Classical encryption techniques
  - Substitution Techniques
    - The letters of plaintext are replaced by other letters or by numbers or symbols.
    - Caesar cipher, Monoalphabetic ciphers
    - Playfair cipher, Hill cipher
  - Transposition Techniques
    - Perform some sort of permutation on the plaintext
  - Product Ciphers

Symmetric cipher

- Block ciphers
  - Process messages in blocks, each of which is then en/decrypted
- Stream ciphers
  - Process messages a bit or byte at a time when en/decrypting

Symmetric cipher

- Ideal Block Cipher

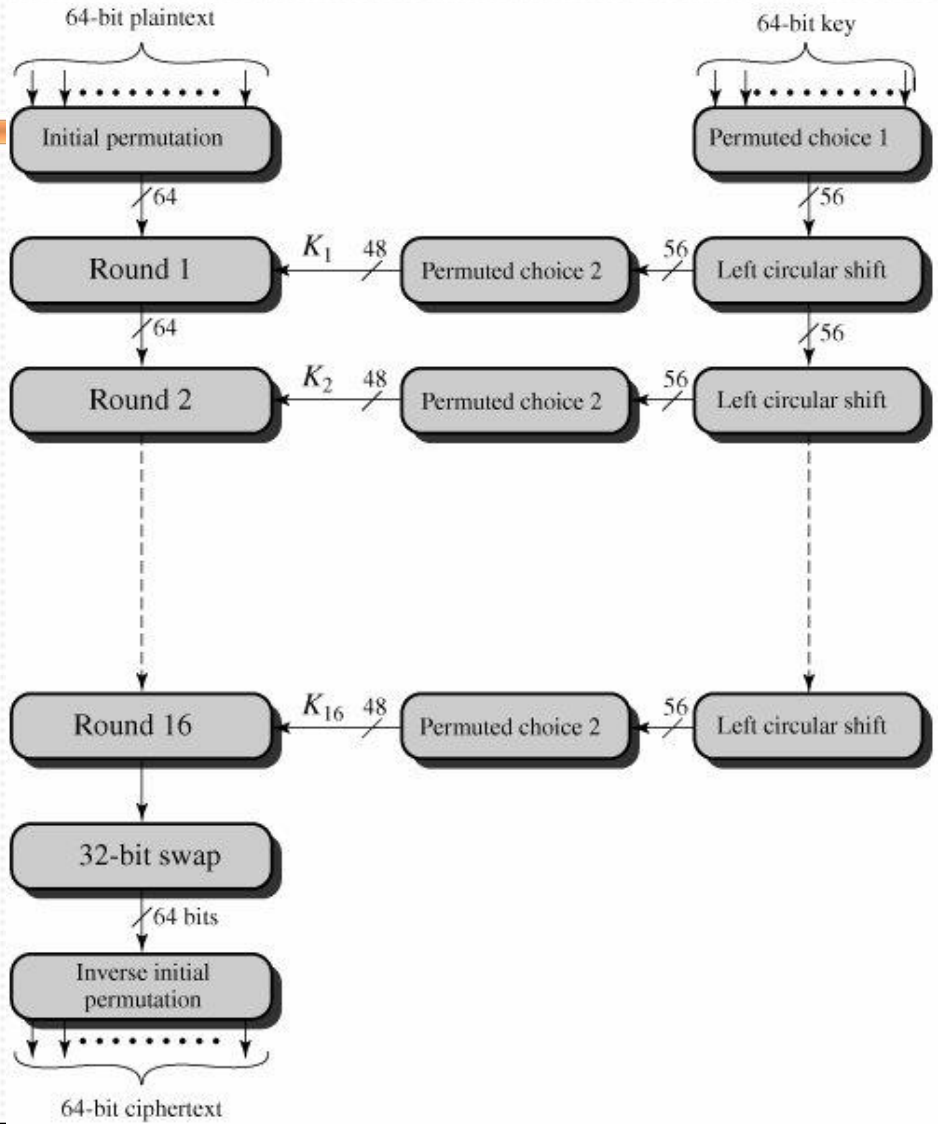


Symmetric cipher

- Modern Block Cipher
  - Substitution-permutation (S-P) networks
    - *substitution* (S-box)
    - *permutation* (P-box)
- Diffusion
  - Make the statistical relationship between the plaintext and ciphertext as complex as possible.
- Confusion
  - Make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible.

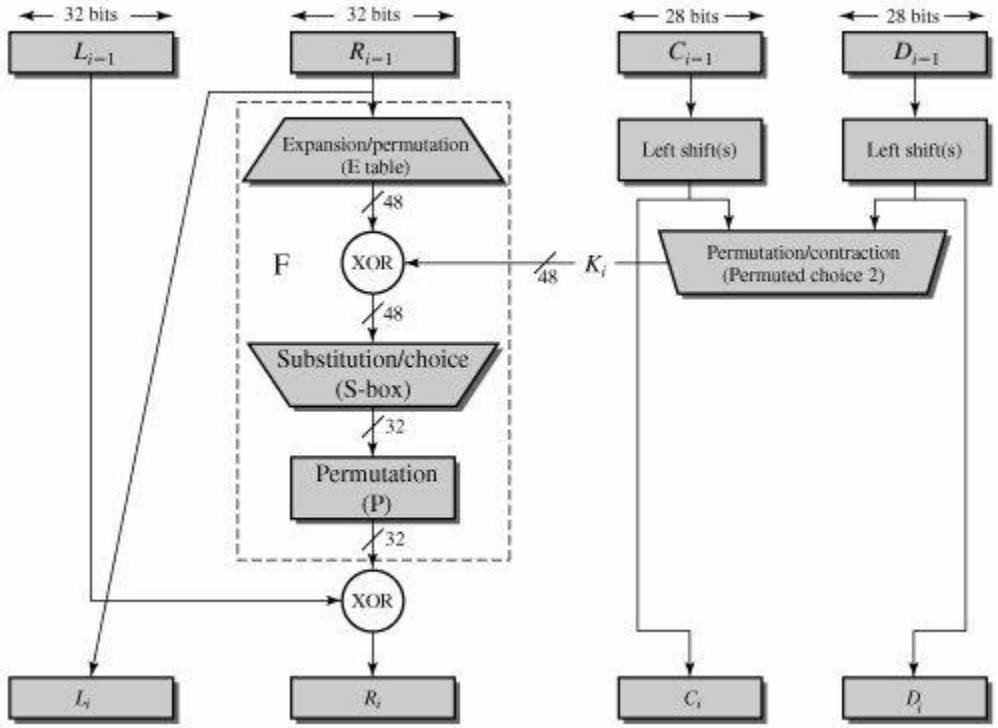
Symmetric cipher

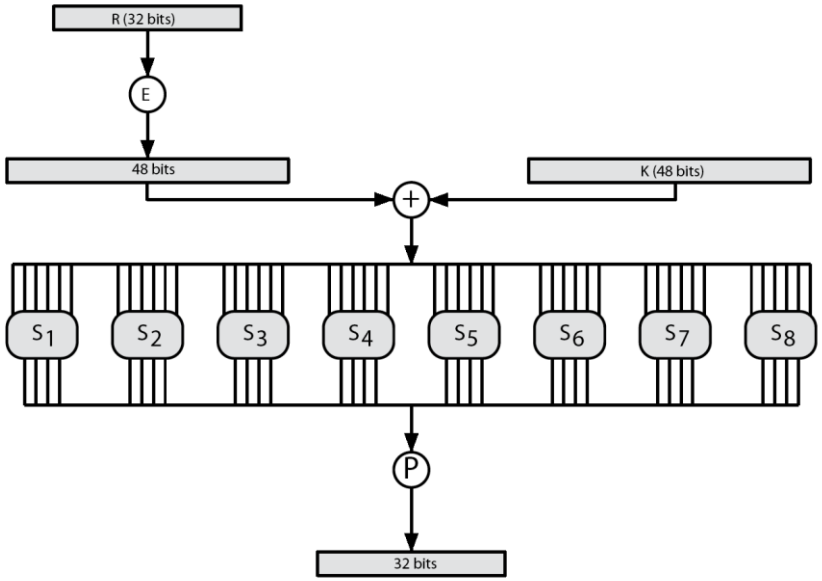
- DES



Symmetric cipher

- DES





Symmetric cipher

- Questions
  - 2.1 – 2.9, 2.13
  - 3.1 – 3.9
  - Problems
    - 2.1, 2.5
    - 3.2, 3.5 - 3.7

Public key cryptography

Number Theory

- Basic theorem of arithmetic (every number can be a product of prime powers), LCM, GCD.
- Computing GCD using the Euclidean Algorithm (Chapter 4.3)
- Modular arithmetic operations (Chapter 4.2)
- Computing modular multiplicative inverse using extended Euclidean Algorithm (Chapter 4.4)

Public key cryptography

Number Theory

- Arithmetic in a finite ring or field
  $Z_m = \{0, 1, \cdots, m-1\}$
- If m is prime, the ring is a field
- Possible to perform additions, multiplication
- Multiplicative inverses
- In a field all numbers have a multiplicative inverse(except zero)
- In a ring only number relatively prime to the modulus have a multiplicative inverse

Public key cryptography

Number Theory

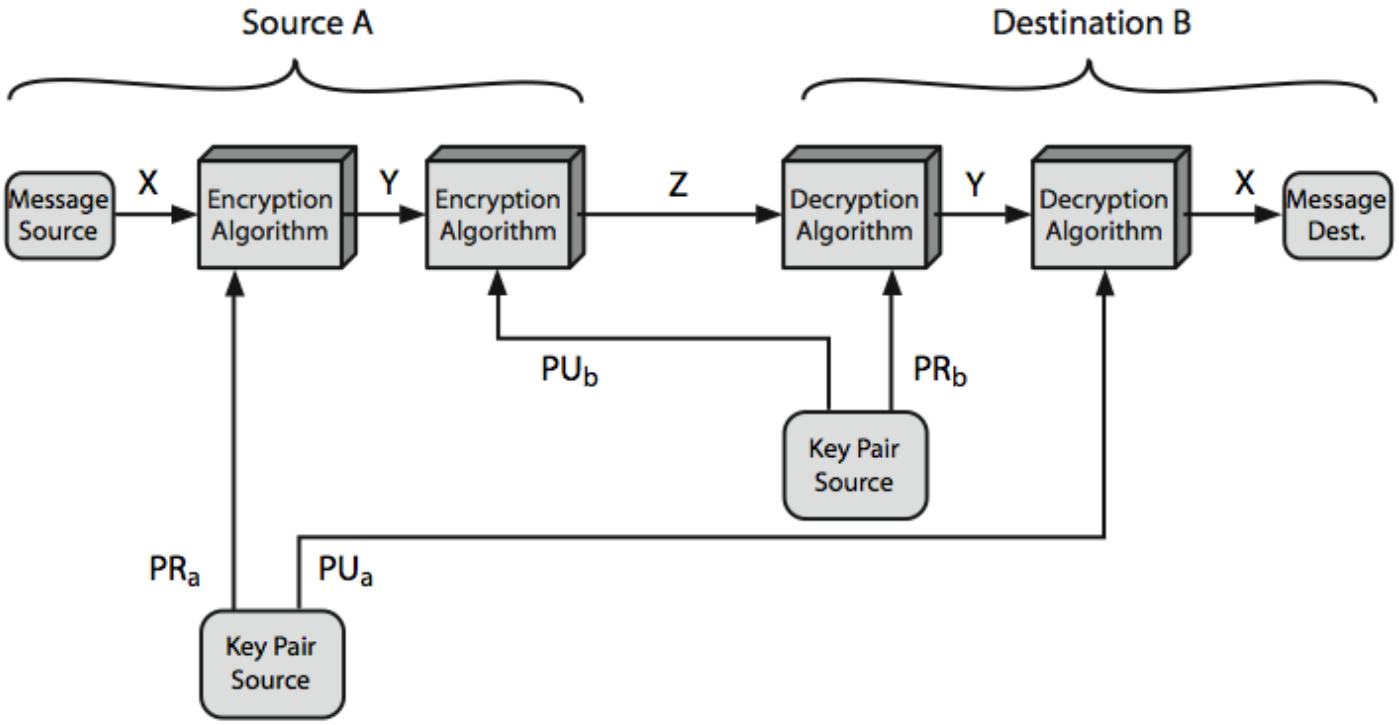
- Fermat's theorem: $a^{p-1} \bmod p \equiv 1$
- Euler - Phi Function (m) - number of numbers below m relatively prime to m.
- Euler's theorem: $a^{\phi(m)} \bmod m \equiv 1$ if GCD(a , m) = 1.

Public key cryptography

- Hard problems
  - Factorization
    - Given two primes p and q finding n = pq is trivial.
    - But given n finding p and / or q is not.
  - Discrete Logarithms
    - Let $y = g^x \bmod p$. Given x, g and p easy to calculate .
    - But given y, g and p practically impossible to calculate x for large p.

Public key cryptography

- Public-Key Cryptosystems



Public key cryptography

- RSA - (Rivest - Shamir - Adelman)
  - Choose two large primes p and q.
  - n = pq is the modulus (Z_n is a ring - not a field)
  - $\phi(n) = (p - 1)(q - 1)$.
  - Choose e such that (e, (n)) = 1.
  - Find d such that $de \equiv 1 \bmod \phi(n)$ (use extended Euclidean algorithm)
  - Destroy p, q and $\phi(n)$.
  - PU = (n,e) are public key; PR= (n,d)
  - Cannot determine p and q from n (factorization is hard).
  - Cannot determine $\phi(n)$ without factoring n.
  - So finding d given e (and n) is hard.

Public key cryptography

- RSA - (Rivest - Shamir - Adelman)
  - Key Generation

    PU = (e,n)

    PR= (d,n)
  - Encryption

    $C = M^e \bmod n$, where $0 \le M < n$
  - Decryption

    $M = C^d \bmod n$

Public key cryptography

Diffie Helman Key Exchange

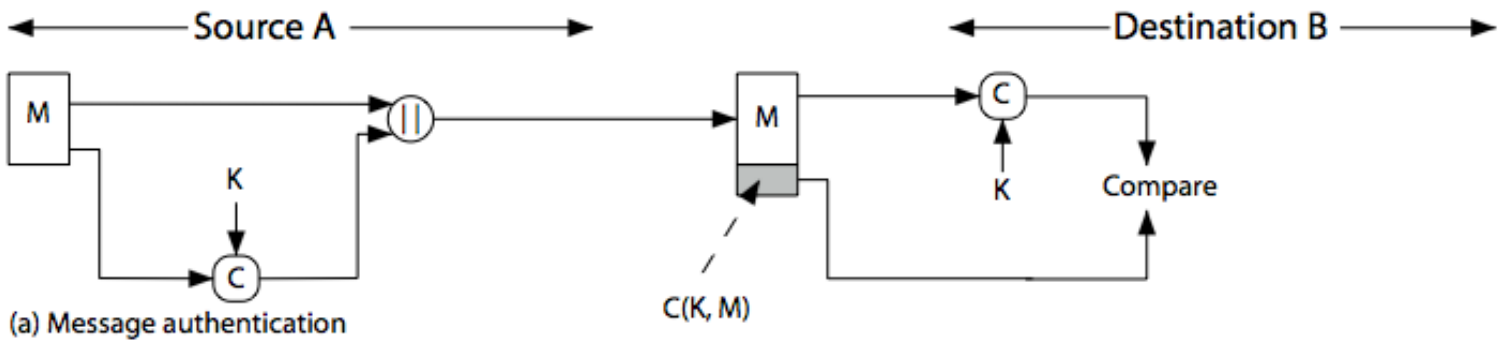
- DH is based on difficulty of calculating discrete logarithms
- A known p, and (preferably) a generator g in Z_p.
- Alice chooses a secret a, calculates $\alpha = g^a \bmod p$.
- Bob chooses a secret b, calculates $\beta = g^b \bmod p$.
- Alice and Bob exchange and
- Alice calculates $K_{AB} = \beta^a \bmod p$.
- Bob calculates $K_{AB} = \alpha^b \bmod p$.
- Both of them arrive at $K_{AB} = g^{ab} \bmod p$.
- K_{AB} is a secret that no one apart from Alice and Bob can calculate!

Public key cryptography

- Questions
  - 8.1 – 8.5
  - 9.1 – 9.3
- Problems
  - 8.4 – 8.8
  - 9.2 – 9.4
  - 10.1 – 10.2

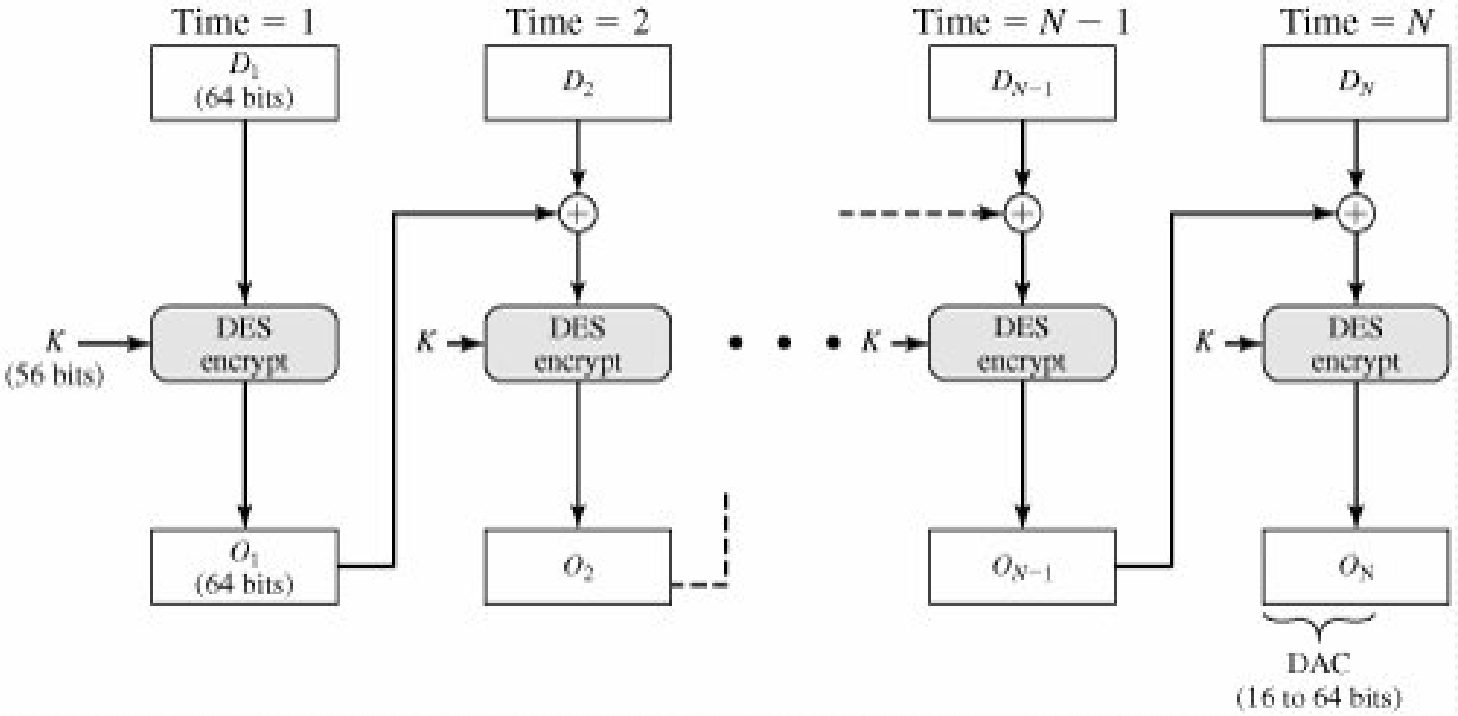
Message Authentication

- Message Authentication Code



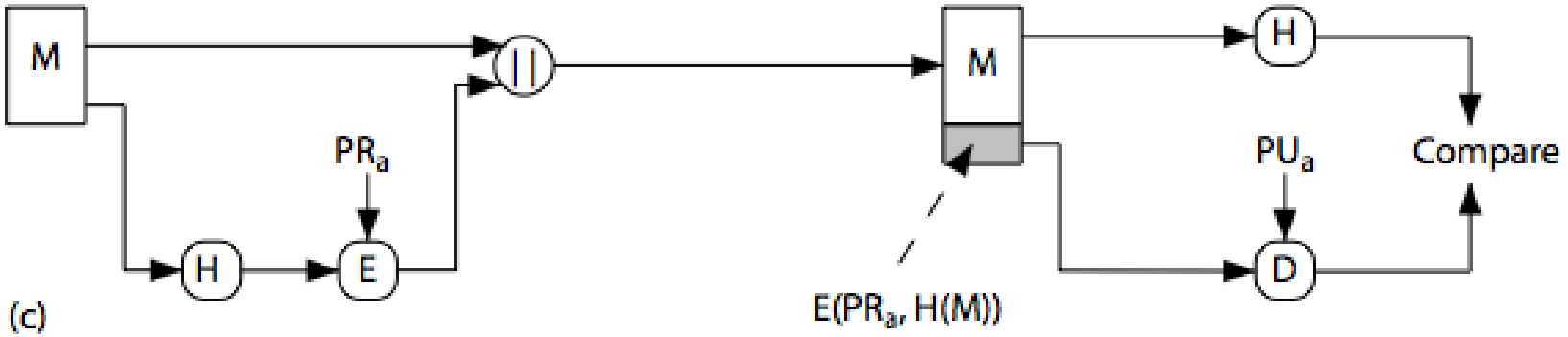
Message Authentication

- Message Authentication Code
  - Data Authentication Algorithm



Message Authentication

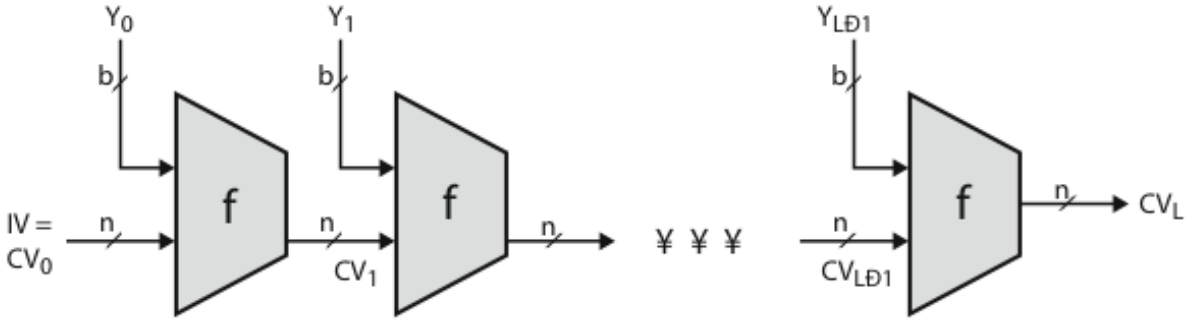
- Hash functions
  - Hash Functions & Digital Signatures



Message Authentication

Hash functions

Modern Hash Functions



IV = Initial value
CV_i = chaining variable
Y_i = ith input block
f = compression algorithm

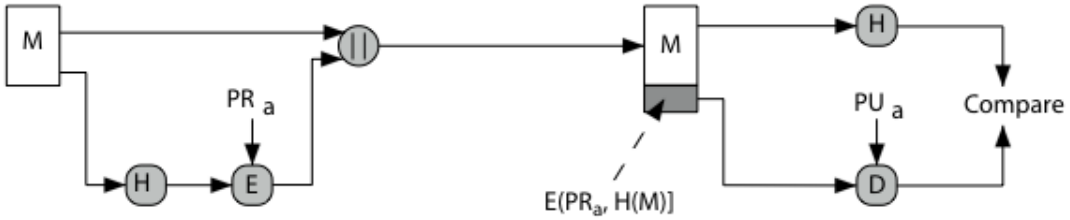
L = number of input blocks
n = length of hash code
b = length of input block

Message Authentication

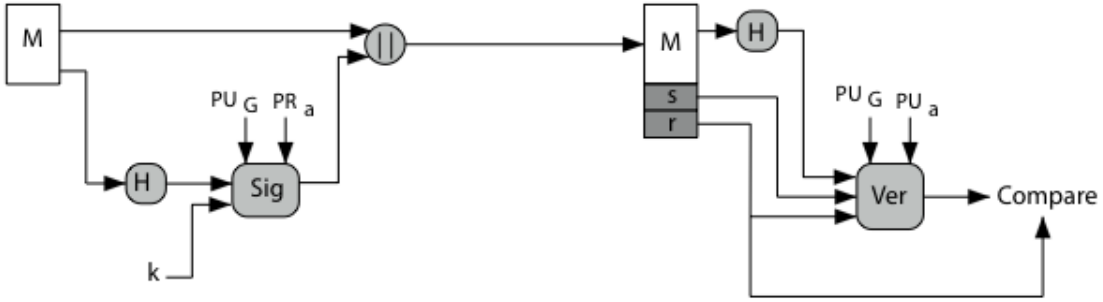
- Questions
  - 11.1 – 11.7
  - 12.2
- Problems
  - 12.2 - 12.3

Digital Signatures

Practical Signature Schemes



(a) RSA Approach



(b) DSS Approach

Digital Signatures

- Distribution of Public Keys
  - public announcement
  - publicly available directory
  - public-key authority
  - public-key certificates

Digital Signatures

- PKI - Public Key Infrastructure
  - X.509 Authentication service
  - Based on asymmetric cryptography
  - Basic function - authentication of public keys
  - Achieved by signing public keys
  - Public key certificates issued by certifying authorities (CA)
  - Permits different public key algorithms
  - Revocation of certificates

Digital Signatures

- PKI - Public Key Infrastructure
  - X.509 Authentication service
  - Based on asymmetric cryptography
  - Basic function - authentication of public keys
  - Achieved by signing public keys
  - Public key certificates issued by certifying authorities (CA)
  - Permits different public key algorithms
  - Revocation of certificates

Digital Signatures

- Questions
  - 10.1 – 10.5
  - 13.7 – 13.9
- Problems
  - 13.3

Outline

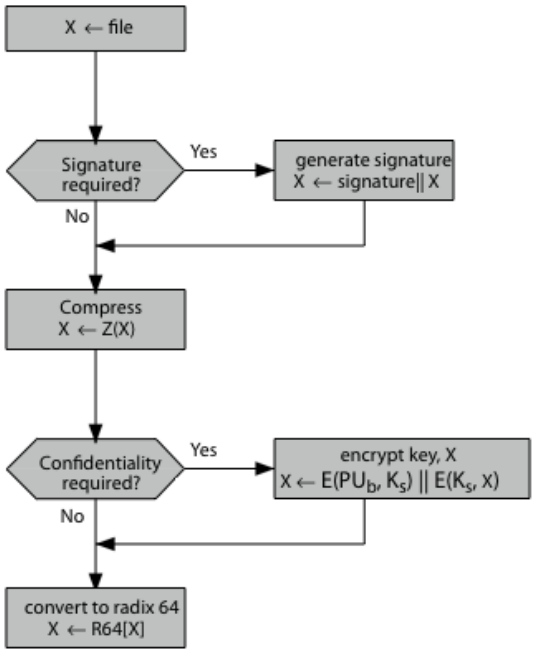
- Introduction
- Basics of Cryptography
- Network Security Applications
  - E-mail Security
  - Web Security
  - IP Security
- System Security

E-mail Security

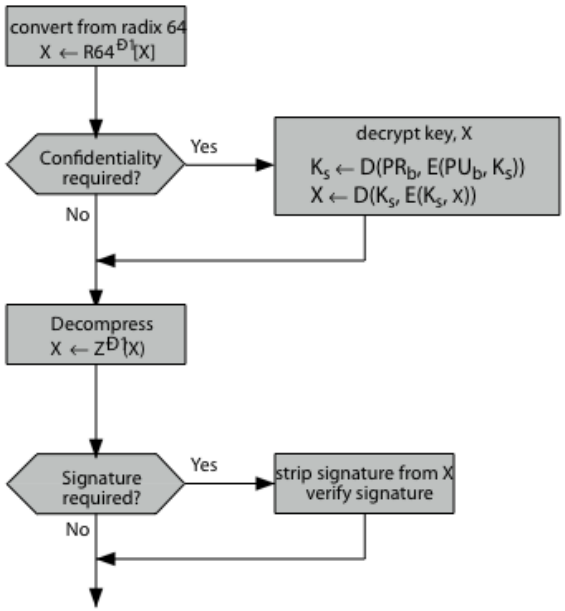
- Email Security Enhancements
  - confidentiality
  - authentication
  - message integrity
  - non-repudiation

E-mail Security

Pretty Good Privacy (PGP)



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

E-mail Security

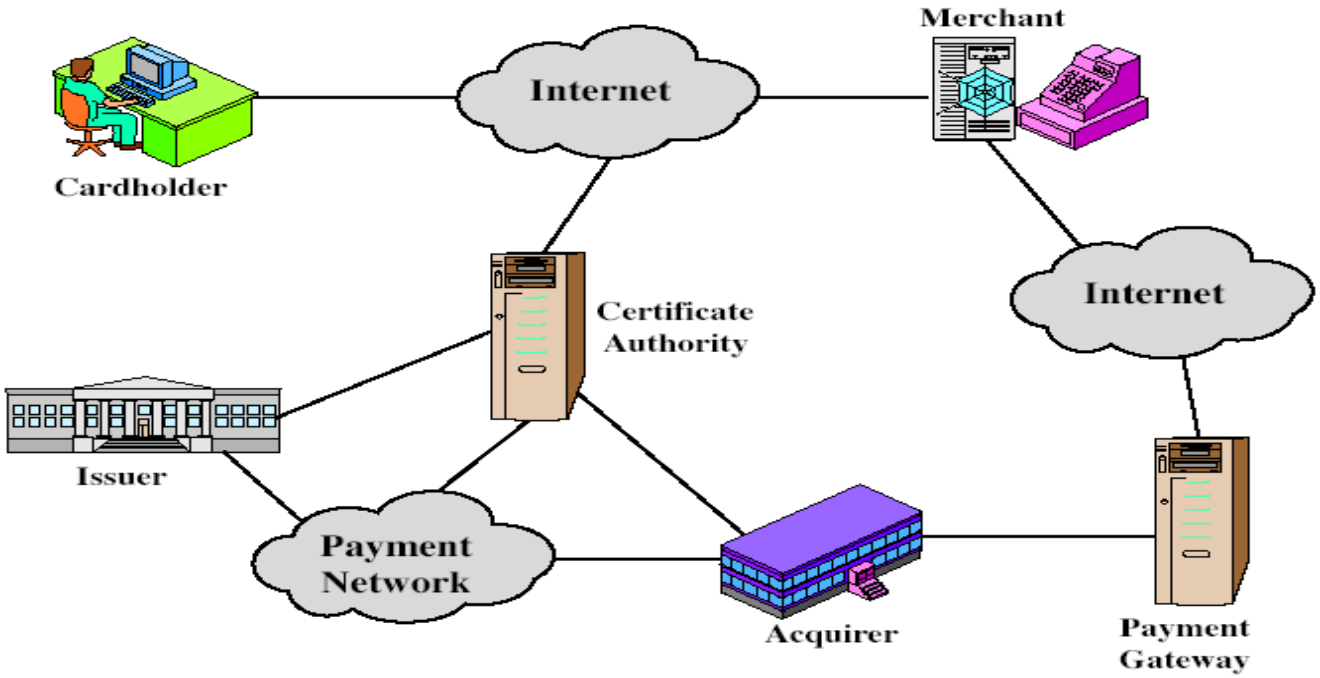
- Questions
  - Why does PGP generate a signature before applying compression
  - How does PGP use the concept of trust
- Problems
  - 15.1
  - 15.2
  - 15.3

Web Security

- Web Security Threats
  - integrity
  - confidentiality
  - denial of service
  - Authentication
- SSL (Secure Socket Layer)
  - SSL Record Protocol
  - SSL Change Cipher Spec Protocol
  - SSL Alert Protocol
  - SSL Handshake Protocol

Web Security

- Secure Electronic Transactions (SET)



Web Security

- Questions
  - What is the difference between an SSL connection and an SSL session
  - List and briefly define the parameters that define an SSL connection
  - List and briefly define the principal categories of SET participants
  - What is a dual signature and what is its purpose
- Problems
  - 17.1, 17.2

IP Security

- IPSec Services
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality
- IPSec modes
  - Transport Mode
  - Tunnel Mode

IP Security

- Questions
  - What services are provided by IPSec
  - What is the difference between transport mode and tunnel mode
  - Why does ESP include a padding field
- Problems
  - 16.2
  - 16.3

Outline

- Introduction
- Basics of Cryptography
- Network Security Applications
- System Security
  - Intruders & IDS
  - Firewalls

System Security

- Intruders & IDS
  - Intrusion Techniques
  - Approaches to Intrusion Detection
    - statistical anomaly detection
    - rule-based detection
    - Distributed Intrusion Detection

System Security

Intruders & IDS

- Questions
  - List and briefly define three classes of intruders.
  - What are two common techniques used to protect a password file?
  - What are three benefits that can be provided by an intrusion detection system?
  - What is the difference between statistical anomaly detection and rule-based intrusion detection?
- Problems
  - 18.5, 18.6

System Security

- Firewalls
  - a **choke point** of control and monitoring
  - Firewall Basic Types
  - Firewall Configurations

System Security

- Firewalls
  - Questions
    - List three design goals for a firewall
    - What are some weaknesses of a packet-filtering router?
    - What is the difference between a packet-filtering router and a stateful inspection firewall?
    - What are the differences among the three configurations of Figure 20.2?
  - Problems
    - 20.2
    - 20.3