Information Protection and Security

KR Chowdhary, Professor & Head
Email: kr.chowdhary@ieee.org

Department of Computer Science and Engineering
MBM Engineering College, Jodhpur

Objective

In order to build a secure system, designers must first decide exactly what "secure" means for their particular need. In a private company secrecy may be related to nondisclosure of confidential accounting data or trade secrets, or to the enforcements of privacy regulations regarding personal, medical, or credit records.

Security services

Information and network security risks are increasing with the growth of the number of threats and sophisticated attacks.

- A user U_A, transmits a file to U_B. User U_H (not authorized to access the file) captures a copy of the file during transmission.
- A network manager Man_D, transmits a message to a networked computer Com_E to grant accesses / authorizations for new users. U_H intercepts the message, alters it and forwards to Com_E.
- A message sent from customer U_A to stockbrocker U_B to execute some transactions. U_H intercepts and sends several copies.
- An employee Y is terminated. The personal manager sends message to server to invalidate $Y's$ account. Y delays the message, and retrieves the sensitive information before message reaches.

Aspects of security needs

Need of a systematic way of defining the requirements for security and characterizing the approaches to satisfy the requirements.

- Identify Security attacks
- Identify Security mechanisms
- Identify Security services

Security Services

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Access-control
- Denial of Service (availability Function)
- Spoofing

Security Attacks

- Interruption
- Interception
- Passive v/s active
- Single source v/s multi-source attacks

  Vulnerabilities: Flaw that allows an unauthorized user to read another user's files, regardless of permissions, or some other kind of the flaw in the system.

Protections

- Security policies
  a. Access policy
  b. Accountability policy
  c. Authentication policy
  d. Availability Policy
  e. Maintenance policy
  f. Violation reporting policy

Protection of users and networks

- Protection of Employees

  a. Shared key encryption schemes

  b. Hash Functions. Hash function H generates $H(m)$ for every variable-length message m. $H(m)$ is message digest

  c. Digital Signature: Binding an information to an originator.

- Protection of networks:

  a. Firewalls

  b. Access, authorization, and authentication tools

  c. Intrusion detection systems

Cryptography

- Method of sending messages in disguised form, so that only the intended recipients can remove the disguise and read the messages.
- Terms:*plain text, cipher text, cryptosystem*

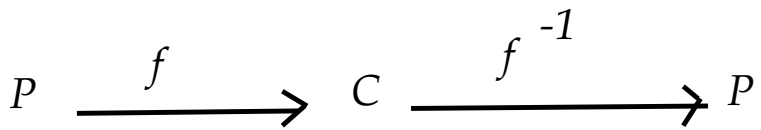


Figure: Cryptosystem

- To facilitate rapid enciphering/deciphering, there should be simple rules.
- For example: $A-Z \Longleftrightarrow 0-25$. Let $p \in \{0,\ldots,25\}$ is plain-text, and f is from $\{0,1,\ldots,25\}$ to itself:

Some Examples of secrecy systems

- Simple Substitution Cipher (Letter of the message is replaced by a fixed substitute) $M = m_1 m_2 \ldots$, where m_1, m_2 are the successive letters, becomes:
  $E = e_1 e_2 \cdots = f(m_1) f(m_2) \ldots$
- Transposition (Fixed Period d): The message is divided into groups of length d and a permutation applied to the first group, the same permutation to the second group, etc.
  Thus for d = 5, we might have 2 3 1 5 4 as the permutation. This means that:
  $m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8 m_9 m_{10} \ldots$ becomes
  $m_2 m_3 m_1 m_5 m_4 m_7 m_8 m_6 m_{10} m_9 \ldots$

Symmetric Encryption

- Secret-key encryption: Message space M, key space K, cipher space C, two maps (encryption and decryption).

$$\phi : M \times K \to C$$

$$\gamma : C \times K \to M.$$

- Both functions must satisfy:

$$\phi(\gamma(c,k),k) = c$$

and

$$\gamma(\phi(m,k),k) = m$$

One way function for all k: $\phi(-,k) : M \to C$
One way function for all m: $\phi(m,-) : K \to C$

Model of secret-key cryptosystem

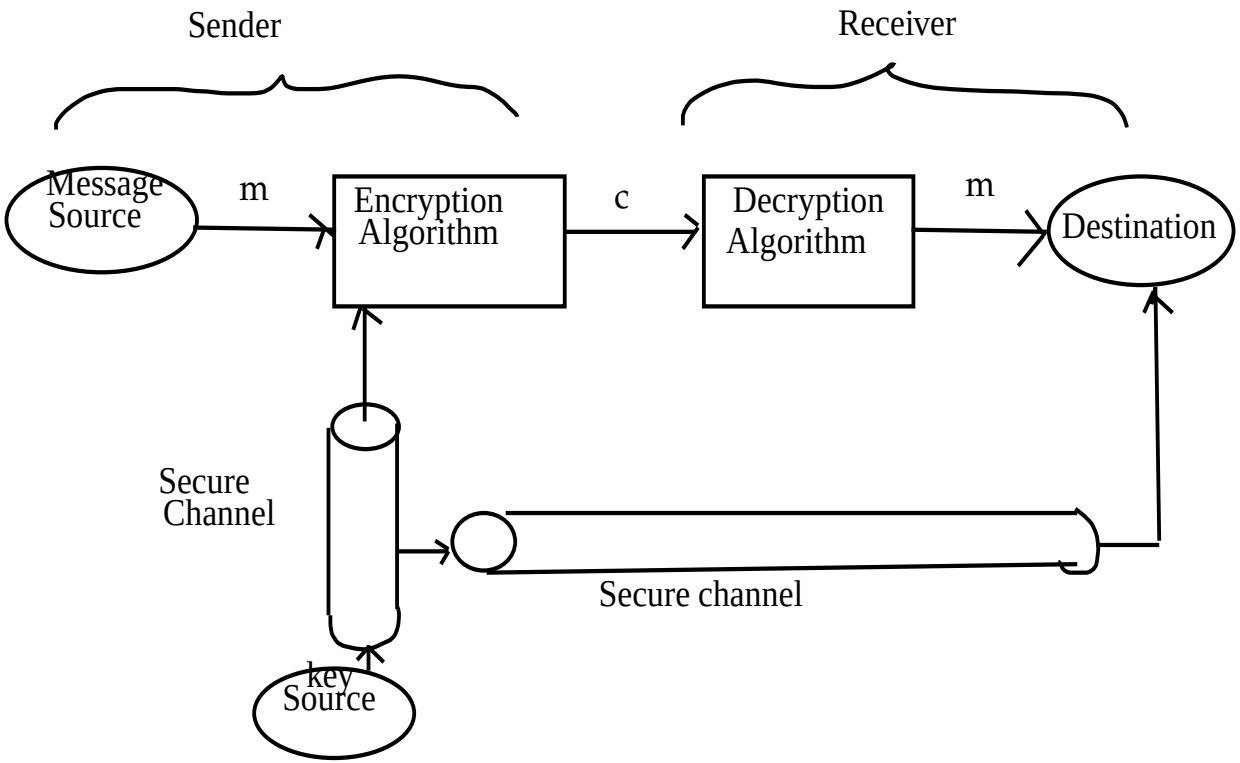


Figure: Secret-key Cryptosystem

Public-key cryptosystem

- User U_b wants to send a secret message to U_a. K_b is public, K_a is secret (in possession of U_a).
- There is a function:

$$\alpha : C \to C \text{ such that } \gamma(\phi(m, \alpha(k)), k) = m$$

and

$$\phi(\gamma(c, k), \alpha(k)) = c$$

- $(\alpha(k), k)$ are pair of private and public keys, and α is link between private and public keys.

Model of Public-key cryptosystem

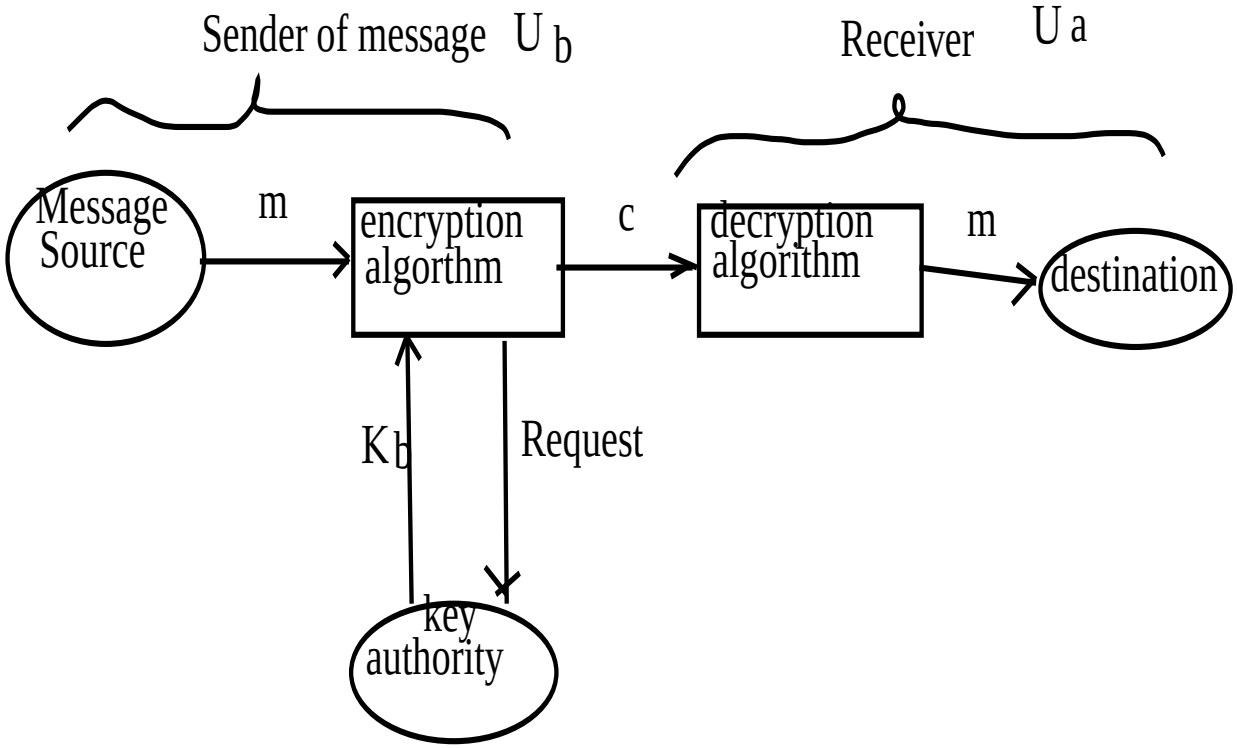


Figure: Public-key Cryptosystem

Public-key main algorithm

RSA Algorithm:

- Block cypher; Plain-text, cipher-text are 0 to $n-1$.
- Two interchangeable keys d (private) and (n, e) (public-key).
- Plain-text block m having value less than n is encrypted/decrypted as:
  $c = m^d \bmod n$, and $m = c^e \bmod n$.
- e is selected such that: $(m^e)^d \bmod n = m$,
  $e.d = k\phi(n) + 1$, $\phi(n)$ is Euler Function.
- let p=17, q=13,
  $\therefore n = pq$=221,$\phi(n) = 192, d = 5, e = 77$,
- Let $m = 6, \therefore, c = 6^5 mod 221 = 41$. is encryption, and $m = 41^{77} mod 221 = 6$ is decryption.

Valuation of cryptosystems

- Amount of Secrecy
- Size of Key
- Complexity of Enciphering and Deciphering Operations
- Propagation of Errors
- Expansion of Message

Other Formal models

Lattice Model for secure information flow

- Lattice: Finite Set + Partial Ordering relation, such that for every pair there is least upper bound and greatest lower bound.
- $(S, \leq)$ is POSET.

Linear ordered lattice

$$S = \{A_1, A_2, \ldots, A_n\}$$

$$A_i \rightarrow A_j \text{iff } A_i \leq A_j$$

$$A_i \oplus A_j = A_{max}(i, j)$$

$$A_i \otimes A_j = A_{min}(i, j)$$

$$L = A_1; H = A_n.$$

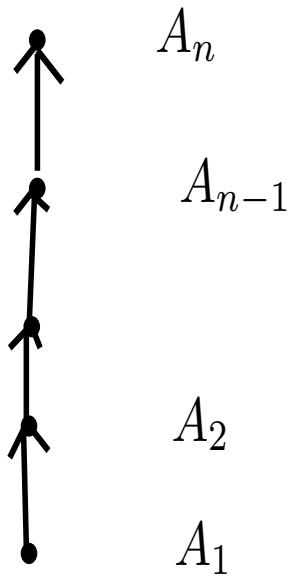
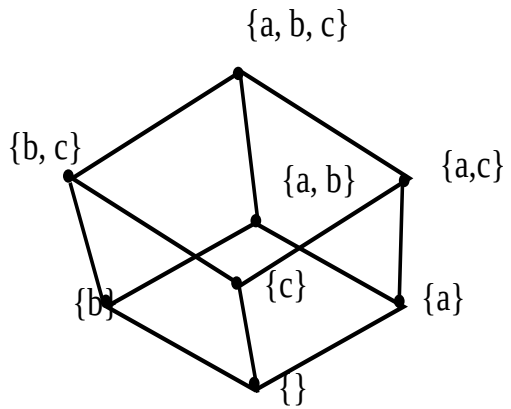


Figure: Linear ordered lattice

Nonlinear lattice model

- It is richer structure; classes are hierarchically ordered.
- Suitable for providing security at different levels (Govt. & Military) or objects in programs, and OS.
- Information may be: unclassified, confidential, secret, top secret.

$$A \to B, (iff) A \subseteq B$$
$$A \oplus B = A \cup B$$
$$A \otimes B = A \cap B$$
$$L = \phi; H = S$$



Lattice Structure for (P(S), <=)
S={a, b, c}

Access Matrix Model

- Three principle components: *(1) Set of passive objects*, *(2) set of active subjects* (which manipulate other objects), and *(3) set of rules governing manipulation of objects by subjects*.
- Objects: files, terminals, devices. Subjects: Processes (every subject may be also an object, hence it may be manipulated by other subjects).
- Entry for a row-column reflects the mode of access and ownership for subject-object

Conclusion

- No security protection mechanism is perfect yet.
- It is claimed that quantum cryptography, which is based on the quantum state of particles, will be a strong cryptosystem, and shall be impossible to break.
- On the other side, as the processing power of CPUs are increasing constantly, and 100 core processors are not far off, it will be easier to break the encryption easier using multiple desktops using these systems.