R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

22CS701- CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

Unit-I

Department: Computer Science and Engineering

Batch/Year : 2022-2026/IV

Created by:

Dr. A.Thilagavathy/ Associate Professor/CSE/RMKEC

Dr.D.Naveen Raju /Associate Professor/CSE/RMKEC

Ms.K.Padmapriya/ Associate Professor/CSE/RMDEC

Ms. J. Sherine Glory/Assistant Professor/CSE/RMDEC

Dr.Anish T P/Associate Professor/CSE/RMKCET

Mr.Vinoth Kumar V/ Assistant Professor/CSE(CS)/RMKCET

Date: 12.05.2025

R.M.K GROUP OF INSTITUTIONS

Table of Contents

S NO	CONTENTS	PAGE NUMBER
1	Contents	1
2	Course objectives	6
3	Pre Requisites (Course Names with Code)	6
4	Syllabus (With Subject Code, Name, LTPC details)	7
5	Course outcomes	9
6	CO- PO/PSO Mapping	10
7	Lecture Plan	11
8	Activity based learning	14
9	Lecture Notes	16
10	Assignments	62
11	Part A Q & A	67
12	Part B Qs	75
13	GATE Questions	76
14	Supportive online Certification courses	85
15	Real time Applications in day to day life and to Industry	86
16	Mini Project Suggestions	87
17	Assessment Schedule	89

R.M.K GROUP OF INSTITUTIONS

22CS701-CRYPTOGRAPHY AND CYBER SECURITY
(Lab Integrated)

COURSE OBJECTIVES

The Course will enable learners to:

- Understand the fundamentals of network security and security architecture.
- Learn the different symmetric key cryptographic algorithms.
- Study the various asymmetric key cryptographic algorithms and techniques.
- Know the importance of message authentication and integrity.
- Learn the various cyber-crimes and cyber security

PREREQUISITE

- 22MA201 Transforms and Numerical Methods
- 22CS501 Computer Networks

22CS701 CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

SYLLABUS

22CS701 CRYPTOGRAPHY AND CYBER SECURITY 3 0 2 4

UNIT I INTRODUCTION TO SECURITY 9+6

Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography –Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

List of Exercise/Experiments:

1. Perform encryption, decryption using the following substitution techniques (i) Ceaser cipher, (ii) playfair cipher iii) Hill Cipher iv) Vigenere cipher
2. Perform encryption and decryption using following transposition techniques i) Rail fence ii) row & Column Transformation

UNIT II SYMMETRIC CIPHERS 9+6

Number theory – Algebraic Structures – Modular Arithmetic - Euclid‘s algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution.

List of Exercise/Experiments:

1. Apply DES algorithm for practical applications.
2. Apply AES algorithm for practical applications.

UNIT III ASYMMETRIC CRYPTOGRAPHY 9+6

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing –Factorization – Euler’s totient function, Fermat’s and Euler’s Theorem – Chinese Remainder Theorem – Exponentiation and logarithm ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange -– Elliptic curve arithmetic – Elliptic curve cryptography.

List of Exercise/Experiments:

1. Implement RSA Algorithm using HTML and JavaScript.
2. Implement the Diffie-Hellman Key Exchange algorithm for a given problem.
3. Calculate the message digest of a text using the SHA-1 algorithm.

22CS701 CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

SYLLABUS

22CS701 CRYPTOGRAPHY AND CYBER SECURITY 3 0 2 4

UNIT IV INTEGRITY AND AUTHENTICATION ALGORITHMS 9+6

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates

List of Exercise/Experiments:

1. Implement the SIGNATURE SCHEME - Digital Signature Standard.
2. Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w

UNIT V CYBER CRIMES AND CYBER SECURITY 9+6

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security

List of Exercise/Experiments:

1. Automated Attack and Penetration Tools

a.Exploring N-Stalker, a Vulnerability Assessment Tool

2. Defeating Malware

i) Building Trojans ii) Rootkit Hunter

COURSE OUTCOMES

CO1	Understand cryptographical concepts.
CO2	Implement various cryptographic algorithms
CO3	Evaluate and apply network security protocols, to secure communications over networks
CO4	Identify common security threats and vulnerabilities and assess their impact on network security
CO5	Implement access control mechanisms and authentication techniques to protect information systems.
CO6	Develop and propose security policies and best practices for securing networks and information systems

CO-PO MAPPING

COs	PO's/PSO's														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO2	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO3	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO4	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO5	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO6	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1

1 – Low, 2 – Medium, 3 – Strong

LECTURE PLAN

S No	Topics	No of periods	Proposed date	Actual Lecture Date	Pertaining CO	Taxonomy level	Mode of Ddelivery
1	Course objective, course outcome delivery & Course introduction	1	03.01.2024		CO1	K1	ICT Tools
2	Security trends -Need for Security at Multiple levels, Security Policies Security	1	04.01.2024		CO1	K2	ICT Tools
3	Model of network security – Security attacks	1	06.01.2024		CO1	K2	ICT Tools
4	services and mechanisms-OSI security architecture	1	08.01.2024		CO1	K2	ICT Tools
5	Classical Encryption techniques: substitution techniques	1	09.01.2024		CO1	K3	ICT Tools
6	Classical encryption techniques: substitution techniques	1	10.01.2024		CO2	K3	ICT Tools
7	Substitution techniques	1	11.01.2024		CO2	K2	ICT Tools
8	Transposition techniques	1	23.01.2024		CO2	K2	ICT Tools
9	Transposition techniques, Steganography	2	24.01.2024		CO2	K2	ICT Tools

LECTURE PLAN

S No	Topics	No of periods	Proposed date	Actual Lecture Date	Pertaining CO	Taxonomy level	Mode of Ddelivery
10		1	03.01.2024		CO1	K1	ICT Tools
11		1	04.01.2024		CO1	K2	ICT Tools
12		1	06.01.2024		CO1	K2	ICT Tools
13		1	08.01.2024		CO1	K2	ICT Tools
14		1	09.01.2024		CO1	K3	ICT Tools
15		1	10.01.2024		CO2	K3	ICT Tools
16		1	11.01.2024		CO2	K2	ICT Tools

VIDEO LINKS

S.NO	TOPICS	Link
1	Cryptographic attacks	https://www.youtube.com/watch?v=BXq2T3BDL_Bo
2	History and Evolution of Cryptography and Cryptanalysis	https://www.youtube.com/watch?v=z9Qi5mDSY_b8&t=67s
3	Network Security	https://www.youtube.com/watch?v=Jt9lxEoWuYs
4	Cybercrime	https://www.youtube.com/watch?v=87N2GPEIy_AE
5	Perfect Secrecy	https://www.youtube.com/watch?v=vKRMWew_GE9A
6	Security Services	https://www.youtube.com/watch?v=bRgL_Dry7uw
7	Security Mechanisms	https://youtu.be/H5ifNVeDXkg?si=EGMc4FPQwPI1kxpX
8	Polyalphabetic Cipher	https://www.youtube.com/watch?v=BgFJD7oCmDE
9	Hill Cipher Encryption	https://youtu.be/-EQ8UomTrAQ?si=1lNwlUvoLZAOBTtq
10	Hill Cipher Decryption	https://youtu.be/JK3ur6W4rvw?si=df9gzjjBeQioaagk

ACTIVITY BASED LEARNING

1. The OSI Security Architecture

Activity: Layer Security Hunt

- Break students into 7 groups, each assigned an OSI layer.
- Each group presents possible security threats and solutions at their layer using posters or slides.
- Conduct a quiz afterward to reinforce.

2. Security Attacks

Activity: Attack Simulation Game

- Students role-play: some are "hackers" (launching specific attacks like spoofing, replay, or DoS), others are "defenders."
- Provide scenarios and allow teams to strategize responses.
- Discuss real-world examples afterward.

3. Substitution Techniques

Activity: Caesar Cipher Puzzle

- Give encoded messages using Caesar or Monoalphabetic ciphers.
- Students must decode the message and explain the process.

4. Threat Classification Chart

Activity: Create a Wall Chart

- In groups, students research different types of attacks (active/passive, internal/external, etc.)
- Populate a collaborative visual threat matrix showing severity, examples, and countermeasures

ACTIVITY BASED LEARNING

5. Authentication Demonstration

Activity: Multi-Factor Auth Simulation

- Demonstrate 1FA, 2FA, and 3FA using mock tokens, passwords, fingerprints (images).
- Let students simulate login processes in different security scenarios (e.g., public WiFi, bank app).

6. Playfair Cipher Game

Activity: Grid Encryption

- Teach Playfair cipher by letting students encode messages using 5x5 matrices.
- Use letter tiles or a printable worksheet to make this physical and interactive.

7. Hill Cipher Puzzle

Activity: Matrix Math in Crypto

- Have students encrypt messages using 2x2 or 3x3 Hill cipher keys.
- Provide calculator support or Python scripts to assist.

8. Image Stego Mystery

Activity: Stego Hunt

- Hide text in PNG/JPG files using OpenStego or similar.
- Students extract the message and explain how the information was hidden.

****

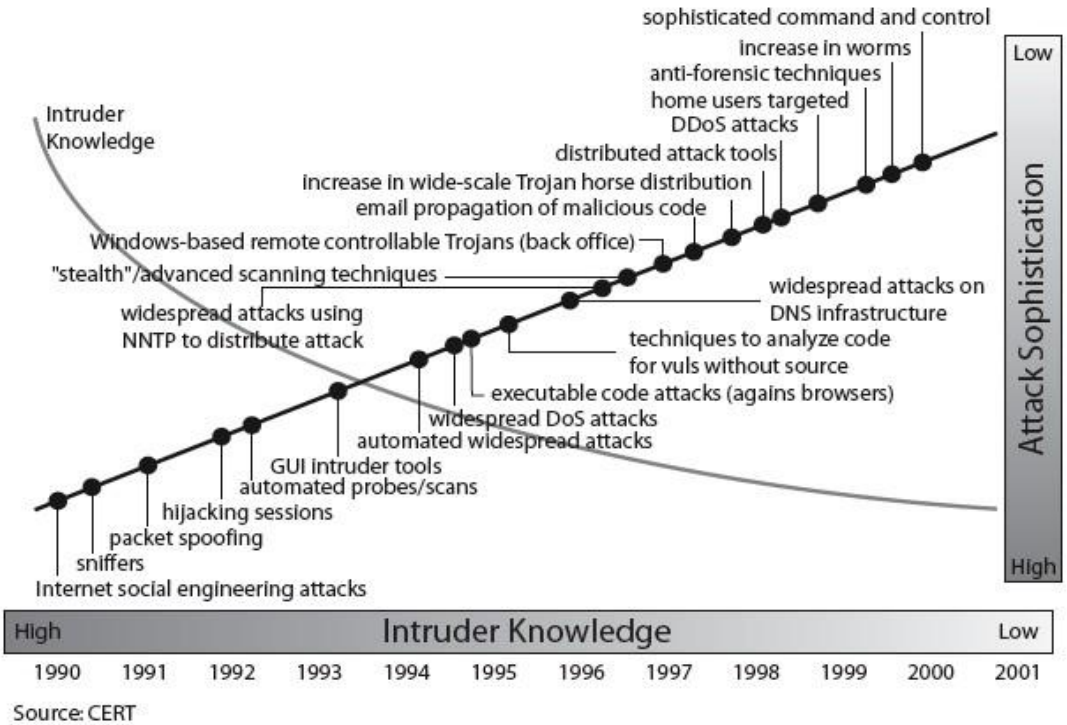
Unit-1

- Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.
- Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing"

- **Types Of Cryptography**
- In general there are three types Of cryptography

1. Symmetric Key Cryptography
2. Hash Functions
3. Asymmetric Key Cryptography

- Security Trends



Need for security at multiple levels

- A Security Domain can have a multi-level policy for one or more security services;
- Example: A Domain Security Policy may allow supporting low & moderate confidentiality services and moderate & high integrity services;
- Two entities from a multi-level domain must be assured that an appropriate level protection is provided for the keys and metadata by the CKMS (Crypto Key Management System) in accordance with the multi-level policy.

- **Multi-Level Security**: Selectable based on requirements and costs (e.g., processing time) ;
- **Scalable Security**: Selects acceptable level of protection while minimizing costs;
- **Selectable Security**: CKMS Multi-Domain Policy Enforcement supports selectable security;
- **Negotiated Security for Transaction**: Based on the policies of two or more entities participating in a sensitive transaction; Requires creation of a new temporary or permanent Security Policy for the transaction.

Computer security refers to protecting and securing computers and their related data, networks, software, hardware from unauthorized access, misuse, theft, information loss, and other security issues. The Internet has made our lives easier and has provided us with lots of advantages but it has also put our system's security at risk of being infected by a virus, of being hacked, information theft, damage to the system, and much more.

Technology is growing day by day and the entire world is in its grasp. We cannot imagine even a day without electronic devices around us. With the use of this growing technology, invaders, hackers and thieves are trying to harm our computer's security for monetary gains, recognition purposes, ransom demands, bullying others, invading into other businesses, organizations, etc. In order to protect our system from all these risks, computer security is important.

Three key objectives that are at the heart of computer security:

1.Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. This term covers two related concepts:

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **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: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.This term covers two related concepts:

This term covers two related concepts:

- **Data integrity:** Assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.
- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

3.Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system .Assures that systems work promptly and service is not denied to authorized users.

Types of computer security

Computer security can be classified into four types:

1. Cyber Security: Cyber security means securing our computers, electronic devices, networks , programs, systems from cyber attacks. Cyber attacks are those attacks that happen when our system is connected to the Internet.

2. Information Security: Information security means protecting our system's information from theft, illegal use and piracy from unauthorized use. Information security has mainly three objectives: confidentiality, integrity, and availability of information.

3. Application Security: Application security means securing our applications and data so that they don't get hacked and also the databases of the applications remain safe and private to the owner itself so that user's data remains confidential.

4. Network Security: Network security means securing a network and protecting the user's information about who is connected through that network. Over the network, hackers steal, the packets of data through sniffing and spoofing attacks, man in the middle attack, war driving, etc, and misuse the data for their benefits.

Types of cyber attack

1. Denial of service attack or DOS: A denial of service attack is a kind of cyber attack in which the attackers disrupt the services of the particular network by sending infinite requests and temporary or permanently making the network or machine resources unavailable to the intended audience.

2. Backdoor: In a backdoor attack, malware, trojan horse or virus gets installed in our system and start affecting it's security along with the main file. Consider an example: suppose you are installing free software from a certain website on the Internet. Now, unknowingly, along with this software, a malicious file also gets installed, and as soon as you execute the installed software that file's malware gets affected and starts affecting your computer security. This is known as a backdoor.

3.Eavesdropping: Eavesdropping refers to secretly listening to someone's talk without their permission or knowledge. Attackers try to steal, manipulate, modify, hack information or systems by passively listening to network communication, knowing passwords etc. A physical example would be, suppose if you are talking to another person of your organization and if a third person listens to your private talks then he/she is said to eavesdrop on your conversation. Similarly, your conversation on the internet maybe eavesdropped by attackers listening to your private conversation by connecting to your network if it is insecure.

4. Phishing: Phishing is pronounced as "fishing" and working functioning is also similar. While fishing, we catch fish by luring them with bait. Similarly, in phishing, a user is tricked by the attacker who gains the trust of the user or acts as if he is a genuine person and then steals the information by ditching. Not only attackers but some certain websites that seem to be genuine, but actually they are fraud sites. These sites trick the users and they end up giving their personal information such as login details or bank details or card number etc. Phishing is of many types: Voice phishing, text phishing etc.

5. Spoofing: Spoofing is the act of masquerading as a valid entity through falsification of data(such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. Spoofing is of several types- email spoofing, IP address spoofing, MAC spoofing , biometric spoofing etc.

6. Malware: Malware is made up of two terms: Malicious + Software = Malware. Malware intrudes into the system and is designed to damage our computers. Different types of malware are adware, spyware, ransomware, Trojan horse, etc.

7. Social engineering: Social engineering attack involves manipulating users psychologically and extracting confidential or sensitive data from them by gaining their trust. The attacker generally exploits the trust of people or users by relying on their cognitive basis.

8. Polymorphic Attacks: Poly means "many" and morph means "form", polymorphic attacks are those in which attacker adopts multiple forms and changes them so that they are not recognized easily. These kinds of attacks are difficult to detect due to their changing forms.

Steps to ensure computer security

In order to protect our system from the above-mentioned attacks, users should take certain steps to ensure system security:

1. Always keep your Operating System up to date. Keeping it up to date reduces the risk of their getting attacked by malware, viruses, etc.

2. Always use a secure network connection. One should always connect to a secure network. Public wi-fi's and unsecured networks should be avoided as they are at risk of being attacked by the attacker.

3. Always install an Antivirus and keep it up to date. An antivirus is software that scans your PC against viruses and isolates the infected file from other system files so that they don't get affected. Also, we should try to go for paid anti-viruses as they are more secure.

4. Enable firewall. A firewall is a system designed to prevent unauthorized access to/from a computer or even to a private network of computers. A firewall can be either in hardware, software or a combination of both.

5. Use strong passwords. Always make strong passwords and different passwords for all social media accounts so that they cannot be key logged, brute forced or detected easily using dictionary attacks. A strong password is one that has 16 characters which are a combination of upper case and lower case alphabets, numbers and special characters. Also, keep changing your passwords regularly.

6. Don't trust someone easily. You never know someone's intention, so don't trust someone easily and end up giving your personal information to them. You don't know how they are going to use your information.

7. Keep your personal information hidden. Don't post all your personal information on social media. You never know who is spying on you. As in the real world, we try to avoid talking to strangers and sharing anything with them. Similarly, social media also have people whom you don't know and if you share all your information on it you may end up troubling yourself.

8. Don't download attachments that come along with e-mails unless and until you know that e-mail is from a genuine source. Mostly, these attachments contain malware which, upon execution infect or harms your system.

9. Don't purchase things online from anywhere. Make sure whenever you are shopping online you are doing so from a well-known website. There are multiple fraud websites that may steal your card information as soon as you checkout and you may get bankrupt by them.

10. Learn about computer security and ethics. You should be well aware of the safe computing and ethics of the computing world. Gaining appropriate knowledge is always helpful in reducing cyber-crime.

11. If you are attacked, immediately inform the cyber cell so that they may take appropriate action and also protect others from getting attacked by the same person. Don't hesitate to complain just because you think people may make your fun.

12. Don't use pirated content. Often, people try to download pirated movies, videos or web series in order to get them for free. These pirated content are at major risk of being infected with viruses, worms, or malware, and when you download them you end up compromising your system security.

THE OSI SECURITY ARCHITECTURE

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

- **Security attack** – Any action that compromises the security of information owned by an organization.
- **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 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.

SECURITY ATTACK

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of passive attacks and active attacks. A **passive** attack attempts to learn or make use of information from the system but does not affect system resources. An **active** attack attempts to alter system resources or affect their operation.

- Security attacks could be broadly categorized as

Passive attacks

- **Release of message contents**
- **Traffic analysis**

Active attacks

- **Masquerade (Fabrication)**
- **Replay**
- **Modification**
- **Denial of service**

Passive attacks:

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks. The goal of the opponent is to obtain information that is being transmitted.

Passive attacks are of two types:

1) **Release of message contents:** A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

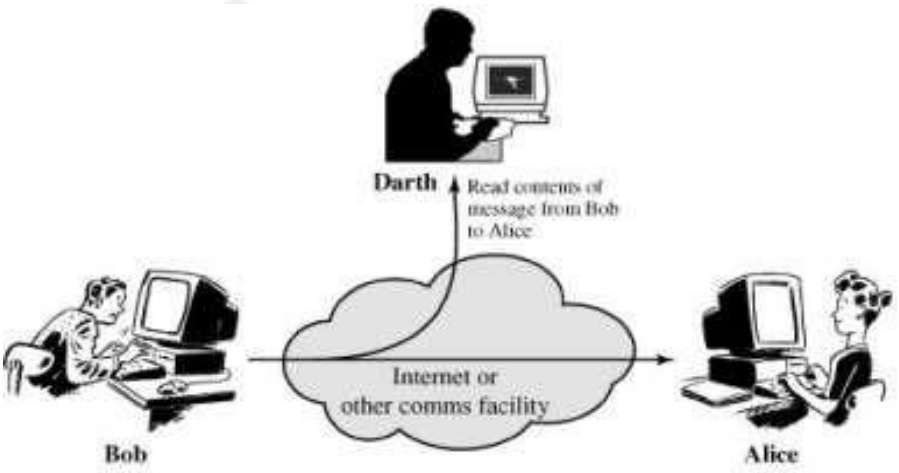


Figure 3: Release of message contents

2) **Traffic analysis**: Even though encryption protection exists in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place

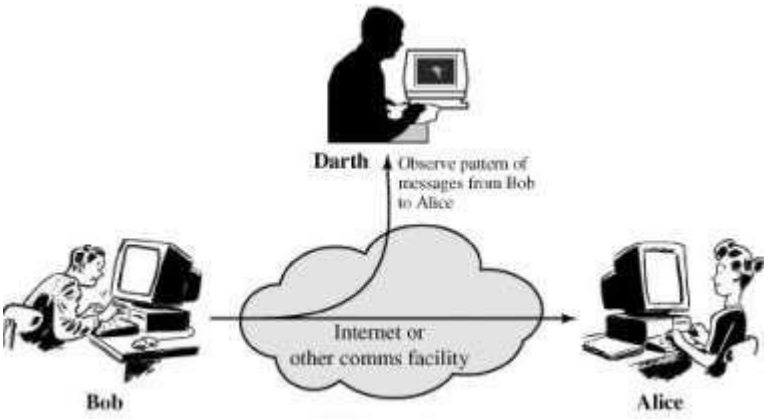


Figure 4: Traffic Analysis

Active attacks:

These attacks involve some modification of the data stream or the creation of a false stream. It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

These attacks can be classified in to four categories:

1) Masquerade (Fabrication) – One entity pretends to be a different entity.

Figure 5: Masquerade

2) Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

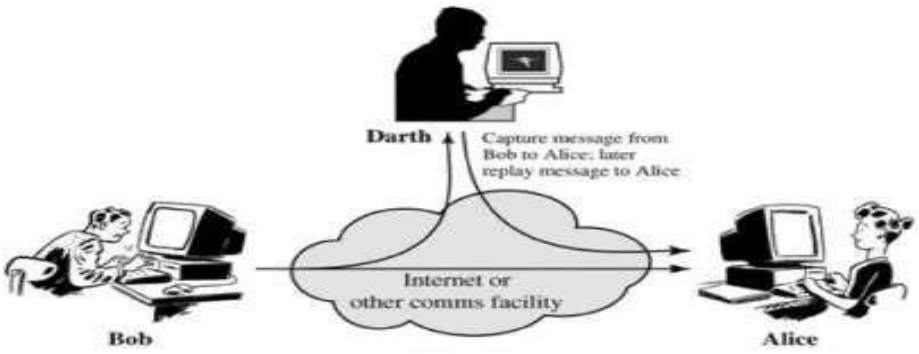


Figure 6: Replay

3) Modification – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

Figure 7: Modification

4) Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

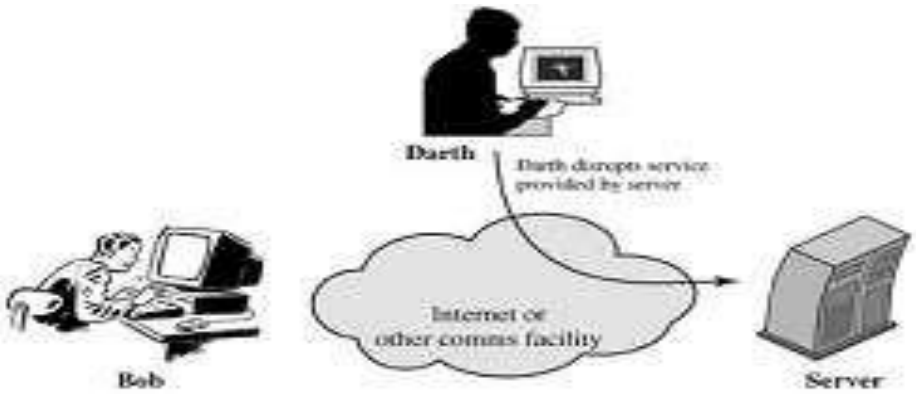


Figure 8: Denial of service

SECURITY SERVICES

X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers. As per RFC 2828, the definition is " **a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms".**

The classification of security services are as follows:

1. **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. Example: printing, displaying and other forms of disclosure.

2. **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false. the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

Two specific authentication services are defined in X.800:

- **Peer entity authentication:** Provides for the corroboration of the identity of a peer entity in an association. It is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.
- **Data origin authentication:** Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

3) **Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

4) **Non repudiation:** Requires that neither the sender nor the receiver of a message be able to deny the transmission.

5) **Access control:** Requires that access to information resources may be controlled by or the target system.

6) **Availability:** Requires that computer system assets be available to authorized parties when needed.

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

1) 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.

2) 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.

3) 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.

4) 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.

5) 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.

SECURITY MECHANISMS

The security mechanisms defined by X.800 are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service. X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms.

A **reversible** encipherment mechanism is simply an encryption algorithm that allows data
to be encrypted and subsequently decrypted. **Irreversible** encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

Specific security mechanisms are encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control and notarization.

Pervasive security mechanisms are trusted functionality, security labels, event detection, security audit trails, security recovery.

SPECIFIC SECURITY MECHANISMS

Encipherment

The use of mathematical algorithms to transformdata into a form that is not readily intelligible. Thetransformation and subsequent recovery of thedata depend on an algorithm and zero or moreencryption keys.

Digital Signature

Data appended to, or a cryptographic transformationof, a data unit that allows a recipient of the data unitto prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control

A variety of mechanisms that enforce access rights toresources.

Data Integrity

A variety of mechanisms used to assure the integrityof a data unit or stream of data units.

Authentication Exchange

A mechanism intended to ensure the identity of anentity by means of information exchange.

Traffic Padding

The insertion of bits into gaps in a data stream tofrustrate traffic analysis attempts.

Routing Control

Enables selection of particular physically secureroutes 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 certainproperties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Trusted Functionality

That which is perceived to be correct with respectto some criteria (e.g., as established by a security policy).

Security Label

The marking bound to a resource (which may be adata unit) that names or designates the security attributes of that resource.

Event Detection

Detection of security-relevant events.

Security Audit Trail

Data collected and potentially used to facilitate asecurity audit, which is an independent review and examination of system records and activities.

Security Recovery

Deals with requests from mechanisms, such as eventhandling and management functions, and takes recovery actions.

A MODEL FOR NETWORK SECURITY

A message that needs to be transferred from one party to another across some sort of internet must cooperate for the exchange of the message. The two parties i.e., the sender and receiver are also called as principals. For the transfer of messages,

- A logical information channel needs to be established between the sender and the receiver.
- communication protocols (e.g., TCP/IP) must be used by the sender and receiver.

A model for network security is shown in Figure 1.

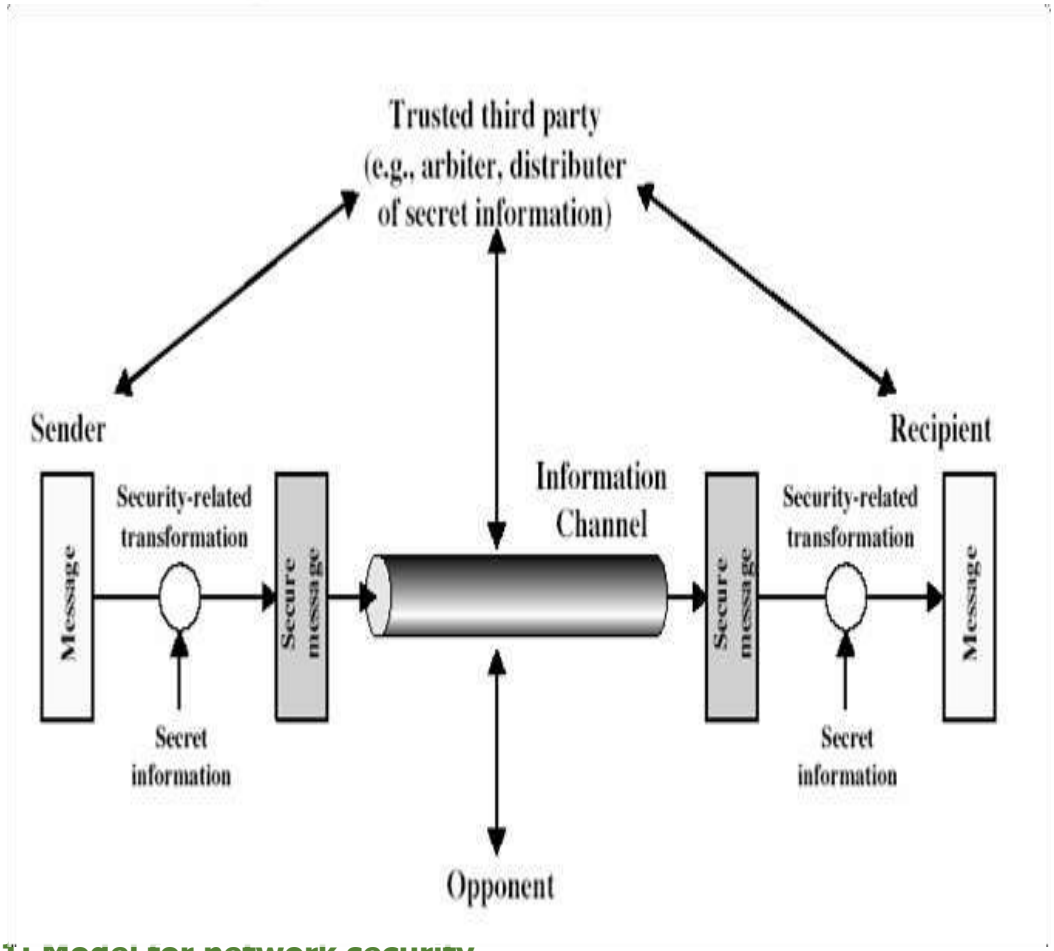


Figure 1: Model for network security.

- All the techniques for providing security have two components:

1. A security-related transformation on the information to be sent.

Examples:

- the encryption of the message, which scrambles the message so that it is unreadable by the opponent,
- addition of a code based on the contents of the message, which can be used to verify the identity of the sender

2. Some secret information shared by the two principals (sender and receiver)

Examples:

- An Encryption key used along with the transformation to scramble the message before its transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

Basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
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.

The security mechanisms needed to cope with unwanted access is shown in Figure 2. The hacker is someone who simply gets satisfaction from breaking and entering a computer system. **Viruses and worms** are two examples of software attacks. Such attacks are introduced into a system by means of a disk that contains the unwanted logic provided along with useful software

The **gatekeeper** function includes password-based login procedures that are designed to allow only authorized users and deny all others. The second level of security consists of a variety of **internal security controls** that detects the presence of unwanted intruders.

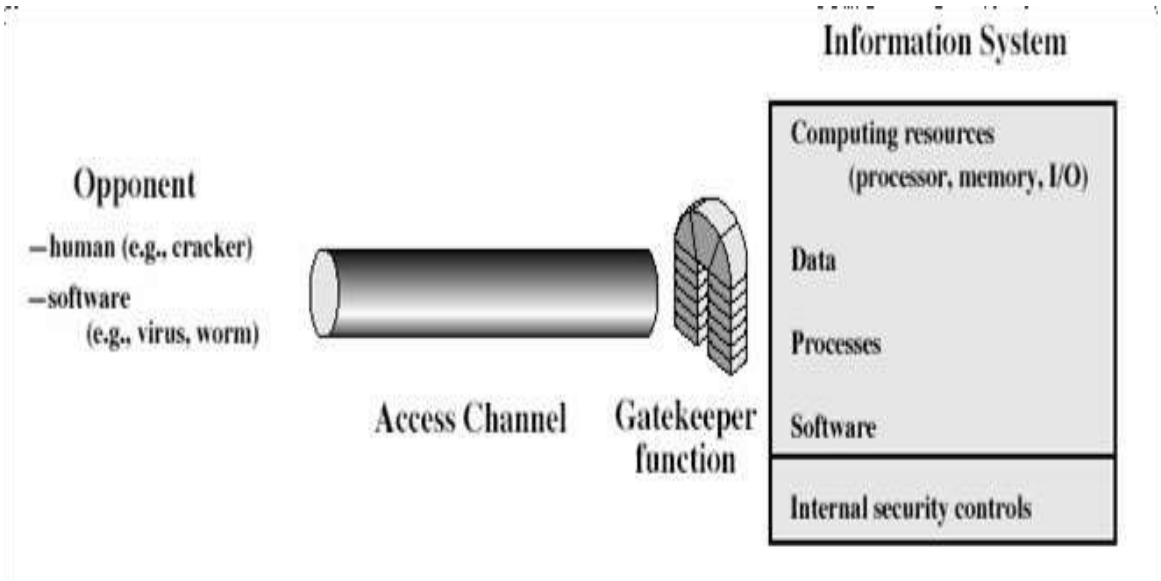


Figure 2: Network Access Security Model

Another type of unwanted access is the placement of logic in a computer system that that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

- Information access threats intercept or modify data on behalf of users who should not have access to that data.
- Service threats exploit service flaws in computers to inhibit use by legitimate users.

Classical Encryption Techniques

Cryptographic systems are characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to ciphertext.

All encryption algorithms are based on two general principles:

- **Substitution**, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and
- **Transposition**, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

2. The number of keys used.

- **Symmetric encryption** : If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.
- **Asymmetric encryption:** If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. The way in which the plaintext is processed.

- Block cipher processes the input one block of elements at a time, producing an output block for each input block.
- Stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Some basic concepts are defined below:

- **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 .
- **Plaintext** : The original intelligible message
- **Cipher text**: The transformed message
- **Cipher** : An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- **Key**: Some critical information used by the cipher, known only to the sender& receiver
- **Encipher (encode)** : The process of converting plaintext to cipher text using a cipher and a key
- **Decipher (decode)** : the process of converting cipher text back into plaintext using a cipher and a key
- **Cryptanalysis** : The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking
- **Cryptology** : Both cryptography and cryptanalysis

SYMMETRIC CIPHER MODEL

A symmetric encryption scheme has five ingredients :

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm.The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm.

Two requirements for secure use of symmetric encryption:

- a strong encryption algorithm
- a secret key known only to sender / receiver

$$Y = E_K(X)$$

$$X = D_K(Y)$$

- assume encryption algorithm is known
- implies a secure channel to distribute key

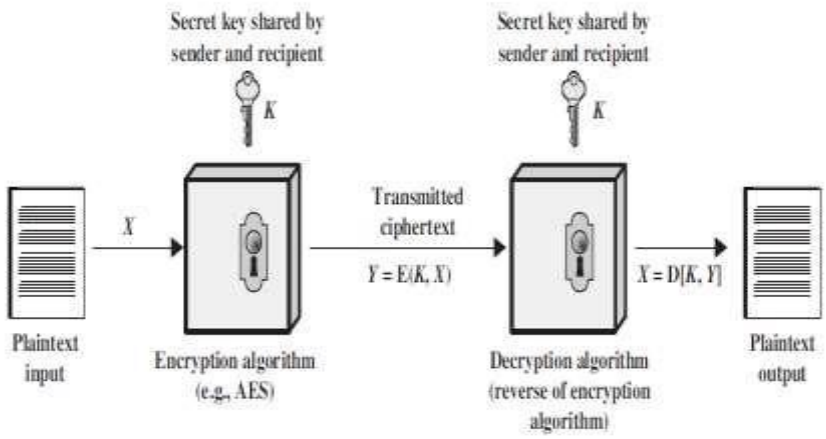


Figure : Simplified Model of Symmetric Encryption

A source produces a message in plaintext, X = [X1, X2, … , XM] where M are the number of letters in the message. A key of the form K = [K1, K2, …, KJ] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, …, YN]. This can be expressed as

$$Y = E_K(X)$$

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D_K(Y)$$

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms. If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate. Often if the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate. The essential elements of a symmetric encryption scheme is shown in the figure below:

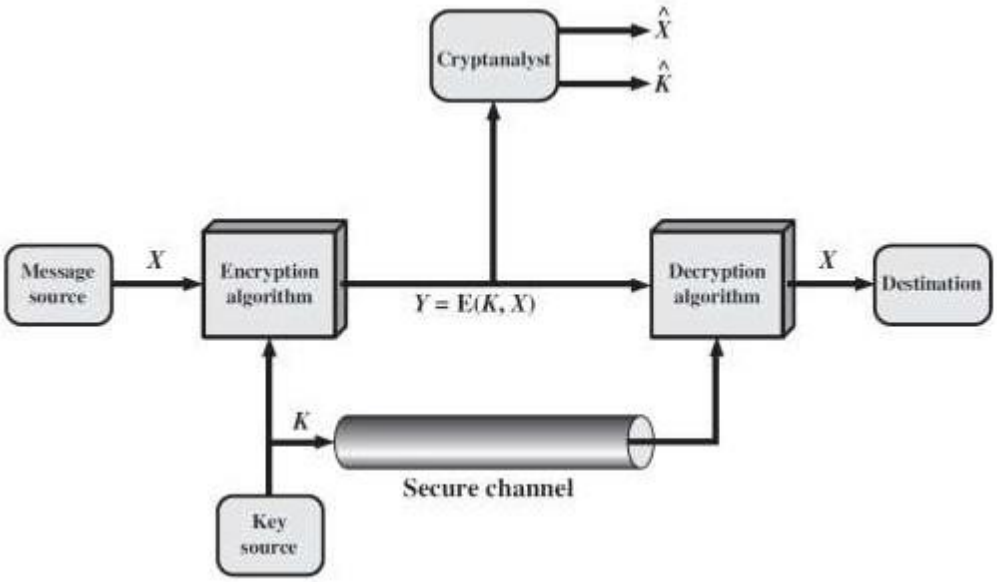


Figure: Model of Symmetric Cryptosystem

SUBSTITUTION TECHNIQUES

1. Caesar cipher (or) shift cipher
2. Playfair cipher
3. Hill cipher
4. Polyalphabetic ciphers
   1. Vigenere cipher
   2. Vernam cipher
   3. One Time Pad cipher

TRANSPOSITION TECHNIQUES

1. Rail fence
2. Row Transposition Ciphers

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

CAESAR CIPHER (OR) SHIFT CIPHER

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

- **Example 1:**
  Plain text: pay more money
  Cipher text: SDB PRUH PRQHB
- **Example 2:**

  Plain text : Return to home
  Cipher text : UHWXUQ WR KRPH
  Note that the alphabet is wrapped around, so that letter following 'z' is 'a'.
  For each plaintext letter p, substitute the cipher text letter c such that

- $$C = E(P) = (P+3) \bmod 26$$

  A shift may be any amount, so that general Caesar algorithm is

- $$C = E(P) = (P+k) \bmod 26$$

- Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$$P = D(C) = (C-k) \bmod 26$$

- **Disadvantages**
  The encryption and decryption algorithm are known.
- There are only 25 keys to try.
- The language of the plain text is known

PLAYFAIR CIPHER

The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be '**monarchy**'. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order. The letter 'i' and 'j' count as one letter. Plaintext is encrypted two letters at a time according to the following rules:

- Repeating plaintext letters that would fall in the same pair are separated with a filler letter such as 'x'.
- Plaintext 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 following the last.
- Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.
- Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

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

- **Example:**

Plaintext = meet me at the school house

Splitting two letters as a unit =>me et me at th es ch ox ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

- **Example 2:**

  Plain text : Balloon

  Repeating plain text letter that fall in the same pair are repeated with the filler letter 'X'.

  Plain text : ba lx lo on

  Cipher text : IB SU PM NA

Strength of playfair cipher

- Playfair cipher is a great advance over simple mono alphabetic ciphers.
- Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual digram is more difficult.
- Frequency analysis is much more difficult.

Advantage

- It is difficult to identify particular diagrams.
- Frequency analysis is more difficult.

Disadvantages

- It is relatively easy to be broken.
- The sufficient number of cipher text letter is very small.

Hill Cipher

- Hill cipher is a poly-graphic substitution cipher based on linear algebra.
- Hill used matrices and matrix multiplication to mix up the plain text.
- Each letter is represented by a number modulo 26.
- To encrypt a message, each block of 'n' letters is multiplied by an invertible n x n matrix, again modulus 26.
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

Example:

$$\text{Key K} = \begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix}$$

Encryption : blah

$$bl = (1, 11)\begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix} = (101, 49) \bmod 26$$

$$= 23, 23$$

$$= (x, x)$$

$$\text{CT} = x, x$$

$$ah = (0, 7)\begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix} = (63, 28) \bmod 26$$

$$= (11, 2)$$

Decryption

$\boxed{K^{-1}\,(CT) \bmod 26}$

$$K^{-1} = \det(K)^{-1}\begin{pmatrix} K_{2,2} & -K_{1,2} \\ -K_{2,1} & K_{1,1} \end{pmatrix}$$

$$K = \begin{pmatrix} 4 & -5 \\ -9 & 2 \end{pmatrix} = -37 \bmod 26$$

$$= 15 \bmod 26$$

$$K^{-1} = 15^{-1} \bmod 2x$$

$$\boxed{15 \times x = 1 \bmod 26}$$

Note:
– 37 mod 26
Two times 26 gives 52.
Difference of 52 and– 37 yields 15

$x = 7$ & $K^{-1} = 7$

$$\therefore 7\begin{pmatrix} 4 & -5 \\ -9 & 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 28 & -35 \\ -63 & 14 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 2 & 17 \\ 15 & 14 \end{pmatrix} \bmod 26$$

$$= (23, 23)\begin{pmatrix} 2 & 17 \\ 15 & 14 \end{pmatrix} \bmod 26$$

$$= (23 \times 2 + 23 \times 15) \bmod 26, (23 \times 17 + 23 \times 14) \bmod 26$$

$$(46 + 345) \bmod 26, (391 + 322) \bmod 26$$

$$= 1, 11$$

$$= b, l$$

$$= (11, 2)\begin{pmatrix} 2 & 17 \\ 15 & 14 \end{pmatrix}$$

$$= (11 \times 2 + 2 \times 15, 11 \times 17 + 2 \times 14) \bmod 26$$

$$= (52, 215) \bmod 26$$

$$= 0, 7$$

$$= a, h$$

$\boxed{\text{plain text} = \text{b l a h}}$

POLYALPHABETIC CIPHERS

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common.

- A set of related monoalphabetic substitution rules are used
- A key determines which particular rule is chosen for a given transformation.
- To encrypt a message, a key is needed that is as long as the message, ignoring spaces and punctuation.

- **Example:**

  Plain text : Good Morning

  Key : text

  Solution : G o o d M o r n i n g

  T e x t t e x t t e x

  Cipher text : z s l w f s o g b r d

KEY LETTERS	PLAIN TEXT															
		a	b	c	d	e	f	g	h	i	j	k	...	x	y	z
	a	A	B	C	D	E	F	G	H	I	J	K	...	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	...	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	...	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	...	A	B	C
	e	E	F	G	H	I	J	K	L	M	N	O	...	B	C	D
	f	F	G	H	I	J	K	L	M	N	O	P	...	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	...	D	E	F
	:	:	:	:	:	:	:	:	:	:	:	:	...	:	:	:
	x	X	Y	Z	A	B	C	D	E	F	G	H	...			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	...			X
	z	Z	A	B	C	D	E	F	G	H	I	J	...			Y

- To encrypt, pick the letter in the plain text and its corresponding letter in the keyword. The plain text is considered as row index and the keyword letter as column index.

Here in the above example letter 'G' from row and letter 'T' from colum intersects and produces the letter 'Z'.

- For decryption, pick the letter from the keyword as column index and search for the cipher text. The intersection of corresponding row gives the plain text.
- In our example letter 't ' is considered as column index searching for cipher text z'. The corresponding row index produces the plain text 'g'.

Cipher text : zslw fsogbrd

Key : text texttex

Plain text : Good morning

Advantage

- Multiple cipher text letters are used for each plain text letters.

VERNAM CIPHER

The ultimate defense against such a cryptanalysis is to choose akeyword that is as long as the plaintext and has no statistical relationship to it. This cipher works on binary data (bits) rather than letters. The system can beexpressed succinctly as follows :

- $ci = pi \oplus ki$

where

pi= ith binary digit of plaintext

ki= ith binary digit of key

ci= ith binary digit of ciphertext

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

Thus, ciphertext is generated by performing the bitwise XOR of the plaintextand the key. Because of the use of the properties of the XOR, decryption simply involves the same bitwise operation:

- $pi = ci \oplus ki$

- Example:

  Plaintext = 0 0 1 0 1 0 0 1

  Key = 1 0 1 0 1 1 0 0

  Ciphertext = 1 0 0 0 0 1 0 1

ONE TIME PAD CIPHER:

An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security. Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, known as a **one-time pad**, is unbreakable.

- It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

- Suppose that we are using a Vigenère scheme with 27 characters in which the twenty-seventh character is thespace character, but with a one-time key that is as long as the message.

  Consider the ciphertext

  ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

- Two different decryptions using two different keys:

  Ciphertext : ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

  Key: *pxlmvmsydofuyrvzwctnlebnecvgdupahfzzlmnyih*

  Plaintext: mr mustard with the candlestick in the hall

Ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Key: *pftgpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt*

Plaintext: miss scarlet with the knife in the library.

Advantage

- It is a highly source method because it generates random keys

Disadvantages

- Sending the key securely is a problem.
- Randomness is also a disadvantage.

TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

RAIL FENCE:

- It is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2, the message is written as follows:

m e e t a t t h e s c o l o s
e t o h u
h e

The encrypted message is

MEATECOLOSETTHSHOHUE

ROW TRANSPOSITION CIPHER:

- A more complex scheme is to 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 columns then becomes the key of the algorithm.

- **Example:**

  Plaintext = meet at the school house

  Key = 4 3 1 2 5 6 7

  Plaintext = m e e t a t t
  h e s c h o o
  l h o u s e z

  Cipertext = ESOTCUEEHMHLAHSTOETOZ

STEGANOGRAPHY

A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text. A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. e.g., (i) the sequence of first letters of each word of the overall message spells out the real (hidden) message. (ii) Subset of the words of the overall message is used to convey the hidden message. Various other techniques have been used historically, some of them are

- **Character marking** – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.

- **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.
- **Pin punctures** – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.
- **Typewritten correction ribbon** – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of Steganography

- Requires a lot of overhead to hide a relatively few bits of information.
- Once the system is discovered, it becomes virtually worthless.

MODERN CRYPTOGRAPHY

Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.

Characteristics of Modern Cryptography

There are four major characteristics that separate modern cryptography from the classical approach. Table below shows the differences between Traditional Encryption and Modern Encryption

Classic Cryptography	Modern Cryptography
For making ciphertext, manipulation is done in the characters of the plaintext	For making ciphertext, operations are performed on binary bit sequence
The whole of the ecosystem is required to communicate confidentiality	Here, only the parties who want to execute secure communication possess the secret key
These are weaker as compared to modern encryption	The encryption algorithm formed by this encryption technique is stronger as compared to traditional encryption algorithms
It believes in the concept of security through obscurity	Its security depends on the publicly known mathematical algorithm

Types of Modern Cryptography

Different algorithms have come up with powerful encryption mechanisms incorporated in them. It gave rise to two new ways of encryption mechanism for data security. These are:

- o Symmetric key encryption
- o Asymmetric key encryption

Key

It can be a number, word, phrase, or any code that will be used for encrypting as well as decrypting any ciphertext information to plain text and vice versa. Symmetric and asymmetric key cryptography is based on the number of keys and the way these keys work. Let us know about both of them in details:

Symmetric key encryption

Symmetric key encryption technique uses a straight forward method of encryption. Hence, this is the simpler among these two practices. In the case of symmetric key encryption, the encryption is done through only one secret key, which is known as "Symmetric Key", and this key remains to both the parties. The same key is implemented for both encodings as well as decoding the information. So, the key is used first by the sender prior to sending the message, and on the receiver side, that key is used to decipher the encoded message. One of the good old examples of this encryption technique is Caesar's Cipher. Modern examples and algorithms that use the concept of symmetric key encryption are RC4, QUAD, AES, DES, Blowfish, 3DES, etc.

Asymmetric Key Encryption

Asymmetric Encryption is another encryption method that uses two keys, which is a new and sophisticated encryption technique. This is because it integrates two cryptographic keys for implementing data security. These keys are termed as Public Key and Private Key. The "public key", as the name implies, is accessible to all who want to send an encrypted message. The other is the "private key" that is kept secure by the owner of that public key or the one who is encrypting.

Encryption of information is done through public key first, with the help of a particular algorithm. Then the private key, which the receiver possesses, will use to decrypt that encrypted information. The same algorithm will be used in both encodings as well as decoding.

Examples of asymmetric key encryption algorithms are Diffie-Hellman and RSA algorithm.

Perfect Security

Definition

Perfect security, as defined by Claude Shannon, means that a ciphertext reveals no information about the original plaintext, even with infinite computational power.

Mathematically, this is expressed as:

$$H(M|C) = H(M)$$

where:

H(M) is the Entropy (uncertainty) of the plaintext.

H(M|C) is the Entropy of the plaintext given the ciphertext.

One-Time Pad (OTP)

The only known cryptosystem providing perfect security.

Key properties:

- Key length must be at least as long as the message.
- Key must be truly random.
- Key must be used only once and never reused.
- Key must be kept completely secret.

Despite its theoretical strength, OTP is impractical for most applications due to key management challenges.

Limitations of Perfect Security

- Requires massive key sizes and flawless key management.
- Impractical for large-scale communication, leading to the adoption of computationally secure systems.

Information Theory

Information theory plays a foundational role in cryptography and network security, providing the mathematical framework to measure and ensure confidentiality, integrity, and availability of information. Here's an overview of its key contributions:

Key Concepts from Information Theory in Cryptography:

a. Entropy (H)

Definition: Measures the uncertainty or randomness in a data source.

Mathematical Form:

$$H(X) = -\sum p(x) \log_2 p(x)$$

Relevance: Higher entropy indicates more secure cryptographic keys, as it makes brute-force attacks harder.

b. Mutual Information (I)

Definition: Measures the amount of information shared between two variables.

Mathematical Form:

$$I(X;Y) = H(X) - H(X|Y)$$

Relevance: Used in cryptanalysis to determine how much information an attacker can gain.

c. Shannon's Perfect Secrecy

Definition: A cryptosystem achieves perfect secrecy if the ciphertext reveals no information about the plaintext.

Condition: $H(M|C) = H(M)$

It denotes that knowing the ciphertext does not reduce the uncertainty about the plaintext.

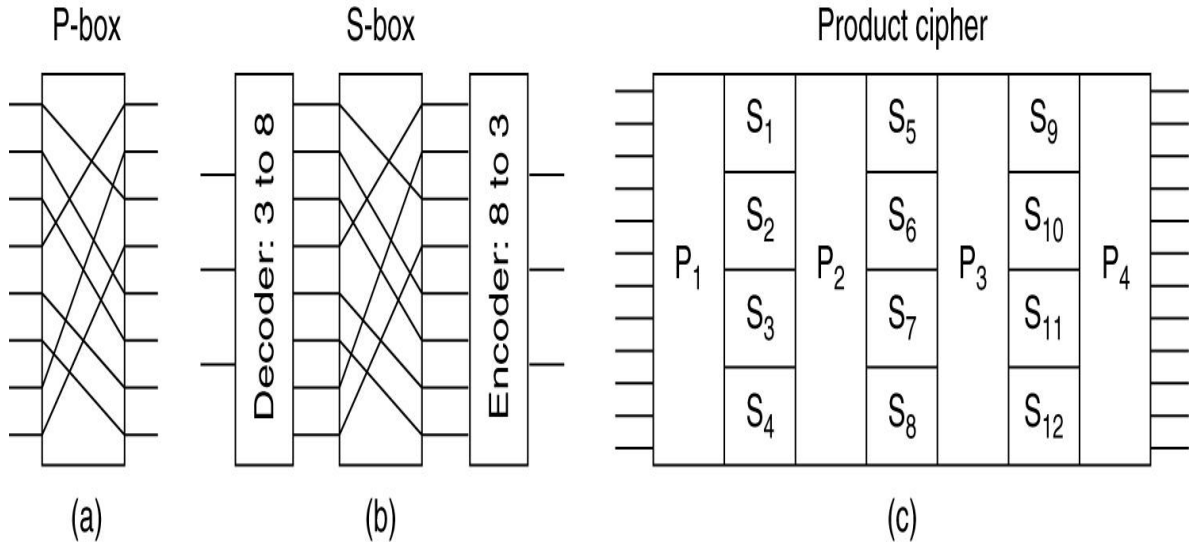
Example: The one-time pad (OTP) is the only known system achieving perfect secrecy.

Product Cryptosystems

A product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis.

The product cipher combines a sequence of simple transformations such as substitution (S-box), permutation (P-box), and modular arithmetic. For transformation involving reasonable number of n message symbols, both of the foregoing cipher systems (the S-box and P-box) are by themselves wanting.

The combination could yield a cipher system more powerful than either one alone. This approach of alternatively applying substitution and permutation transformation has been used by IBM in the Lucifer cipher system, and has become the standard for national data encryption standards such as the Data Encryption Standard and the Advanced Encryption Standard. A product cipher that uses only substitutions and permutations is called a SP-network. Feistel ciphers are an important class of product ciphers.



Basic elements of product ciphers. (a) P-box. (b) S-box. (c) Product.

Cryptanalysis

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

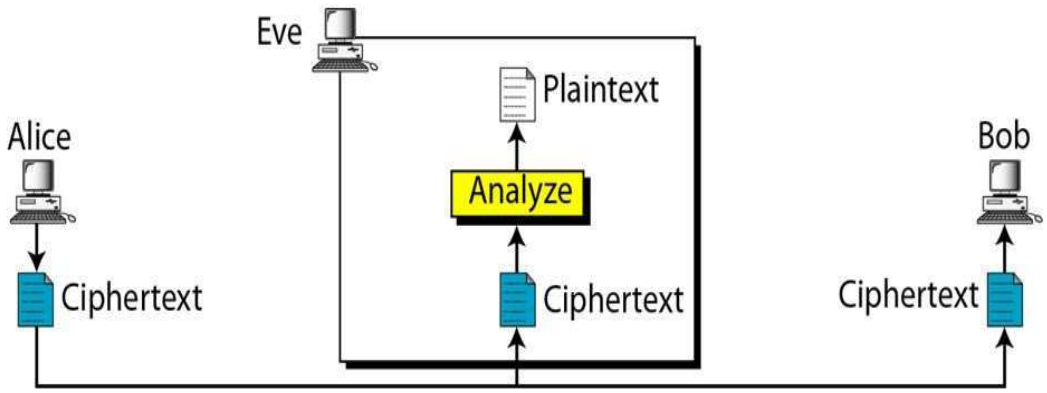
There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Cipher text only – A copy of cipher text alone is known to the cryptanalyst.

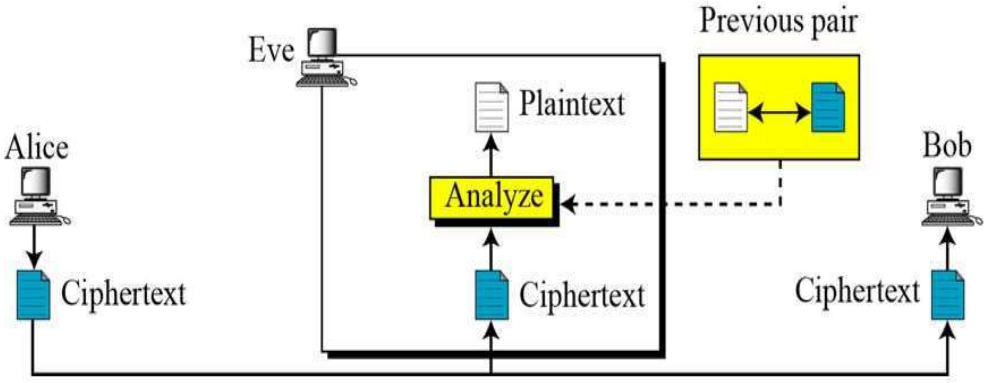
The attacker only has access to one or more encrypted messages but knows nothing about the plaintext data

- the encryption algorithm being used
- any data about the cryptographic key being used

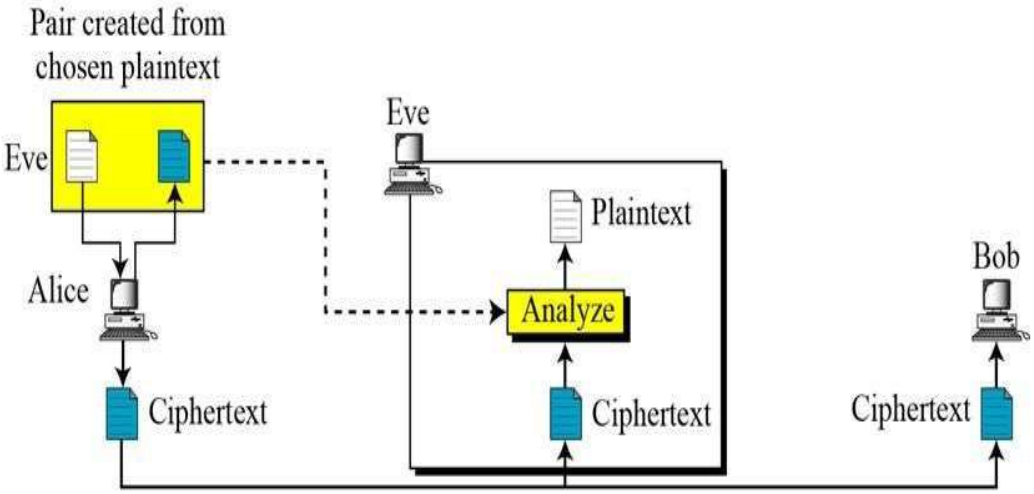
This is the type of challenge that intelligence agencies often face when they have intercepted encrypted communications from an opponent



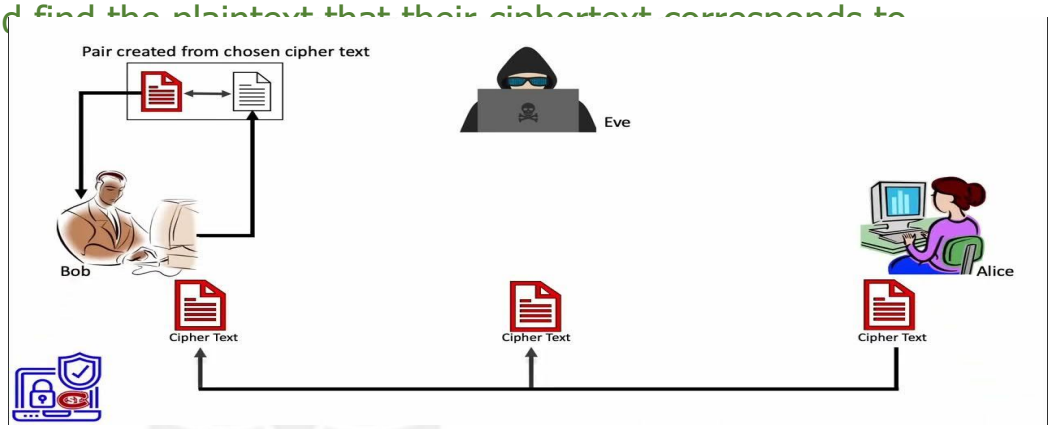
Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext. The analyst may have access to some or all of the plaintext of the ciphertext. The analyst's goal in this case is to discover the key used to encrypt the message and decrypt the message. Once the key is discovered, an attacker can decrypt all messages that had been encrypted using that l



Chosen plaintext – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key. The analyst either knows the encryption algorithm or has access to the device used to do the encryption. The analyst can encrypt the chosen pl



Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key. A chosen ciphertext attack sends a fake ciphertext and retrieves the correctly decrypted message. In particular, an attacker needs the decrypted version of their own ciphertext. If successful at that, the attacker can figure out the keys. This means they can decrypt other parties' messages and forge new ones. A system's vulnerability to this attack depends on the encryption technique and how easy it is for an attacker to eavesdrop and find the plaintext that their ciphertext corresponds to.



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding • ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Assignment

Set – I

1. Let message = "graduate", Key = "word", find ciphertext and then convert into plain text using playfair cipher.

2. Construct a play fair matrix with a

   a)key=largest

   b)key=occurrence

   Make a reasonable assumption about how to treat redundant letters in a key.

3. Using

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

Encrpty the message p= "must see you over calgon west coming at once"

4. A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter a. For example, for a = 2 and b = 3, then

   E([a, b], 0) = E([a, b], 13) = 3.

   a. Are there any limitations on the value of b? Explain why or why not.

   b. Determine which values of a are not allowed.

   Provide a general statement of which values of a are and are not allowed. Justify your statement. Justify your statement.

5. Perform encryption and decryption using Hill Cipher. Message is "Pay more money" with

   the following key matrix

   k = 17 17 5

   21 18 21

Assignment

Set– 2

1. Perform encryption and decryption using Hill Cipher. Message is "NET" with the following key matrix. (13)

   k = 17 17 5
   21 18 21
   2 2 19

2. Explain Play fair cipher substitution technique in detail and encrypt the message "networksecurity" with the key "SCISSORS" .

3. Explain Vignere Cipher and convert the plain text "If the sight of the blue skies fills you with joy, if a blade of grass springing up in the fields has power to move you, if the simple things of nature have a message that you understand, rejoice, for your soul is alive" with keyword as " CSE DEPARTMENT" .

4. Encrypt using play fair cipher using the keyword 'PARK' and plain text " JURASSIC KINGDOM".

5. Encrypt using play fair cipher using the keyword 'MONARCHY' and plain text "SWARAJ IS MY BIRTH RIGHT'.

Assignment

Set -3

1. Demonstrate encryption and decryption process in hill cipher. Consider m = "sh" and key = hill".

2. Explain the Vignere cipher and perform the encryption and decryption process of given input " Cryptography and network security" and Key "Passphrase".

3. Compute the ciphertext for the plaintext "SECURE WORLD" using the Vignere cipher with key "CRYPTO". Also verify whether it is feasible to generate back the Plain text.

4. Encrypt the following using play fair cipher using the keyword 'DECEPTIVE' and plaintext "WAIT NEAR SCHOOL HOUSE'.

5 . P=COMPUTER SCIENCE AND ENGINEERING
K=SECURITY

   a. Perform Caesar cipher with key=4
   b. Perform Rail fence cipher
   c. Perform Row and column transposition technique k=6,4,3,1,2,5
   d. Perform Play fair
   e. Vigenere cipher.

Assignment

Set - 4

1. List out any two di-gram, two tri-gram. Discuss the application of di-gram and tri-gram in cryptography.

2. Given the keyword SECURITY, encrypt the following plaintext using the autokey system.

   We are discovered. Save yourself.

   Given a long ciphertext which has been encrypted with the autokey system, how can one find the secret key used?

3. Compute the ciphertext for the plaintext "SECURE WORLD" using the Vignere cipher with key "CRYPTO". Also verify whether it is feasible to generate back the Plain text.

4. Compute the ciphertext for the plaintext "Get well soon" using the playfair cipher with key "care". Also verify whether it is feasible to generate back the plain text.

5. Find modulo exponentiation for 5^117 mod 19

Assignment

Set – 5

1. The plaintext is COMMUNICATION and the key used to encipher the plaintext is COMPUTER. Perform Vignere cipher to get the cipher text.

2. Explain the Caesar cipher and perform the encryption and decryption process of given input plain text" welcome to RMK College".

3. Explain the Rail fences cipher and perform the encryption and decryption process of given input "Simple Snippets" , N=2.

4. Encrypt the message "this is an exercise" using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext.

5. Find modulo exponentiation for 64^72 mod 13

Real life case study

- Cryptography in the Field of Social Media.
- High Performance Elliptic Curve Engine for Car-to-Car Communication
- Lightweight Cryptography for RFID Tags
- Side-Channel Attacks against Remote Keyless Entry Systems.

PART-A TWO MARKS Q & A

- **Define cryptography .(CO1,K1)**

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

- **Define cryptanalysis. (CO2,K1)**

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code."

- **Define security Attack, mechanism and service. (CO1,K1)**

Security attack: Any action that compromises the security of information owned by an organization.

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

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.

- **Distinguish Threat and Attack .(CO1,K1)**

Threat -A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack -An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

- **Differentiate active attacks and passive attacks. (CO1,K1)**

A **passive attack** attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are the release of message contents and traffic analysis.

An **active attack** attempts to alter system resources or affect their operation. It can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

- **What is an unconditionally secure cipher? (CO1,K1)**

An unconditionally secure cipher is one that does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. That is, no matter how much time an opponent has, it is impossible for him to decrypt the ciphertext, simply because the required information is not there. Example: One-time pad

- **Differentiate block and stream cipher (CO1,K1)**

  A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

- **What are the essential ingredients of a symmetric cipher?(CO1,K1)**

  - Plain Text
  - Encryption algorithm
  - Secret Key
  - Decryption algorithm
  - Cipher text

- **Specify four categories of security threats (CO1,K1)**

  - Interruption
  - Interception
  - Modification
  - Fabrication

- **What is brute-force attack? (CO1,K1)**

  The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

- **List the types of cryptanalysis attack (CO2,K1)**

  - Cipher text only
  - Known plain text
  - Chosen plaintext
  - Chosen cipher text
  - Chosen text

- **Compare Substitution and Transposition techniques. (CO2,K1)**

A **substitution technique** is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.1 If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Example: Caesar cipher, monoalphabetic cipher, Playfair cipher,

In **transposition technique,** a very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Example: rail fence

- **Define Steganography. (CO2,K1)**

A plaintext message may be hidden . The methods of steganography conceal the existence of the message

Example Techniques: character marking, invisible ink, pin punctures, type writer correction ribbon.

- **What is a computationally secure cipher?(CO1,K1)**

A computationally secure cipher is one which satisfies any one of the following two criteria:

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

- **What are the two problems with the one-time pad?(CO2,K1)**

- Generating large quantities of random keys.
- Key distribution and protection.

- **Compare Vernam Cipher and One-time Pad(CO2,K1)**

VERNAM CIPHER

- Key is eventually repeated
- It works on binary data rather than letters.

ONE-TIME PAD

- Key never repeated
- It works on letters.

- **What are the techniques that have been used historically for steganography?(CO2,K1)**

- Character marking
- Invisible ink
- Pin punctures
- Typewriter correction ribbon

- **What are the two general approaches to attacking a cipher?(CO1,K1)**

- ***Cryptanalysis:*** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.

- ***Brute-force attack:*** The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

- **What are the various types of cryptanalytic attacks?(CO2,K1)**

- Ciphertext only
- Known Plaintext
- Chosen plaintext
- Chosen ciphertext
- Chosen text

- **What is computer crime?(CO1,K1)**

  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.

- **List the types of computer crime. (CO1,K1)**

- Computers as targets
- Computers as storage devices
- Computers as communications tools

- **What is Intellectual property? (CO1,K1)**

  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.

- **What are the types of Intellectual property. (CO1,K1)**

- Copyright
- Patents
- Trademarks

- **What are the Intellectual Property that are relevant to Network and Computer Security? (CO1,K1)**

- Software
- Databases
- Digital content
- Algorithms

- **What are the Ethical issues related to Computers and Information security? (CO1,K1)**

- Repositories and processors of information
- Producers of new forms and types of assets
- Instruments of acts
- Symbols of intimidation and deception

- **What is Modern cryptography? (CO2,K1)**

Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.

- **What are the characteristics of Modern Cryptography? (CO2,K1)**

- It operates on binary bit sequences.
- It relies on publicly known mathematical algorithms for coding the information.
- Modern cryptography requires parties interested in secure communication to possess the secret key only.

- **What is cryptosystem? (CO1,K1)**

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services.

A cryptosystem is also referred to as a cipher system.

- **What is product cryptosystem? (CO2,K1)**

Product cryptosystem is a block cipher that repeatedly performs substitutions and permutations, one after the other, to produce ciphertext.

- **What is Symmetric Key Encryption? (CO1,K1)**

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems

- **What is Asymmetric Key Encryption? (CO1,K1)**

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption.

Part B

1. Explain the following: (CO1, K2)
   (a) Playfair cipher.
   (b) Vernam cipher in detail.
2. Discuss in detail about Steganography (CO1, K2)
3. Compute the ciphertext for the plaintext "SECURE WORLD" using the playfair cipher with key "CRYPTO. Also verify whether it is feasible to generate back the plaintext, (CO1, K3)
4. "Explain the OSI security architecture. (CO1, K2)
5. Explain various transposition ciphers in detail. (CO1, K2)
6. Explain in detail about various types of attacks. (CO1, K2)
7. Illustrate the legal and ethical aspects of security (CO1, K3)
8. Explain in detail (CO1, K2)
   1. Product cryptosystem
   2. Perfect security
9. Compute the ciphertext using Hill cipher for the plaintext "PAY ORE MONEY" and key given below. Verify whether your ciphertext reproduces plaintext. (CO1,K3)

3	10	20
20	9	17
9	4	17

10. Describe a classification of computer crime based on the role that the computer plays in the criminal activity. (CO1,K2)
11. Explain in detail about copyright. (CO1,K2)
12. Describe the Digital Millennium Copyright Act. (CO1,K2)
13. Describe the principal categories of users of digital rights management systems. (CO1,K2)
14. Summarize the Law Enforcement of Cybercrimes with the vicious cycle of cybercrime. (CO1,K2)
15. Explain the role of Information theory in Cryptography. (CO1, K2)

GATE QUESTIONS

1. Which of the following is not a security service defined by the OSI Security Architecture?

a) Confidentiality

b) Authentication

c) Non-repudiation

d) Packet filtering

Answer: d) Packet filtering

Explanation:

The OSI defines services like confidentiality, authentication, integrity, non-repudiation, and access control. Packet filtering is a mechanism, not a service.

2. Which of the following attacks is classified as an active attack?

a) Eavesdropping

b) Traffic analysis

c) Masquerading

d) Passive sniffing

Answer: c) Masquerading

Explanation:

Active attacks modify data (e.g., masquerade, replay, DoS). Passive attacks (like eavesdropping) only observe.

3.In a monoalphabetic substitution, how many possible keys exist?

a) 2262^{26}226

b) 26!26!26!

c) 21282^{128}2128

d) 128!128!128!

Answer: b) 26!26!26!

Explanation:

Each letter maps to another → total permutations of 26 letters = 26!≈4×102626! \approx 4 \times 10^{26}26!≈4×1026

GATE QUESTIONS

4.A transposition cipher changes:

a) The identity of characters

b) The order of characters

c) The frequency of characters

d) Both b and c

Answer: b) The order of characters

Explanation:

Substitution changes identity, transposition changes position but leaves frequency unchanged.

5.Which of the following best describes steganography?

a) Encrypting data using AES

b) Hiding data within another medium

c) Masking IP addresses in a firewall

d) Obfuscating variable names in code

Answer: b) Hiding data within another medium Explanation:

Steganography hides the existence of a message, unlike cryptography which hides content.

6.According to Shannon's definition, a cryptosystem achieves perfect secrecy if:

a) Ciphertext can be decrypted by brute force

b) Probability distribution of plaintexts is changed

c) Ciphertext reveals no information about plaintext

d) Key is reused for multiple messages

Answer: c) Ciphertext reveals no information about plaintext

Explanation:

Perfect secrecy means $P(M|C)=P(M)P(M|C) = P(M)P(M|C)=P(M)$, i.e., knowing ciphertext doesn't change the probability of plaintext. Achieved only if:

- Key is truly random
- Key is as long as message
- Key used only once (one-time pad)

GATE QUESTIONS

7.Why do modern ciphers use product cryptosystems?

a) To increase brute-force resistance only

b) To combine strength of substitution and transposition

c) To simplify S-boxes

d) To prevent statistical attacks only

Answer: b) To combine strength of substitution and transposition

Explanation: Product ciphers use multiple transformations — substitution for confusion, transposition for diffusion (Shannon's principles). DES and AES use product structures.

8.Shannon’s entropy in cryptography measures:

a) Message size

b) Computational cost

c) Uncertainty or randomness in the source

d) Key length

Answer: c) Uncertainty or randomness in the source

Explanation: Entropy quantifies the unpredictability of information — a key metric for randomness and security.

9.In known-plaintext attack, the attacker has:

a) Only ciphertext

b) Access to ciphertext and corresponding plaintext

c) Choice of plaintexts

d) Only encrypted files and keys

Answer: b) Access to ciphertext and corresponding plaintext

Explanation:

This helps deduce the key or pattern in the encryption algorithm.

GATE QUESTIONS

10.Which of the following is a mechanism, not a service?

a) Authentication

b) Access control

c) Digital signature

d) Data confidentiality

Answer: c) Digital signature

Explanation:

Services = what is provided (e.g., confidentiality), mechanisms = how it's implemented (e.g., digital signature for non-repudiation).

11.Which of the following is not a component of the OSI Security Architecture?

A. Security Attacks

B. Security Mechanisms

C. Security Services

D. Security Protocols

Answer:

D. Security Protocols

12. In a Caesar cipher with a shift of 3, what is the ciphertext for the plaintext "HELLO"?

A. KHOOR

B. IFMMP

C. JGNNQ

D. EBIIL

Answer:

A. KHOOR

GATE QUESTIONS

13. Which of the following best describes steganography?

A. Encrypting data to prevent unauthorized access

B. Hiding data within other non-secret data

C. Using complex algorithms to scramble data

D. Compressing data to save storage space

Answer:

B. Hiding data within other non-secret data

14. In information theory, what does entropy measure?

A. The speed of data transmission

B. The average amount of information produced by a stochastic source of data

C. The redundancy in a data set

D. The error rate in data transmission

Answer:

B. The average amount of information produced by a stochastic source of data

15. What is the primary advantage of using a product cipher in cryptography?

A. It simplifies the encryption process

B. It combines multiple encryption methods to enhance security

C. It reduces the size of the ciphertext

D. It eliminates the need for key exchange

Answer:

B. It combines multiple encryption methods to enhance security

16. Which type of attack involves the attacker having access only to ciphertexts?

A. Known-plaintext attack

B. Chosen-plaintext attack

C. Ciphertext-only attack

D. Chosen-ciphertext attack

Answer:

C. Ciphertext-only attack

GATE QUESTIONS

17. Which of the following is not a component of the OSI Security Architecture?

A. Security Attacks

B. Security Mechanisms

C. Security Services

D. Security Protocols

Answer:

D. Security Protocols

18. Which of the following is an example of a passive security attack?

A. Denial-of-Service (DoS) attack

B. Man-in-the-Middle (MitM) attack

C. Traffic analysis

D. SQL injection

Answer:

C. Traffic analysis

19. Which security service ensures that the sender cannot deny having sent a message?

A. Confidentiality

B. Integrity

C. Authentication

D. Non-repudiation

Answer:

D. Non-repudiation

20. Which of the following is not considered a security mechanism in the OSI Security Architecture?

A. Encipherment

B. Digital signatures

C. Access control

D. Data compression

Answer:

D. Data compression

GATE QUESTIONS

17. Which of the following is not a component of the OSI Security Architecture?

A. Security Attacks

B. Security Mechanisms

C. Security Services

D. Security Protocols

Answer:

D. Security Protocols

18. Which of the following is an example of a passive security attack?

A. Denial-of-Service (DoS) attack

B. Man-in-the-Middle (MitM) attack

C. Traffic analysis

D. SQL injection

Answer:

C. Traffic analysis

19. Which security service ensures that the sender cannot deny having sent a message?

A. Confidentiality

B. Integrity

C. Authentication

D. Non-repudiation

Answer:

D. Non-repudiation

20. Which of the following is not considered a security mechanism in the OSI Security Architecture?

A. Encipherment

B. Digital signatures

C. Access control

D. Data compression

Answer:

D. Data compression

GATE QUESTIONS

1.Assume an attacker has intercepted a ciphertext encrypted with a simple substitution cipher. The attacker also knows part of the corresponding plaintext.
Describe a step-by-step approach the attacker might use to perform a known-plaintext attack and deduce the substitution key. How would the attack change if the cipher were polyalphabetic?

2. A cryptographer designs a product cipher by first applying a substitution cipher and then a transposition cipher. Explain how this design improves the cipher's resistance to cryptanalysis. What would happen if the order were reversed?

3.Prove that the one-time pad provides perfect secrecy using Shannon's definition of information-theoretic security. Assume uniformly distributed keys and messages.

4. Compare the strength and weaknesses of monoalphabetic and polyalphabetic substitution ciphers from the perspective of frequency analysis and key space size. Why is the Vigenère cipher historically considered more secure than Caesar cipher?

5.Given a ciphertext encrypted using a transposition cipher:
Ciphertext: WECRLTEERDSOEEFEAOCAIVDEN
The key used was of length 5. Recover the plaintext, showing the steps of decryption.

6. You are given the ciphertext ZEBRAS encrypted using a Playfair cipher. Assume that the keyword is MONARCHY and construct the key matrix. Decrypt the ciphertext completely, showing intermediate steps.

7. You are given a scenario where secret data is embedded in the least significant bits (LSBs) of an image file. Explain how an attacker could statistically detect this using chi-square analysis. How would you design a more resilient steganographic method to evade such analysis?

GATE QUESTIONS

8. Explain how confusion and diffusion principles are implemented in a product cipher like Feistel structure. If a 3-round Feistel network uses weak round functions (like XOR with a fixed value), explain how it might be vulnerable to differential cryptanalysis.

9.Consider a network with multiple layers of security implemented using the OSI model. Describe the security mechanisms at the network layer and transport layer that can protect against various attacks (e.g., man-in-the-middle, session hijacking, IP spoofing). How do these mechanisms interact with the security services provided at the application and data link layers?

10. You are tasked with securing a system that transmits sensitive information over an insecure network. Describe how active attacks like denial-of-service (DoS), man-in-the-middle, and replay attacks can be mitigated using proper security mechanisms. For each attack, discuss the most appropriate countermeasures (e.g., cryptographic protocols, network monitoring).

Supportive online Certification courses

NPTEL

- Cryptography and Network Security
- Introduction to Cryptology
- Foundations of Cryptography
- Computational number theory and cryptography

COURSERA

- Cryptography
- Applied Cryptography
- Number theory and cryptography
- Cryptography anf Information theory
- Asymmetric cryptography and key management
- Symmetric Cryptography

UDEMY

- Introduction to Cryptography
- Cryptography with python
- Complete Cryptography master class

Real time Applications in day to day life and to Industry

- Authentication/Digital Signatures
- Time Stamping
- Electronic Money
- Secure Network Communications
- Disk Encryption
- Encryption/Decryption in email:
- Encryption in WhatsApp, Instagram
- Sim card Authentication:
- Secrecy in
- transmission Secrecy
- in storage
- Integrity in transmission

Authentication of identity

MINI PROJECT SUGGESTIONS

Set 1

1. Create a Banking software to provide the basic services to manage bank accounts at a bank. Ensure to provide security in the transaction. Apply cryptographic algorithms for safe online transaction for the bank customers.
2. Create software that can encrypt and decrypt using a 2 * 2 Hill cipher.
3. Design a peer-to-peer chat application that uses symmetric or asymmetric encryption (e.g., AES or RSA) to secure messages during transmission.

Set 2

1. Create a cross platform Secret sharing Tool that can be used as offline Password Backup System.
2. Create software that can perform a fast known plaintext attack on a Hill cipher, given the dimension m. How fast are your algorithms, as a function of m?
3. Develop a tool that evaluates the strength of user-entered passwords based on criteria like length, complexity, and resistance to dictionary attacks.

Set 3

1. Build an Image Steganography software.
2. Develop a command-line or GUI-based application that implements classical encryption techniques such as Caesar, Playfair, Hill, and Vigenère ciphers. Include features for encryption, decryption, and frequency analysis.
3. Create a simulator that allows users to define firewall rules and test how different traffic types are handled, enhancing understanding of access control mechanisms.

MINI PROJECT SUGGESTIONS

Set 4

1. Develop an application for a brute force based Cipher-Dicipher with UI/UX.
2. Create a tool that hides messages within images or audio files using Least Significant Bit (LSB) techniques. Implement both embedding and extraction functionalities.

Set 5

1. Develop a hybrid cryptography system based on Vignere cipher
2. Build a simulator that demonstrates basic cryptanalysis methods, such as brute-force attacks on Caesar cipher or frequency analysis on monoalphabetic ciphers.

ASSESSMENT SCHEDULE

Assessment	Proposed Date	Actual Date
IAT I		
IAT II		
MODEL		

Thank you

Disclaimer:

R.M.K GROUP OF INSTITUTIONS