CS 8792 - CRYPTOGRAPHY AND NETWORK SECURITY

UNIT- I

INTRODUCTION

Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of Network security - Security attacks, services and mechanisms - OSI Security architecture - classical encryption techniques: Substitution techniques, transposition techniques, steganography - Foundations of modern cryptography : perfect Security - information theory - product cryptosystem - cryptanalysis.

INTRODUCTION

Network Security:

* The security provided to a network from unauthorized access and risks.
* It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Types of Network Security Devices:

1. Active Devices:

* Block the surplus traffic

EX:

* Firewalls
* Antiviruses scanning devices.
* Content Filtering devices.

2. Passive Devices:

* Identify and report on unwanted traffic.

EX:

* Intrusion detection appliances.

3. Preventive Devices:

* Devices scan the networks and identify potential security problems.

EX:

* Penetration testing devices.
* Vulnerability Assessment appliances.

4. Unified Threat Management:

* Serve as all-in-one security devices.

EX:

* Firewalls, content filtering, web caching etc.

Goals of Network Security.

* It aims to ensure that the entire network is secure.

→ Network security involves protecting the usability, reliability, integrity and safety of network and data.

* Effective network security defeats a variety of threats from entering or spreading on a network.

→ The primary goal of network security is confidentiality, Integrity and Availability.

→ Represented as CIA Triangle.

1) Confidentiality:

- Two concepts.

i) Data confidentiality:

- Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

ii) Privacy:

- Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

2) Integrity:

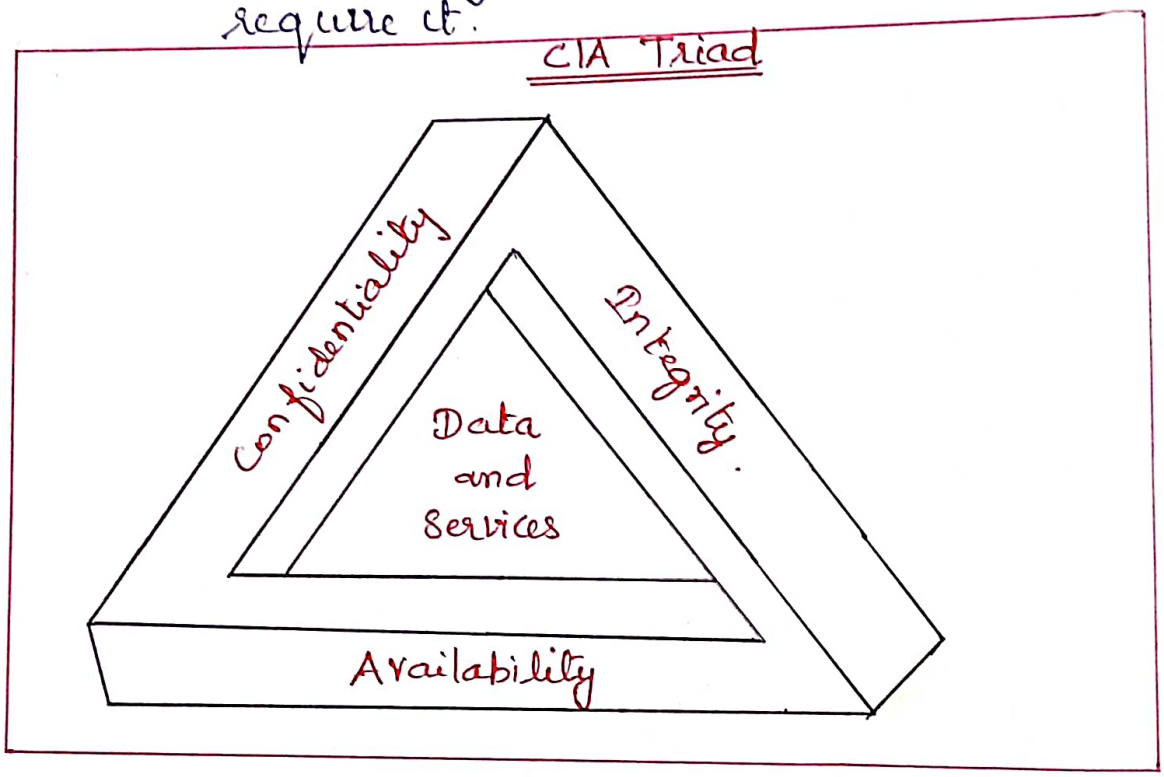
- Maintaining and assuring the accuracy and consistency of data.

i) Data Integrity:

- Assures that information and programs are changed only in a specified and authorized manner.

ii) System Integrity:
- Assures that a system performs its intended function in an proper manner.

3) Availability:
- To make sure that the data, network resources / services are continuously available to the legitimate users, whenever they require it.



Computer Security:
* Collection of tools designed to protect data and to the hackers.

Network Security:
* Measures to protect data during their transmission

Internet Security:
* Measures to protect data during their transmission over a collection of interconnected networks.

Basic Concepts: cryptology - Both Cryptography and Cryptanalysis.

cryptography:

* The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then retransforming that message back to its original form.

Plain Text:

* original intelligible message.

Cipher Text:

* Transformed message.

Cipher:

* An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods.

Key:

* Critical information used by the cipher, known only on the sender & receiver.

Encipher: (Encode)

* Process of converting plaintext to cipher text using a cipher and a key.

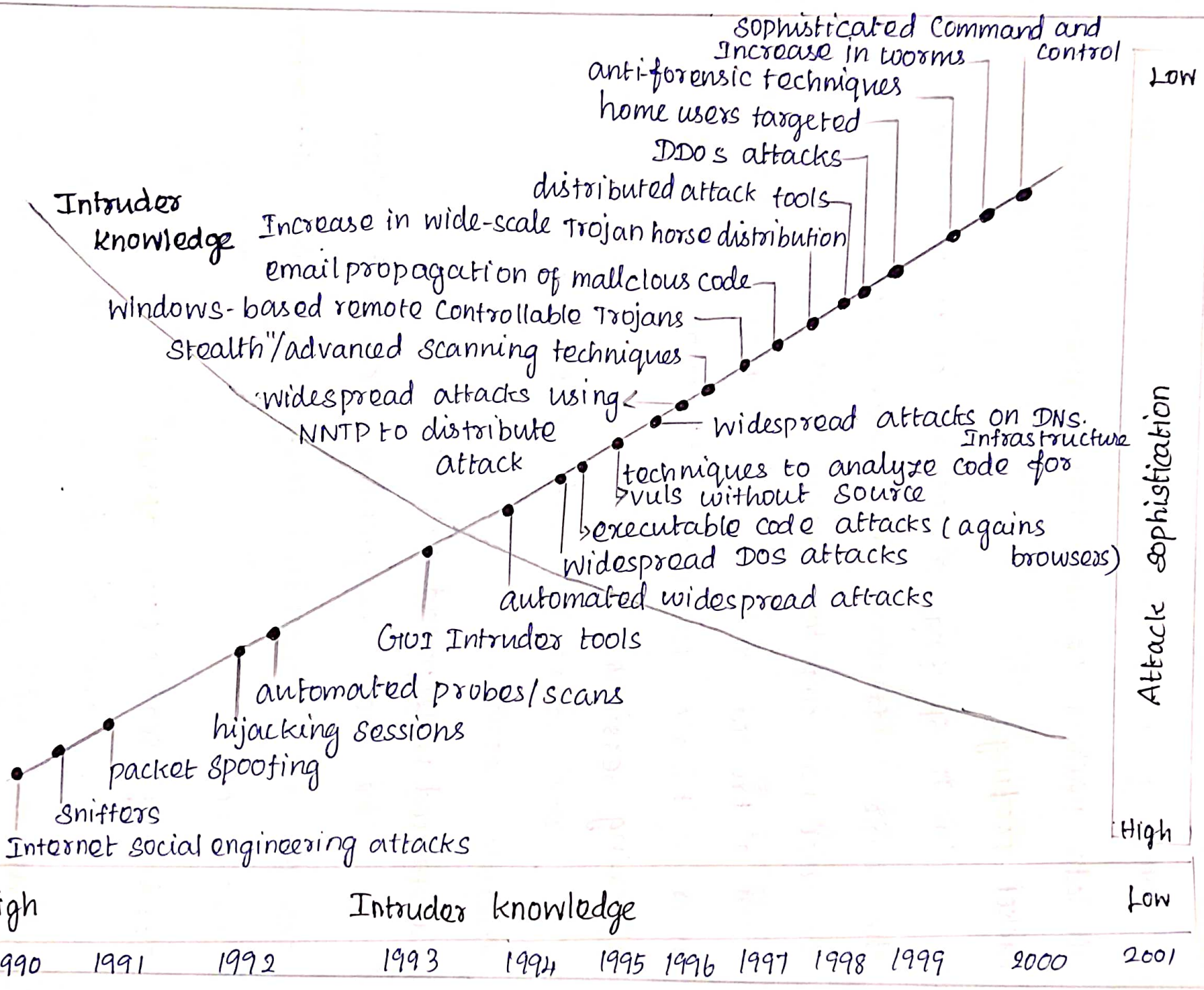
Decipher: (Decode)

* Process of converting cipher text back into plaintext using a cipher and a key.

cryptanalysis: (code breaking)

* Study of principles & methods of transforming an unintelligible message back into an intelligible message without knowledge of the key.

Code: → Algm for transforming an intelligible message into an unintelligible one using a code-book.


Sophisticated Command and control
Increase in worms
anti-forensic techniques
home users targeted
DDOS attacks
distributed attack tools
Increase in wide-scale Trojan horse distribution
email propagation of mallclous code
Windows-based remote Controllable Trojans
Stealth"/advanced scanning techniques
widespread attacks using NNTP to distribute attack
widespread attacks on DNS. Infrastructure
techniques to analyze code for vuls without source
executable code attacks (agains browsers)
Widespread DOS attacks
automated widespread attacks
GUI Intruder tools
automated probes/scans
hijacking sessions
packet spoofing
Sniffers
Internet social engineering attacks
Intruder knowledge
Low
High
Attack sophistication
High
Intruder knowledge
Low
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001

Sniffers :-

Sniffing is a process of monitoring and capturing all data packets passing through given network

Packet spoofing :-

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it.

hijacking sessions :-

Cookie hijacking is the exploitation of a valid computer session.

automated widespread attacks :-

The most frequently used automated attacks are : Credential stuffing. Scraping. Application layer DDOS.

Denial-of-service (DOS) attack :

A Denial-of-service attack is an attack meant to shutdown a machine or network, making it inaccessible to its intended users.

Executable code attacks:

The classic example is an email attachment containing malicious executable code.

Vuls attack:

Vuls is an open-source, agentless vulnerability scanner written in Go. It automates security vulnerability analysis of the software installed on a system, which can be a burdensome task for system administrators to do manually in a production environment.

Widespread attacks on DNS Infrastructure:

Hijacking huge volumes of email passwords and other sensitive data from multiple governments and private companies.

NNTP - Network News Transfer protocol

"stealth"/advanced scanning techniques:

Stealth - Robbery

port scanning - used to list open ports and services.

Network scanning - used to list IP addresses

Vulnerability scanning - used to discover the presence of known vulnerabilities.

Windows-based remote Controllable Trojans :

Trojan is a type of malware that is often disguised as legitimate software.

email propagation of malicious code :

Once inside your environment, malicious code can enter network drives and propagate. Malicious code can also cause network and mail server overload by sending email messages; stealing data and passwords; deleting document files, email files or passwords; and even reformatting hard drives

Distributed attack tools :

LOIC (Low Orbit Ion Canon) LOIC is one of the most popular DOS attacking tools freely available on the Internet.

- XOIC. XOIC is another nice DOS attacking tool
- HULK (HTTP Unbearable load king)
- DDOSIM - Layer 7 DDOS Simulator
- R-U-Dead-yet
- Tor's Hammer
- PyLoris
- OWASP DOS HTTP POST

Home users targeted:

Many Internet-connected copiers and printers use this protocol

Anti-forensic techniques:

Facinating Anti-Forensic Techniques to cover Digital Footprints.

Steganography: steganography is the act of Concealing data in plain sight.

Tunneling
Onion Routing
Obfuscation
spoofing

Increase in worms:

Worms can modify and delete files, and they can even inject additional malicious software onto a computer.

Sophisticated Command and control:

A Command-and-control [C&C] server is a Computer controlled by an attacker or cybercriminal which is used to send commands to systems Compromised by malware and receive stolen data from a target network.

TOP Trends in 2020:

Growing Attacks of Ransomware & phishing.
Integrating AI, & ML to Counter Security Threats
Expanding Cloud Security Threats
Mounting Mobile Apps Security Risks
Increasing Attacks on IOT Devices
Striking Cyber-Security Skills Gap
Increasing Investments in Cyber-Security.

1.2 LEGAL, ETHICAL AND PROFESSIONAL ASPECTS OF SECURITY

1. Cybercrime and Computer Crime

Computer crime or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.

These categories are not exclusive, and many activities can be characterized as falling in one or more categories.

The term cybercrime has a connotation of the use of networks specifically, whereas computer crime may or may not involve networks.

Types of Computer Crime

- **Computers as targets:** This form of crime targets a computer system, to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server.
- **Computers as storage devices:** computers can be used to further unlawful activity by using a computer or a computer device as a passive storage medium. For example, the computer can be used to store stolen password lists credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software).
- **Computers as communications tools:** Many of the crimes falling within this category are simply traditional crimes that are committed online. Examples: Illegal Sale of Prescription Drugs, Controlled Substances, Alcohol, and Guns; Fraud; Gambling; and Child Pornography.

Law Enforcement Challenges

The deterrent effect of law enforcement on computer and network attacks correlates with the success rate of criminal arrest and prosecution. The nature of cybercrime is such that consistent success is extraordinarily difficult.

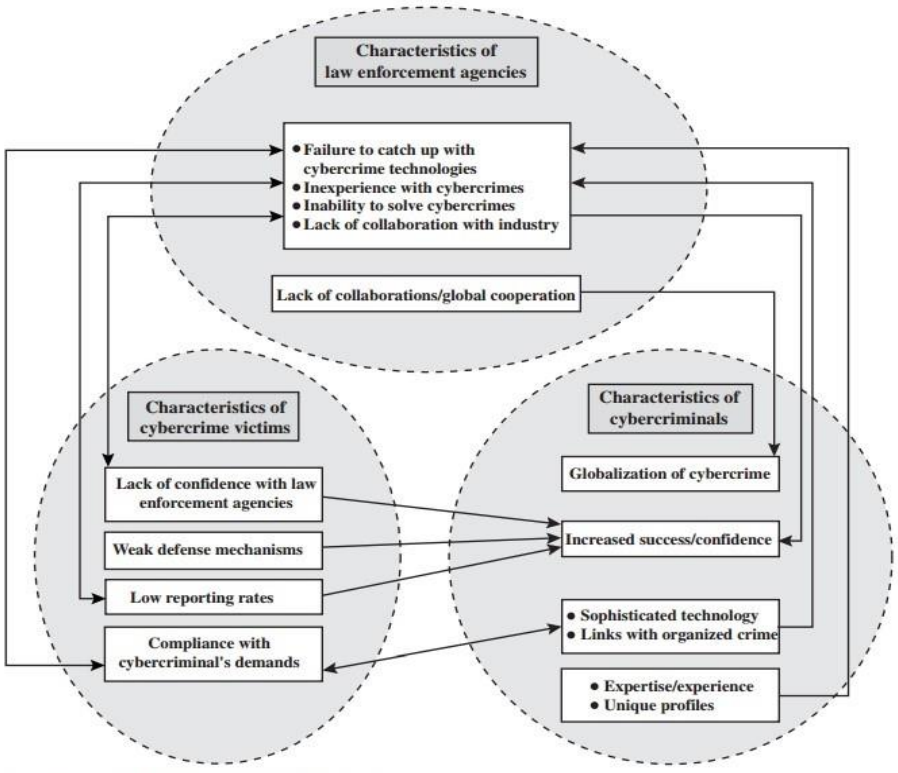


Figure 23.1 The Vicious Cycle of Cybercrime

Working With Law Enforcement

- Executive management and security administrators need to look upon law enforcement as another resource and tool, alongside technical, physical, and human-factor resources.
- The successful use of law enforcement depends much more on people skills then technical skills.
- Management needs to understand the criminal investigation process, the inputs that investigators need, and the ways in which the victim can contribute positively to the investigation.

2. Intellectual property

Three primary types of property:

- **Real property:** Land and things permanently attached to the land, such as trees, buildings, and stationary mobile homes.
- **Personal property:** Personal effects, moveable property and goods, such as cars, bank accounts, wages, securities, a small business, furniture, insurance policies, jewelry, patents, pets, and season baseball tickets.
- **Intellectual property:** Any intangible asset that consists of human knowledge and ideas. Examples include software, data, novels, sound recordings, the design of a new type of mousetrap, or a cure for a disease.

Types of Intellectual property:

- Copyrights
- Trademarks
- patents

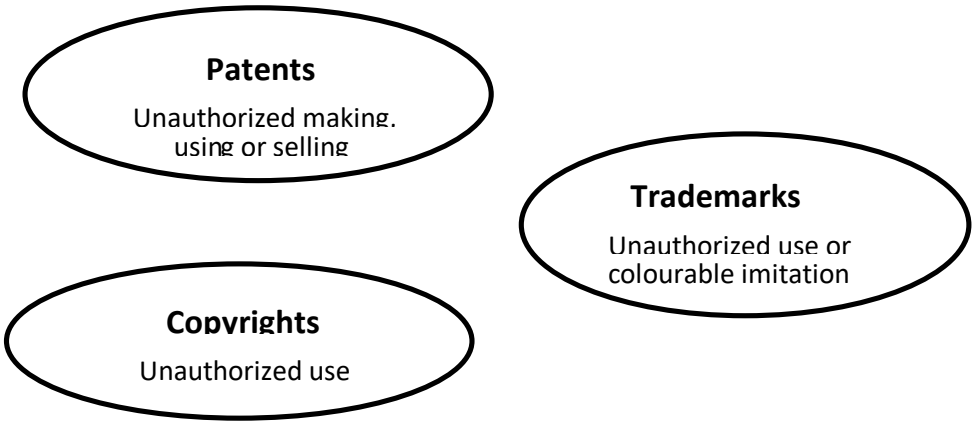


Fig: Intellectual property infringement

Copyrights:

Copyright law protects the tangible or fixed expression of an idea, not the idea itself. A creator can claim copyright, and file for the copyright at a national government copyright office, if the following conditions are fulfilled:

- The proposed work is original.
- The creator has put this original idea into a concrete form, such as hard copy(paper), software, or multimedia form.

Trademarks: A trademark is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.

Patents:

A patent for an invention is the grant of a property right to the inventor. The right conferred by the patent grant is, in the language of the U.S. statute and of the grant itself, "the right to exclude others from making, using, offering for sale, or selling" the invention in the United States or "importing" the invention into the United States. Similar wording appears in the statuses of other nations.

Types

- Utility patents

- Design patents
- Plant patents

Intellectual Property Relevant to Network and Computer Security

- **Software:** This includes programs produced by vendors of commercial software (eg: operating systems, utility programs, applications) as well as shareware, proprietary software created by an organization for internal use, and software produced by individuals.
- **Databases:** A database may consist of data that is collected and organized in such a fashion that it has potential commercial value.
- **Digital content:** This category includes audio files, video files, multimedia, courseware, web site content, and any other original digital work that can be presented in some fashion using computers or other digital devices.
- **Algorithms:** An example of a patentable algorithm is the RSApublic-key cryptosystem.

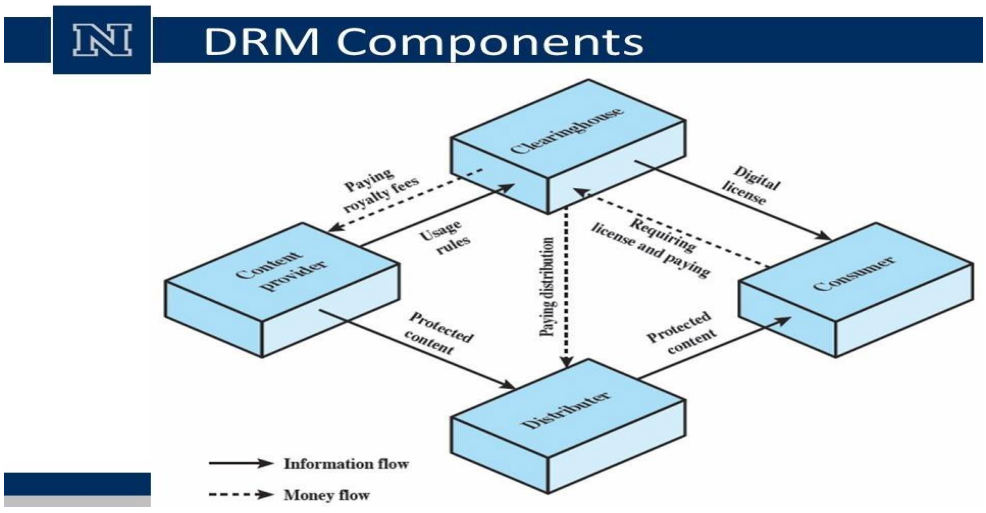
Digital Millennium Copyright Act (DMCA)

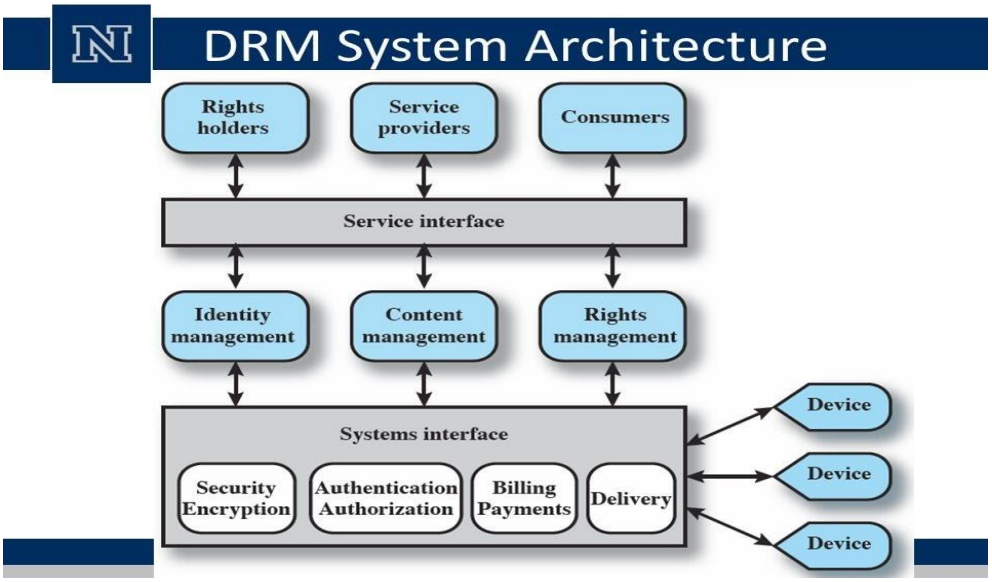
The U.S. Digital Millennium Copyright Act (DMCA) has had a profound effect on the protection of digital content rights in both U.S. and worldwide. The DMCA encourages copyright owners to use technological measures to protect copyrighted works.

Digital Rights Management (DRM)

Digital Rights Management (DRM) refers to systems and procedures that ensure that holders of digital rights are clearly identified and receive the stipulated payment for their works. Components:

- Content provider
- Distributor
- Consumer
- Clearinghouse





3. Privacy

The scale and interconnectedness of personal information collected and stored in information system has increased dramatically, motivated by law enforcement, national security, and economic incentives.

Privacy law and Regulation

Two initiatives

- European Union Data Protection Directive
- United States Privacy Initiatives

Organizational Response

Organizations need to deploy both management controls and technical measures to comply with laws and regulations concerning privacy as well as to implement corporate policies concerning employee privacy.

Privacy and Data Surveillance

- Data transformation
- Anonymization
- Selective revelation
- Immutable audit
- Associative memory

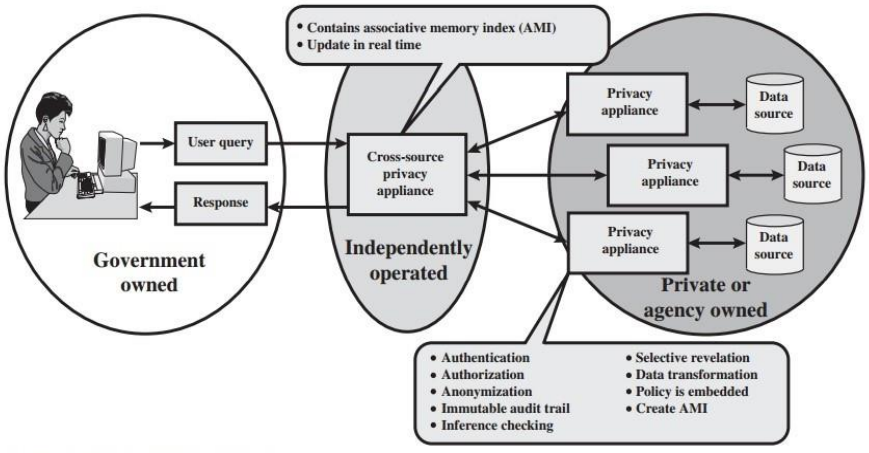


Figure 23.5 Privacy Appliance Concept

4. Ethical Issues

Ethics refers to a system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions

Ethics and the IS Professions

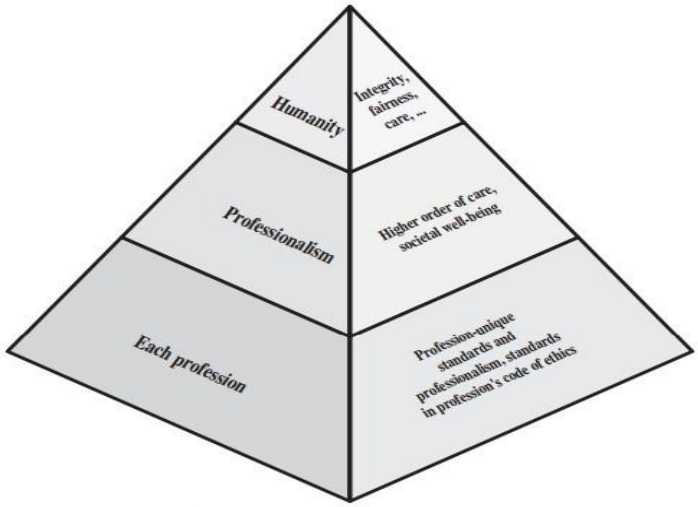


Figure 23.6 The Ethical Hierarchy

Ethical Issues Related to Computers and Information Systems

Technology Intrusion	Privacy internal to the firm Privacy external to the firm Computer surveillance Employee monitoring Hacking
Ownership Issues	Moonlighting Proprietary rights Conflicts of interest Software copyrights Use of company assets for personal benefit Theft of data, software, or hardware
Legal Issues and Social Responsibilities	Embezzlement, fraud and abuse, such as through EFT's or ATM's Accuracy and timeliness of data Over-rated system capabilities and "smart" computer Monopoly of data
Personal Issues	Employee sabotage Ergonomics and human factors Training to avoid job obsolescence.

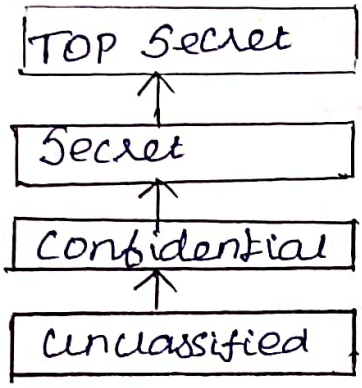
Codes of Conduct

- Dignity and worth of other people
- Personal integrity and honesty
- Responsibility for work
- Confidentiality of information
- Public safety, health, and welfare
- Participation in professional societies to improve standards of the profession.
- The notion that public knowledge and access to technology is equivalent to social power.

1.3 Need For Security at multiple Levels

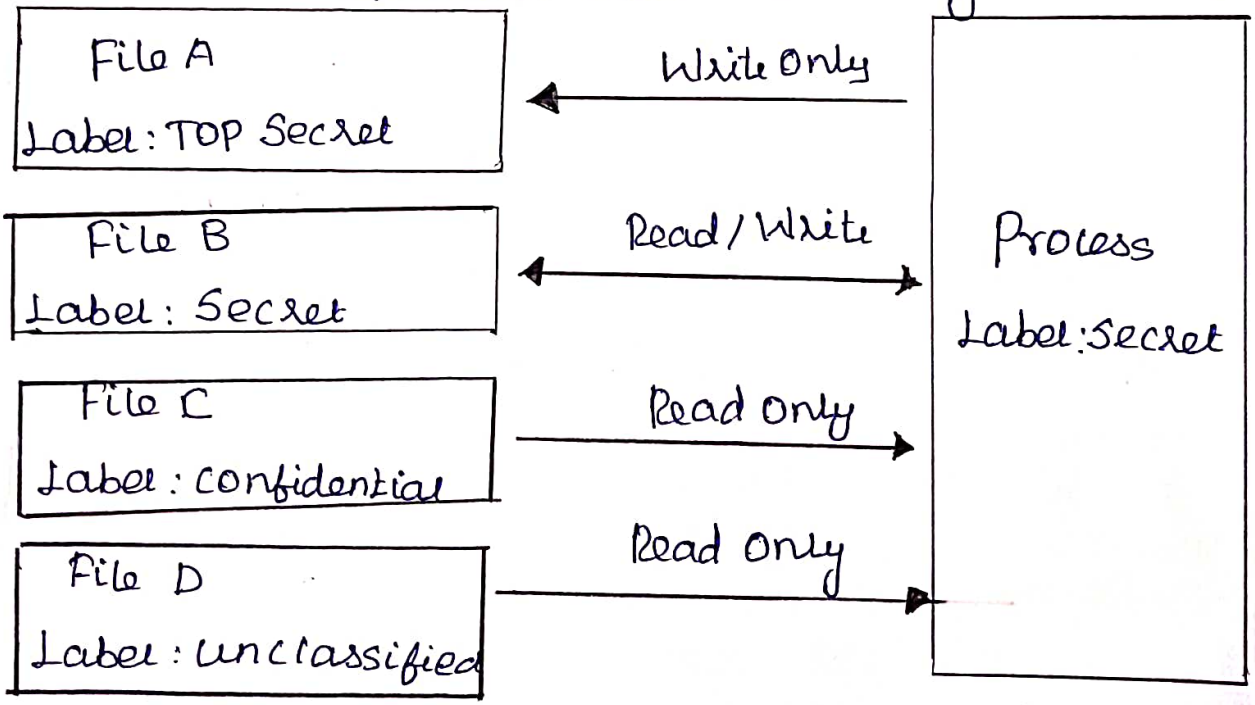
A class of system that has system resources (particularly stored information) at more than one security level (has different types of sensitive resources) and that permits concurrent access by users who differ in security clearance and need-to-know, but is able to prevent each user from accessing resources for which the user lacks authorization.

multi-levels:-



The Bell-La Padula Model (BLP)

Available data flows using an MLS system



Processes can read the same or lower security levels but can only write to their own or higher security levels.

Security Levels, Objects and Subjects

Security Levels (SLs). Which are composed of two types of entities:

1) Sensitivity – A hierarchical attribute such as "Secret" or "Top Secret".

2) Categories: – A set of non-hierarchical attributes such as "US Only" or "UFO".

Security levels on objects are called Classifications.

Security levels on subjects are called Clearances.

1.4 Security Policies

A network Security Policy (NSP) is a generic document that outlines rules for computer network access, determine how policies are enforced and lays out some of the basic architecture of the company security network security environment.

The document itself is usually several pages long and written by a commitee. A security policy goes far beyond the simple idea of "keep the bad guys out". Its a very complex document, meant to govern data access, Web browsing habits. Use of Passwords and encryption, email attachments and more. It specifies these rules for individuals or groups of individuals throughout the company.

Security Policies

* Cryptography and compliance
* Use of encryption
* Managing electronic keys
* Using and receiving digital signatures

1) Cryptography and compliance:

A Policy on cryptographic controls will be developed with Procedures to Provide appropriate levels of Protection to sensitive information whist ensuring compliance with statutory, regulatory and contratual requirements.

8) Use of encryption:

Classified information shall only be taken for use away from the organization in an encrypted form unless its confidentiality can otherwise be assured.

3) Managing electsonic keys

A Procedure for the management of electsonic keys, to control both the encyption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best Pratice guidelines and compliance with both legal and constratual requirements.

4) Using and receiving digital Signatures

important business information being communicated electronically shall be authenticated by the use of digital signatures. information received without a digital signature shall not be relied upon.

1.5 MODEL OF NETWORK SECURITY

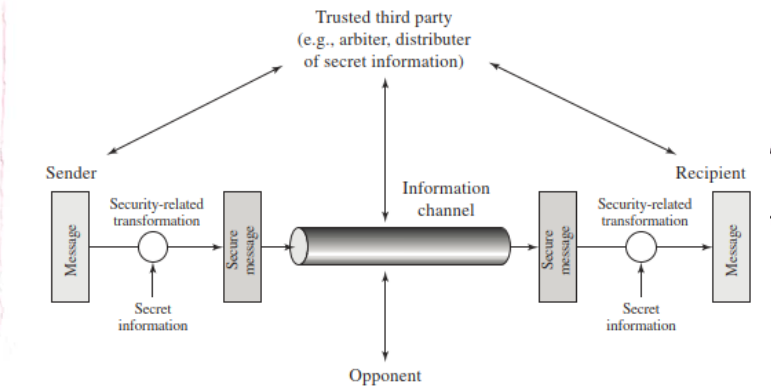


Figure 1.4 Model for Network Security

* A message is to be transferred from one party to another across some sort of Internet.

* Two parties → principals
  * cooperate for the exchange to take place.

Logical information channel:

- established (i) by defining a route through the i/n from source to destination.
  ii) by the cooperative use of communication protocols e.g (TCP/IP) by the two principals.

Two components for providing security:

(i) A security-related transformation on the information to be sent.

Ex: - encryption.

ii) Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

* A trusted third party may be needed to achieve secure transmission.

Four basic tasks in designing security service:

1. Design an algorithm for performing the security-related transformation.
2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Network Access Security Model:

* Protecting an information system from unwanted

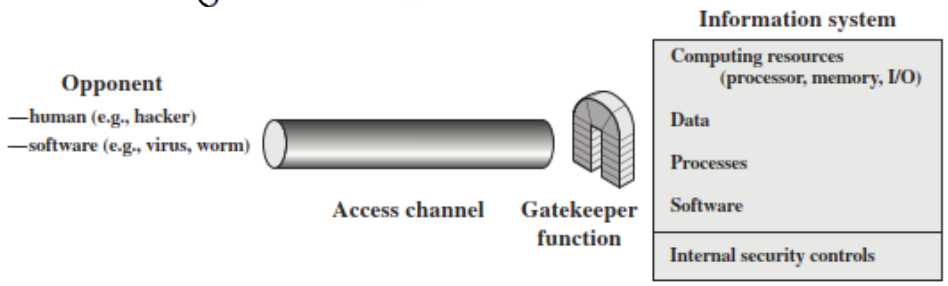


Figure 1.5 Network Access Security Model

Hackers:
- Who attempt to penetrate systems that can be accessed over a network.

Intruder:
- disgruntled employee who wishes to do damage
- a criminal who seeks to exploit computer assets for financial gain.

Another type of unwanted access:
- placement in a computer system of logic that exploits vulnerabilities in the system and can affect application program as well as utility programs (editors, compilers)

Two kinds of Threats:

i) Information access Threats:
- intercept or modify data on behalf of users who should not have access to that data.

ii) Service Threats:
- exploit service flaws in computers to inhibit use by legitimate users.

S/w attacks → Viruses, Worms

1.6.1 SECURITY ATTACKS

Classification : used both in X.800 & RFC 2828

i) Passive Attacks

ii) Active Attacks.

* Passive Attack:
  - Attempts to learn or make use of information from the system but does not affect system resources.

* Active Attack:
  - Attempts to alter system resources or affect their operation.

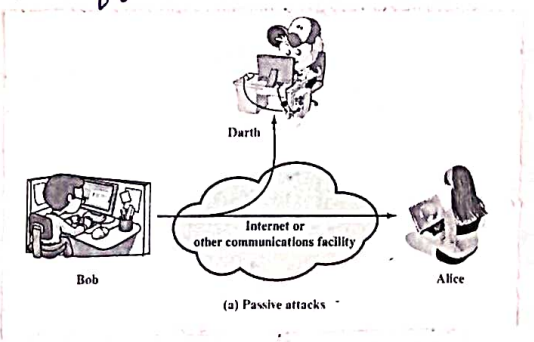
1. Passive Attacks:

* Nature of eavesdropping on, or monitoring of transmissions
- The goal of the opponent is to obtain information that is being transmitted.

Two types:

a) Release of message contents

b) Traffic analysis.



(a) Passive attacks

a) Release of Message contents:

* A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

b) Traffic Analysis:

- subtler.
- Had encryption protection, an opponent might still be able to observe the pattern of the messages.

* The opponent could determine the location & identity of communicating hosts
- observe the frequency and length of messages being exchange

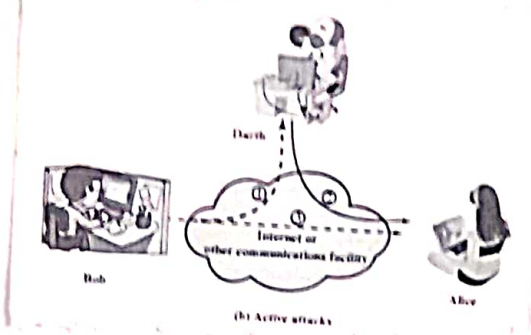
* The info might be useful in guessing the nature of the communication.

→ Passive attacks are very difficult to detect
- Do not involve any alteration of data.
- Feasible to prevent the attacks.

2. Active Attacks

* Active attacks involve some modification of the data stream or the creation of a false stream.

Four categories



1) Masquerade
2) Replay
3) Modification of messages
4) Denial of Service.

1) Masquerade:

* Takes place when one entity pretends to be a different entity

2) Replay:

* Passive capture of a data unit
* Subsequent retransmission to produce an unauthorized effect.

3) Modification of messages

* Some portion of a legitimate message is altered
  - messages are delayed or reordered to produce an unauthorized effect

Ex: Allow John Smith to read confidential file accounts

modified to

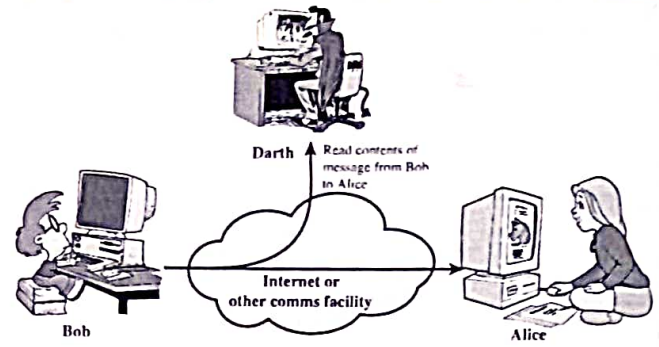
Allow Fred Brown to read confidential file accounts.

4) Denial of Service

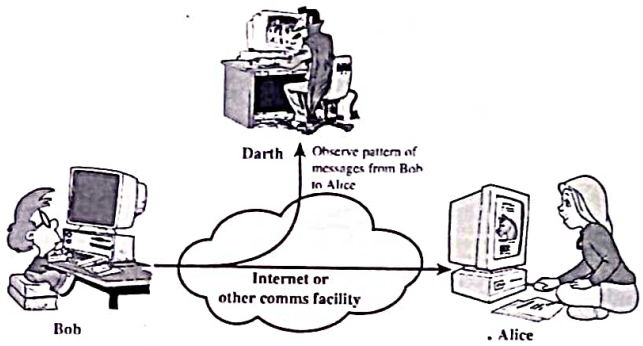
* prevents or inhibits the normal use or management of communications facilities
  - has a specific target.

* Active Attacks are easy to detect and prevent

PASSIVE ATTACKS



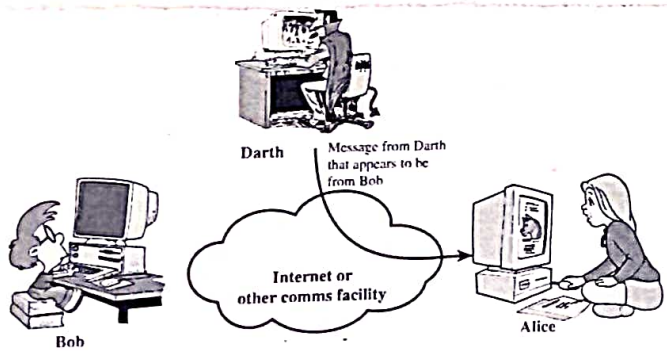
(a) Release of message contents



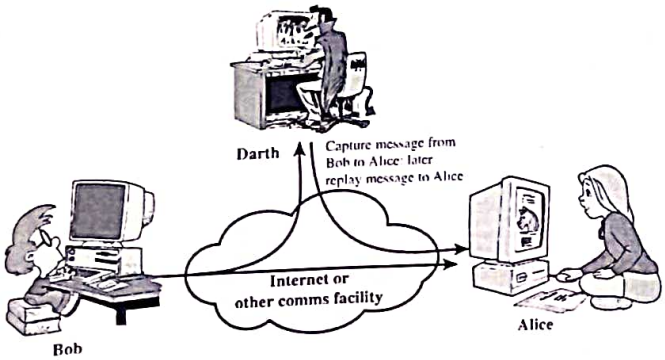
(b) Traffic analysis

Figure 1.2 Passive Attacks

ACTIVE ATTACKS

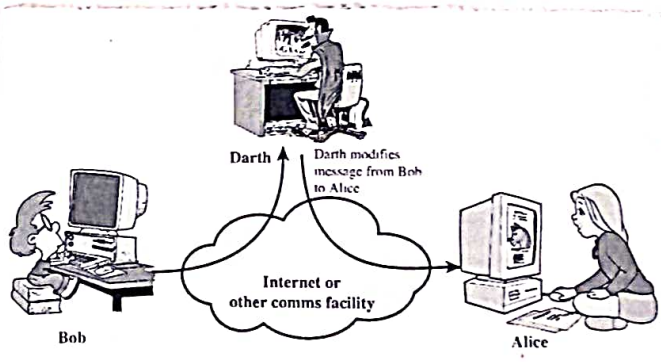


(a) Masquerade

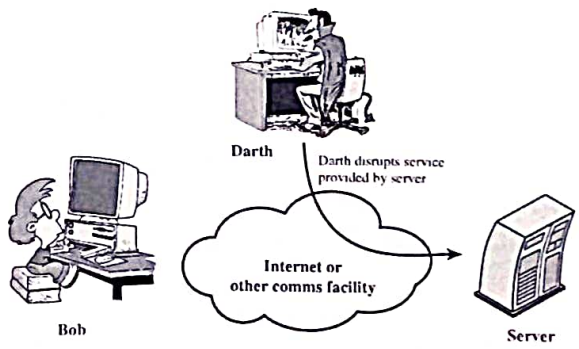


(b) Replay

Figure 1.3 Active attacks (*Continued*)



(c) Modification of messages



(d) Denial of service

Figure 1.3 Active attacks

1.6.2 SECURITY SERVICES

* X.800 defines a security service as a service provided by a protocol layer of communicating open systems.
  - ensures adequate security of the systems or of data transfers.

* RFC 2828
  - a processing or communication service that is provided by a system to give a specific kind of protection to s/m resources

* Security services implement security policies and are implemented by security mechanisms.

→ X.800 divides the services into five categories and fourteen specific services.

Table 1.2 Security Services (X.800)

AUTHENTICATION The assurance that the communicating entity is the one that it claims to be. **Peer Entity Authentication** Used in association with a logical connection to provide confidence in the identity of the entities connected. **Data-Origin Authentication** In a connectionless transfer, provides assurance that the source of received data is as claimed. **ACCESS CONTROL** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do). **DATA CONFIDENTIALITY** The protection of data from unauthorized disclosure. **Connection Confidentiality** The protection of all user data on a connection. **Connectionless Confidentiality** The protection of all user data in a single data block **Selective-Field Confidentiality** The confidentiality of selected fields within the user data on a connection or in a single data block. **Traffic-Flow Confidentiality** The protection of the information that might be derived from observation of traffic flows.	**DATA INTEGRITY** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). **Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. **Connection Integrity without Recovery** As above, but provides only detection without recovery. **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. **Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. **Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

1.6.3 SECURITY MECHANISMS

* X.800 defined the lists of security mechanisms

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Reversible encipherment mechanisms

* An encryption algorithm that allows data to be encrypted and subsequently decrypted.

Irreversible encipherment mechanisms

* Include hash algorithms and message authentication codes.
  - used in digital signature and message authentication applications.

* Relationship between security services and security mechanisms.

Table 1.4 Relationship Between Security Services and Mechanisms

	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

1.7 OSI SECURITY ARCHITECTURE

OSI → Open System Interconnection

* OSI provides a systematic framework for defining security attacks, mechanisms and services.

ITU-T[2] Recommendation X.800 Security Architecture for OSI, defines a systematic approach.

* OSI Security architecture is useful to managers as a way of organizing the task of providing security
* The OSI security architecture focuses on security attacks, mechanisms and services.

(i) Security Attack:

* Any action that compromises the security of information owned by an organization.

ii) Security Mechanism:

* A process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack.

iii) 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.

Threat and Attack:

- Used to mean more or less the same thing.

Threat:

* A potential for violation of security, which exists when there is a circumstance, capability, action, or event

that could break security and cause harm.
- a threat is a possible danger that might exploit a vulnerability.

Attack:

* An assault on system security that derives from an intelligent threat.
- An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

1.8 CLASSICAL ENCRYPTION TECHNIQUES

* Two basic building blocks of all encryption techniques
  - i) Substitution Techniques
  - ii) Transposition Techniques

1.8.1 SUBSTITUTION TECHNIQUES

* A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
  - a) Caesar cipher
  - b) Monoalphabetic Ciphers
  - c) Playfair cipher
  - d) Hill cipher
  - e) Polyalphabetic ciphers
  - f) One-Time pad.

a) Caesar Cipher:

- by Julius Caesar

* Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet

Assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption: A shift may be of any amount.

$$C = E(K, p) = (p + K) \bmod 26 \quad , K = 1 \text{ to } 25$$

$K = 3$

$$C = E(3, p) = (p + 3) \bmod 26.$$

* For each plaintext letter p, substitute the ciphertext letter C.

Define the transformation

plain : a b c d e f g h i j k l m n o p q r s t u v w x y z

cipher : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

EX:

plain : meet me after the toga party

cipher : PHHW PH DIWHU WKH WRJD SDUWB

Decryption:

The decryption algorithm is

$$p = D(K, C) = (C - k) \bmod 26.$$

Disadvantage:

* Brute-force cryptanalysis is easily performed.

Characteristics:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try
3. The language of the plaintext is known and easily recognizable.

b) Monoalphabetic ciphers:

* Eliminate brute-force techniques for cryptanalysis.

→ A single cipher alphabet is used per message.

Steps:

1. The relative frequency of the letters can be determined
2. Compare to a standard frequency distribution for English

Ex:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

Relative frequencies of the letters.

P	13.33	H	5.83	F	3.33	B	1.67	C	0.00		
Z	11.67	D	5.00	W	3.33	G	1.67	K			
S	8.33	E	5.00	O	2.50	Y	1.67	L			
U	8.33	V	4.17	T	2.50	I	0.83	N			
O	7.50	X	4.17	A	1.67	J	0.83	R			
M	6.67										

Relative frequency of letters in English Text.

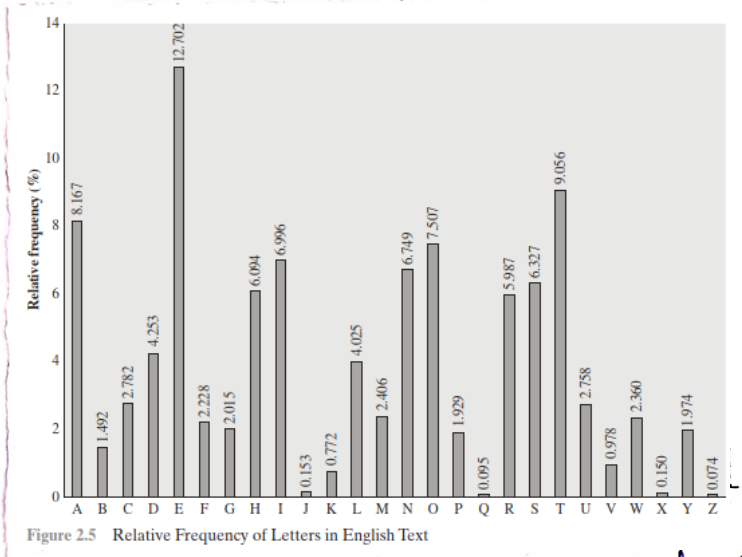


Figure 2.5 Relative Frequency of Letters in English Text

Cipher texts P & Z are the equivalents of plain letters e & t.

S, U, O, M, H → high frequency.

probability correspond to plain letters {a, h, i, n, o, r, s}

A, B, G, Y, I, J → lowest frequency. ⇒ {b, j, k, q, v, x, z}

ZW → th

two-letter combinations → digram.

three-letter combinations → trigram, ZWP → the

ZWSZ → that

Plaintext:

it was discovered yesreday that several informal but

* Mono alphabetic ciphers are easy to break
  - they reflect the frequency data of the original alphabet.

Countermeasure:
  - to provide multiple substitutes known as homophones, for a single letter.

c) Playfair cipher: - Lord Peter Wimsey

* Best-known multiple-letter encryption cipher
  → treats digrams in the plaintext as single units and translates the units into ciphertext digrams.
* Based on the use of a 5x5 matrix of letters constructed using a keyword.

Example: Keyword : Monarchy.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

* The matrix is constructed by filling the letters of the keyword from left to right and from top to bottom
  - and then filling in the remainder of the matrix with the remaining letters in alphabetic order.
  - The letters I & J count as one letter.
* Plaintext is encrypted two letters at a time.

Rules:

1. Repeating P.T letters that would fall in the same pair are separated with a filler letter, X.

   Ex: balloon

   ba lx lo on

2. P.T letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.

   ar → RM.

3. P.T letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last.

   mu → CM.

4. Each P.T letter is replaced by the letter that lies in its own row and the column occupied by the other P.T letter.

   hs → BP

   ea → IM (JM)

* Only 26 letters, 26×26 = 676 digrams
  - identification of individual digrams is more difficult.

* used as
  - Standard field system by British Army in World war I
  - by U.S. Army & other Allied forces during World war II

* Easy to break.

d) **Hill cipher:** Leslie Hill, 1929

* The encryption algorithm takes m successive P.T letters and substitutes for them m C.T letters.

– The substitution is determined by m linear equations in which each character is assigned a numerical value

$a = 0,\ b = 1, \ldots z = 25$

$m = 3.$

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26.$$

Encryption:

$$\boxed{C = KP \bmod 26}$$

C, P – Column vectors of length 3.

K – 3×3 matrix → encryption key.

Operations are performed mod 26.

Ex: Plaintext : paymoremoney

encryption key: $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

* First three letters of the P.T are represented by the vector (15 0 24)

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} (15\ 0\ 24) \bmod 26 = (375\ 819\ 486) \bmod 26$$
$$= (11\ 13\ 18)$$
$$= LNS.$$

Ciphertext : LNSHDLEWMTRW

Decryption:

$$\boxed{P = K^{-1}C \bmod 26.}$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 & 13 & 18 \end{pmatrix} \bmod 26 = \begin{pmatrix} 15 & 0 & 24 \end{pmatrix}$$

$$= PAY$$

Continuing this fashion.

P.T is paymoremoney.

* hides single letter frequency.

e) Polyalphabetic Ciphers:

* To improve monoalphabetic cipher.
- to use different monoalphabetic substitutions

features:

1. A set of related monoalphabetic substitution rules is used
2. A key determines which particular rule is chosen for a given transformation

3 Algorithms

i) Vigenere Cipher
ii) Auto-Key System
iii) Vernam cipher

Vigenere cipher:

* use Vigenere tableau.
- Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left.
- A normal alphabet for the P.T runs across the top.

Encryption:

* Given a key letter x and a plaintext y, the ciphertext is at the intersection of the row labeled x and the column labeled y, the ciphetext is V

KEY \ --PLAINTEXT--	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

* To encrypt a message, a key is needed that is as long as the message.
  - Usually the key is a repeating keyword.

Ex:

Keyword : deceptive
plaintext : we are discovered save yourself

Encryption

Key : deceptivedeceptivedeceptive
plaintext : wearediscoveredsaveyourself
ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption

* The key letter again identifies the row.
* The position of the ciphertext letter in that row determines the column and the P.T letter is at the top of that column.

ii) Auto key system.

* A keyword is concatenated with the plaintext itself to provide a running key.

Encryption:

Ex:

Key: deceptive we arediscovered sav

Plaintext: we arediscovered save yourself

Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

iii) Vernam cipher: Gilbert Vernam, 1918

* Choose a keyword that is as long as the plaintext and has no statistical relationship to it.

— works on binary data rather than letters.

Encryption:

$$C_i = P_i \oplus K_i$$

P_i = ith binary digit of plaintext

K_i = ith binary digit of key.

C_i = ith binary digit of ciphertext.

$\oplus$ = exclusive-or (XOR) operation.

* Ciphertext is generated by performing bitwise XOR of the plaintext and the key.

Decryption:

$$P_i = C_i \oplus K_i$$

* Construction of the key.

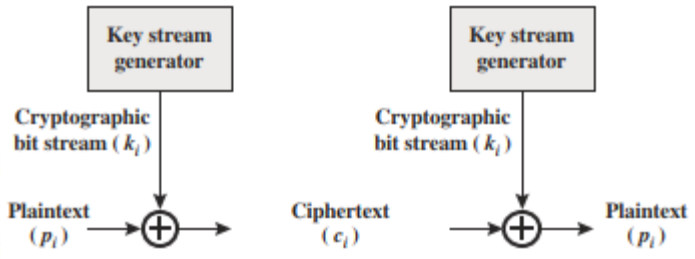


Figure 2.7 Vernam Cipher

f) One-Time Pad: Joseph Mauborgne

* Use a random key that was truly as long as the message, with no repetitions.
- unbreakable
* Produces random output that bears no statistical relationship to the plaintext.
- No way to break the code.
* Using a Vigenere scheme with 27 characters in which twenty-seventh character is the space character.
* Vigenere tableau must be expanded to 27×27.

Ex:

CipherText.

ANKYODKYUREPFJ

Two different decryptions using two different keys:

① ciphertext: ANKYODKYUREPFJB
key: pxlmvmsydofktqzv
plaintext: mr mustard with

② ciphertext: ANKYODKYUREPFJBYOJ
key: mfugpmiydgaxgoufh
plaintext: miss scarlet with

* Two plaintexts are produced.
* Cryptanalyst cannot decide the correct decryption.

→ The security of the one-time pad is entirely due to the randomness of the key.
* The one-time pad offers complete security.

Two difficulties
i) making large quantities of random keys.
ii) problem of key distribution & protection.

1.8.2 TRANSPOSITION TECHNIQUES

* Kind of mapping is achieved by performing some sort of permutation on the plaintext letters.

i) Rail fence technique

ii) Row column Transposition.

i) Rail fence Technique:

* The plaintext is written down as a sequence of diagonals & read off as a sequence of rows.

Ex:

plaintext: meet me after the toga party.

depth = 2.

Encryption:

m e m a t r h t g p r y
e t e f e t e o a a t

ciphertext: MEMATRHTGPRYETEFETEOAAT

Decryption:

$23/2 = 11.5 = 12$

* Write first half: M E M A T R H T G P R Y
* Then write remaining:

M E M A T R H T G P R Y
E T E F E T E O A A T

* Read column wise.
* Trivial to cryptanalyze

ii) Row Column Transposition:

* Write the message in a rectangle, row by row, and read the message off, column by column
- but permute the order of the columns

* The order of the columns then becomes the key to the algorithm

Ex:

Encryption:

Key: 4 3 1 2 5 6 7

PlainText:
a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

CipherText: TTNAAPTMTSUOAODWCOIXKNLYPETZ

* The transposition cipher can be made significantly more secure by performing more than one stage of transposition.
— more complex permutation that is not easily reconstructed.

Key: 4 3 1 2 5 6 7

Input:
t t n a a p t
m t s u o a o
d w c o i x k
n l y p e t z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

* Much difficult to cryptanalyze.

1.9 STEGANOGRAPHY

* A plaintext message may be hidden in one of two ways

i) methods of steganography
   - conceal the existence of the message

ii) methods of cryptography.
   - render the message unintelligible to outsiders by various transformations of the text.

* Simple form
* time consuming to construct

Various Techniques:

Ex:

a) character marking
b) Invisible inks
c) Pin punctures
d) Typewriter correction ribbon

a) character marking:

* Selected letters of printed or typewritten text are over written in pencil.
- The marks are ordinarily not visible unless the paper is held at an angle to bright light

b) Invisible ink:

* A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

c) Pin punctures:

* Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light

d) Typewriter correction ribbon

* Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

One time pad:-

* one-time pad (OTP), also called Vernam-ciphers or the perfect ciphers, is a crypto algorithm whose plaintext is combined with a random key.

* The key is at least as the message or data that must be encrypted.

* Each key is used only once, and both senders and reciever must destroy their key after use.

* There should only be two copies of the key : Senders, reciever

Encryption process:

(i) Assign a numbers to each chasactes of the plain text, like (a=0, b=1, c=2, ... z=25); As per given table.

a	b	c	d	e	f	g	h	i	j	k	l	m	
0	1	2	3	4	5	6	7	8	9	10	11	12	
n	o	p	q	r	s	t	u	v	w	x	y	z	
13	14	15	16	17	18	19	20	21	22	23	24	25	

(ii) Assign a number to each character of the plain text and the key according to alphabetical order.

Plain Text	I	A	M	S	T	U	D	E	N	T
	8	0	12	18	19	20	3	4	13	19
Key	E	N	G	I	N	E	E	R	E	N
	4	13	6	8	13	4	4	17	4	13

(iii) Add Both the number (corresponding plain text character Number and key character Number)

P.T char	8	0	12	18	19	20	3	4	13	19
key char	4	13	6	8	13	4	4	17	4	13
sum (P.T+key)	12	13	18	26	32	24	7	21	17	32

(iv) Subtract the number from 26 if the added number is greater than 26. Otherwise left it. Assign alphabets of numbers, it produce ciphes text.

Sum	12	13	18	26	32	24	7	21	17	32
Sum-26	12	13	18	0	6	24	7	21	17	6
Cipher Text	M	N	S	A	G	Y	H	V	R	G

Ciphes Text : MNSAGYHVRG

Decsyption process:

(i) Assign a numbes to each characters of the ciphes text, like (a=0, b=1, c=2 ··· Z=25)

(ii) Assign a number to each character of the ciphes text and the key according to alphabetical order.

Cipher Text	M	N	S	A	G	Y	H	V	R	G
	12	13	18	0	6	24	7	21	17	6
key	E	N	G	I	N	E	E	R	E	N
	4	13	6	8	13	4	4	17	4	13

(iii) Subtract cipher text alphabet number from key alphabet number. (Reverse process of Encryption)

Cipher Text	12	13	18	0	6	24	7	21	17	6
key	4	13	6	8	13	4	4	17	4	13
Sum(CT-key)	8	0	12	-8	-7	20	3	4	13	-7

(iv) If any number less than zero then add 26 in that number. Otherwise left it.

Sum(CT-key)	8	0	12	-8	-7	20	3	4	13	-7
Sum+26 (<0)	8	0	12	18	19	20	3	4	13	19
plain Text	I	A	M	S	T	U	D	E	N	T

plain Text : IAMSTUDENT

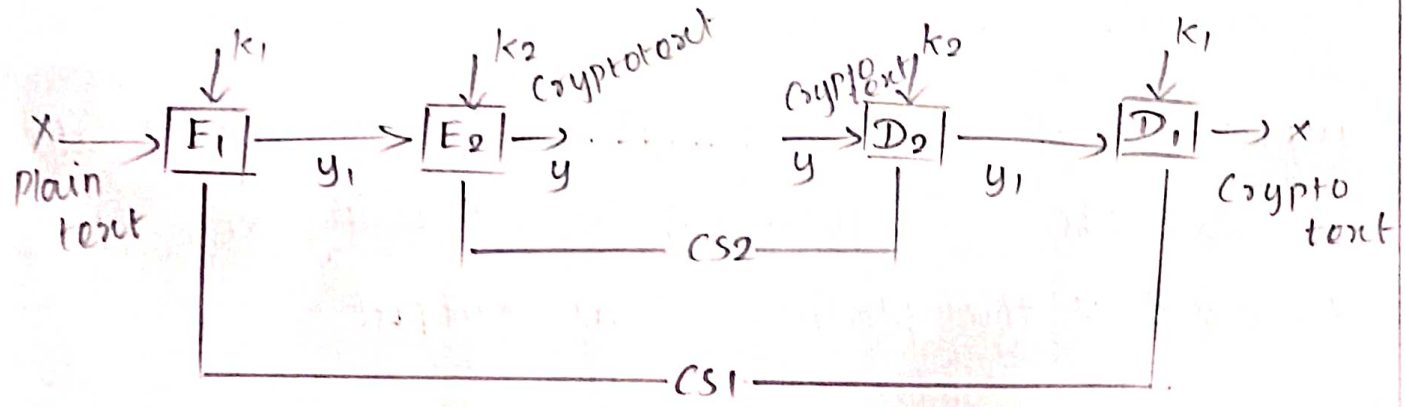
Product Cryptosystem:

All the cryptosystems provide a limited level of security: all are vulnerable to attacks.

The Hill cipher looks an apparent exception. It can make an attack cumbersome by increasing the size of the linear equation used. However, the encryption/decryption processes too become equally cumbersome.

None of the cryptosystems by itself offers flexibility in terms of enhancing the security to a desired level.

Such flexibility can be offered by a 'product cryptosystem' which uses two cryptosystems in tandem



. We assume that the plaintext and the cryptotext are of the same type and size.

. For example, each can be a binary data file of size n.

. x is the sample plaintext

. It is encrypted using key k1, conforming to the scheme of cryptosystem CS1.

. y1 represents the intermediate text.

. It forms the input to the second cryptosystem CS2 where it is encrypted conforming to CS2 using key k2.

. Its output y represents the overall encrypted output.

. At the receiving end, decryption is carried out again in two stages.

* Decryption conforming to CS2 using key k2 yields the intermediate text y1, which is the input to the second decryption stage where it is decrypted conforming to CS1 using key k1 to yield x - the plaintext - as output

* The Combined encryption operation can be represented as

$$Y = E_2[E_1(X, K_1), K_2)$$

Similarly the combined decryption can be represented as

$$X = D_1(D_2(Y, K_2), K_1)$$

* The key space of the product cryptosystem is decided by those of CS1 and CS2 together.

* If the key K1 and K2 are decided independently of each other and the two cryptosystems - CS1 and CS2 - are also independent, the probability of the key set of the product cryptosystem is given by

$$P(K_1, K_2) = P(K_1) \times P(K_2)$$

* with such an enhanced key set, the product system offers a much higher level of security compared to the two component systems

* If S is a cryptosystem $S \times S = S^2$ represents a possible product Crypto-System

Consider the shift cipher; repeated use of the shift cipher is equivalent to a single shift

Ciphers ; for such ciphers the product cipher S^2 is S itself ($S^2 = S$).

Such a cryptosystem which remains the same despite its repeated use is called an 'idempotent cipher'

product cryptosystems formed by the repeated and tandem use of non-idempotent ciphers can offers desired levels of security.

Cryptanalysis:

Usually eve is aware of the specific cryptosystem employed by Alice and Bob for their secure communication.

As such, the scope of cryptanalysis is restricted to Eve's finding the key used.

If Eve succeds, all the messages transmitted so far are compromised.

Messages planned to be exchanged between Alice and Bob using the same key or algorithm, are also compromised.

Depending on what Eve can access, different possibilities arise:

1. Ciphertext-only attack:

Eve has access to a string of

Cryptotext characters based on which cryptanalysis is carried out. This possibility constitutes the most challenging situation for Eve to face. Normally Eve looks for patterns inthe cryptotext and tries to relate it to known or possible patterns in plaintext.

2. known plaintext attack:

Eve has access to a string of the plaintext and the corresponding cryptotext. Eve resorts to matching corresponding elements; Correlation techniques can be of use here.

3. Chosen plaintext attack:

Eve has access to the encryption machinery. Eve selects specific plaintext strings for encryption, gets corresponding crypto text and launches a cryptanalysis attack.

4. chosen cryptotext attack:

Eve has access to decryption machinery for a limited time. Eve selects specific cryptotext strings for decryption, gets corresponding plaintext and launches a cryptanalysis attack. The situation is the dual of the chosen plaintext attack.

* In Cryptanalysis, wherever possible we use the Ciphertext only attack for cryptanalysis. known plaintext attack is used in the other cases.

* Apart from all the above approaches, one can use the 'brute force attack'.

* One starts with a known Ciphertext, uses all possible keys, and obtains the respective plaintexts

* Out of these, a meaningful plaintext is to be identified and the corresponding key recovered.

* Despite it being tedious and morose, if the situation demands one has to fall back on the brute force attack in the absence of any better approach.