As per the New Syllabus of Gujarat Technological University (GTU)

This book is specially written for students of

Diploma Information Technology

Semester-6

Subject Code : 4361601

CYBER SECURITY AND DIGITAL FORENSICS

Authors

J. B. Patel
M.E., C.E.
Lecturer, Government Polytechnic, **Dahod.**

H. K. Patel
B.E., I.T.
Sr. Lecturer, SAL Institute of Diploma Studies
Ahmedabad.

D. K. Thakar
B.E., C.E.
Lecturer, SAL Institute of Diploma Studies
Ahmedabad.

First Edition : 2024 - 2025

Price : ₹ 150-00

ATUL PRAKASHAN
GANDHI ROAD, AHMEDABAD.

Publishers :

ATUL PRAKASHAN

Under Farnandis Bridge,

Gandhi Road, Ahmedabad-1.

Phone : (079) 26426677, 22160475

First Edition : 2024 - 2025

Price : ₹ 150-00

Cyber Security and Digital Forensics, Edition First

Type-Setting :

Imkha Graphics

Kalupur, Ahmedabad.

PREFACE

In the dynamic landscape of Information Technology, the need for robust cybersecurity skills has never been more crucial. This book, tailored for 6th-semester Diploma IT students, is a guiding beacon into the multifaceted domain of Information Security.

The journey begins with a foundational exploration of information security, laying the groundwork for understanding cryptographic principles and advanced hashing techniques. As readers progress, they will unravel the diverse landscape of network and system security, gaining insights into the techniques employed to safeguard digital assets and the threats that loom in the digital shadows.

Cybercrimes have become an unfortunate reality, and this book addresses this challenge head-on. Readers will not only understand the various types of cybercrimes but will also delve into the analysis of cybercriminal activities, providing a deeper comprehension of the adversary's mindset.

Practical application is a core focus of this resource, guiding students through the implementation of ethical hacking methodologies using Kali Linux. The hands-on experience in vulnerability analysis prepares students to proactively identify and address security weaknesses in digital systems.

The journey concludes with an exploration of digital forensics methodologies, shedding light on how these techniques are employed to investigate and analyze cybercrimes. By combining theoretical knowledge with practical skills, this book aims to mold students into adept cybersecurity professionals, ready to face the challenges of securing the digital landscape.

As you embark on this educational odyssey, envision not just learning but mastery. Information Security is not merely a subject; it is a skill set, and by the end of this journey, you will be equipped to navigate the complexities of the digital frontier with confidence and expertise. Welcome to the future of cybersecurity.

source4jitendra@gmail.com,
hptechpln@gmail.com,
thakardevans@gmail.com

GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)

Diploma for Information Technology

Subject Code : 4361601

Semester-6

Subject Name : Cyber Security and Digital Forensics

Teaching and Examination Scheme :

Teaching Scheme (In hours)			Total Credits (L+T/2+P/2)	Examination Scheme				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	CA*	ESE	CA	ESE	
4	--	4	6	30	70	25	25	150

(*) : Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

Legends : L – Lecture; T – Tutorial/Teacher Guided Theory Practice; P – Practical; C – Credit, CA – Continuous Assessment, ESE – End Semester Examination.

Underpinning Theory

Unit	Unit Outcomes (UOs)	Topics and Sub-topics
Unit – I Introduction of Information Security and Cryptography	1a. Learn about how to maintain the Confidentiality, Integrity and Availability of a data. 1b. Analyze and design hash and MD5 algorithms.	1.1. Basic Concept of Information Security 1.2. CIA Triad 1.3. OSI Security Architecture (Security Servic Mechanisms and Attacks) 1.4. Private & Public Key Cryptography 1.5. Message Digest 5 Hashing & SHA
Unit– II Network and System security	2a. To understand various protocols for network security to protect against the threats in the networks. 2b. Understand the threats and risks to modern data and information systems. 2c. Understand the working and configuration of firewall.	2.1. Types of attacks 2.2. Digital signatures : Definition and Properties 2.3. Pretty Good Privacy (PGP)(brief) 2.4. Secure Socket Layer and Transport Layer Security 2.5. IPsec 2.6. HTTPS (Connection initiation & Connection closure) 2.7. Malicious software: Virus and Related Threats (Trojans, Rootkit, Backdoors, keylogger) 2.8. Firewall : Need and Types 2.9. Proxy Server : Need and Types
Unit – III Cyber Crime	3a. Understand the cybercrimes from the nature of the crime. 3b. Analyze various aspects of Cyber-crimes. 3c. Understand the security and privacy methods in development of modern applications and in organizations to protect people and to prevent cyber-crimes.	3.1 Overview of Cybercrime • Definition • Cybercriminals • Cybercrime 3.2 Classification of cyber-crimes 3.2.1. Organization a. Email Bombing b. Salami Attack c. Logic Bomb d. Trojan Horse e. Web Jacking f. Data diddling

Unit	Unit Outcomes (UOs)	Topics and Sub-topics
	3d. Analyze how particular social engineering attacks are important consideration for cyber security 3e. Understand the Objectives and features of IT ACT, 2008.	g. Denial of Service/Distributed h. Ransomware 3.2.2. Individual a. Cyber bullying b. Cyber stalking c. Cyber defamation d. Phishing e. Cyber fraud and Cyber theft f. Spyware g. Email spoofing h. Man in the middle attack 3.2.3. Society a. Cyber pornography b. Cyber terrorism c. cyber spying d. Social Engineering Attack e. Online gambling 3.2.4. Property a. Credit Card Fraud b. Software Piracy c. Copyright infringement d. Trademarks violations 3.3 Challenges & Prevention of Cyber Crime 3.4 Cyber Law The Information Technology ACT, 2008 OFFENCES • Section 65 • Section 66 • Section 67
Unit– IV Ethical Hacking	4a. Understand the ethical behaviour with unethical behaviour. 4b. Understand basic terminologyas it relates to the Kali Linux distri-bution. 4c. To learn about various types of attacks, attackers and security threats and vulnerabilities. 4d. To learn about scanning of systems/applications and System Protection.	4.1. Concept of Hacking Types of Hackers 4.2. Basics of Ethical Hacking 4.3. The terminology of Hacking (Vulnerability, Exploit, 0-Day) 4.4. Five Steps of Hacking (Information Gathering, Scanning, Gaining Access, Maintaining Access, Covering Tracks) 4.5. Information Gathering (Active, Passive) 4.6. Introduction to Kali Linux OS • Configuration of Kali Linux • Basic Commands Kali Linux • Vulnerability Scanning/ Vulnerability Based Hacking a. Foot printing b. Scanning c. Password Cracking d. Brute Force Attacks e. Injection Attacks f. Phishing Attacks g. Block chain Attacks 4.7. Port Scanning 4.8. Remote Administration Tool (RAT) 4.9. Protect System from RAT 4.10. What is Sniffing and Mechanism of Sniffing Session Hijacking

Unit	Unit Outcomes (UOs)	Topics and Sub-topics
Unit– V DIGITAL FORENSICS	5a. Describe the basic concepts of Forensic and Branches of Digital Forensic. 5b. Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective. 5c. To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices. 5d. To understand how to examine digital evidences such as the data acquisition, identification analysis.	5.1. Introduction to Digital Forensics 5.2. Locard's Principle of Exchange in Digital Forensics 5.3. Branches of Digital Forensics • Disk / Memory Forensics • Database Forensics • Email Forensics • Mobile Forensics • Network Forensics • Software Forensics • Malware Forensics 5.4. Phases of digital/computer forensics investigation • Identification • Preservation • Analysis • Documentation • Presentation 5.5. Methods to Preserve a Digital Evidence • Drive Imaging • Hash Values • Chain of Custody 5.6. Critical Steps in Preserving Digital Evidence 5.7. Evidence Role of devices as in Digital Forensics investigations • Computing Devices • Network Devices and Servers • CCTV • Vehicles

SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
1	Overview of Information Security and Cryptography	08	4	4	4	12
2	Network and System Security	10	2	4	6	12
3	Cyber Crime	12	2	6	6	14
4	Ethical Hacking	14	4	6	6	16
5	Digital Forensics	12	2	8	6	16
	Total	**56**	**12**	**30**	**28**	**70**

Legends : R = Remember, U = Understand, A = Apply and above (Revised Bloom's taxonomy)

***Note** : This specification table provides general guidelines to assist students for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary slightly from the above table.*

Contents

TO THE READER

Authors and publisher would welcome suggestions towards future edition of this book or the pointing out of any misprint or obscurity. Please write to The Technical Editor, ATUL PRAKASHAN, Under Farnandis Bridge, Gandhi Road, Ahmedabad-1.

Chapter 1

INTRODUCTION OF INFORMATION SECURITY AND CRYPTOGRAPHY

1.1 INTRODUCTION : BASIC CONCEPTS OF INFORMATION SECURITY

- WHY INFORMATION SECURITY ?
- WHAT IS INFORMATION SECURITY

1.2 CIA TRIAD : FUNDAMENTAL GOALS OF INFORMATION SECURITY

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY
- NON-REPUDIATION, AUTHENTICATION AND ACCOUNTABILITY

1.3 OSI SECURITY ARCHITECTURE

- SECURITY ATTACKS
- SECURITY MECHANISM
- SECURITY SERVICES

1.4 PRIVATE AND PUBLIC KEY CRYPTOGRAPHY

- BASIC CRYPTOGRAPHIC TERMS
- CRYPTOGRAPHIC TECHNIQUES
  - SUBSTITUTION TECHNIQUE
  - TRANSPOSITION TECHNIQUE
- PRIVATE AND PUBLIC KEY CRYPTOGRAPHY

1.5 MESSAGE DIGESTING, 5 HASHING AND SHA

- HASHING
- MESSAGE DIGEST 5 (MD 5)
- SECURE HASHING ALGORITHM(SHA)
- RSA ALGORITHM

Self - Assessment

1.1 INTRODUCTION : BASIC CONCEPTS OF INFORMATION SECURITY

As we know, due to increase in hardware technology speed and internet speed, it became growing very rapidly in different domains like Autonomous Systems, E-commerce, Gaming, Natural Resource Management, Education, Space Exploration, Agriculture, Energy Management, Healthcare, Finance, Retail, Manufacturing, Automotive, Entertainment and Media, Government and Defence, Environmental Conservation, Human Resources, Hospitality and Tourism etc.

In the increasingly globalized digital economy, information assets are critical to the existence of some organizations as well as to any business. It is unacceptable for information to leak. Confidential information about a company's customers, their personal information, finances, or new product line that is obtained by a rival may result in lost revenue, legal action, or even the company's demise.

1.1.1 Why information security ?

Let us understand why information security is important for organisation as well as individuals with some real examples.

- **Protection of Sensitive Personal Information :**

  Online Banking Information security ensures that personal financial data, such as account numbers and passwords, etc are protected from hackers. In the absence of strong security protocols, internet banking systems may be breached, resulting in unapproved access to bank accounts and possible monetary losses for users.

- **Business Confidentiality :**

  Theft of Intellectual Property- Businesses greatly rely on information security to protect their product designs, trade secrets, and intellectual algorithms. If this data is not protected, rivals may obtain sensitive information and suffer large financial losses as well as a loss of competitive advantage.

- **Prevention of Data Breaches :**

  Credit card details are stored in a retail company's customer database. A cyberattack could cause a data breach if this data is improperly safeguarded, exposing the private financial information of thousands of consumers. The company's reputation suffers, regulatory fines are imposed, and the impacted customers suffer losses as well.

- **Maintaining Operational Continuity :**

  Information security guards against ransomware attacks, which have the ability to encrypt important company data and make it unreadable. In the absence of sufficient security measures, a ransomware attack has the potential to cause financial losses and service disruptions by impeding operations until a ransom is paid.

- **Compliance with Regulations :**

  General Data Protection Regulation, or GDPR, for data protection rules to be followed, information security is essential. Organizations managing personal data may face severe fines and legal repercussions if they fail to secure the data in compliance with laws like the GDPR.

- **Protection Against Cyber Threats :**

  Firewalls and antivirus software are examples of information security techniques that guard against malware infections. Without these defences, systems may be susceptible to trojans, worms, or viruses that tamper with data integrity and interfere with regular operations.

In essence, information security is crucial across various domains, including personal privacy, business operations, regulatory compliance, and safeguarding against cyber threats. It's essential to implement robust security measures to mitigate risks.

1.1.2 What is Information Security ?

Information security encompasses more than just protecting data from unwanted access. Preventing unauthorized access, use, disclosure, interruption, alteration, inspection, recording, or destruction of information is the essence of information security. Either physical or electronic information is possible. Information can refer to anything, such as your biometrics, phone number, social network profile, or other details. Therefore, a wide range of academic fields are covered by information security, including cryptography, mobile computing, cyber forensics, online social media, etc.

Effective information security requires a comprehensive approach that considers all aspects of the information environment, including technology, policies and procedures, and people.

Thus, Information security can be defined as

"The practice of protecting sensitive data, systems, networks, and information assets from unauthorized access, disclosure, alteration, destruction, or any form of cyber threat."

It encompasses a set of strategies, technologies, policies, and practices designed to ensure the confidentiality, integrity, and availability of information.

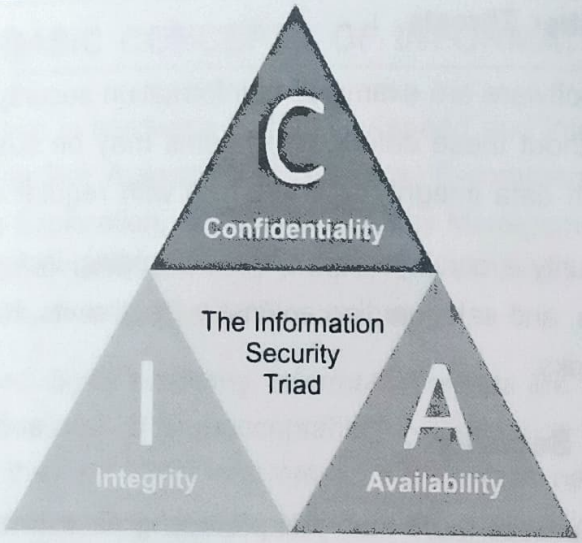
1.2 CIA TRIAD : FUNDAMENTAL OBJECTIVES

When talking about Information Security, the three fundamental objectives are Confidentiality, Integrity and Availability, commonly known as **CIA** triad which is one of the most important models designed to guide policies for information security.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability

These three CIA triad concepts are considered as fundamental objectives for achieving information security. In the below discussion we will try to understand how these three concepts are important for information security.



[Fig. 1.1 : CIA Triad-Fundamental Objectives]

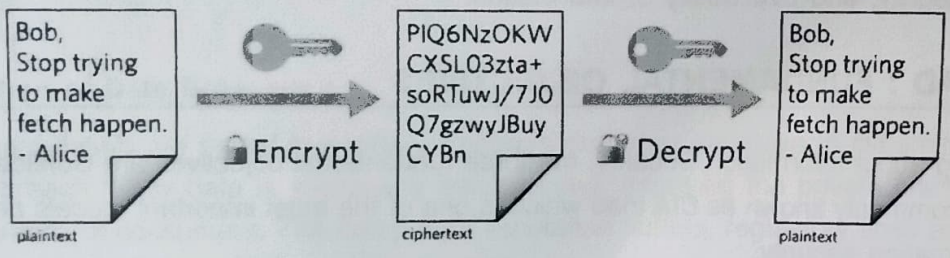
Confidentiality

"Confidentiality refers to that the information is not disclosed or revealed to unauthorised party, except the parties involved in communication."

As an illustration, let's imagine I had a password for my Gmail account, someone saw while I was doing a login into Gmail account. In that instance, confidentiality has been violated and my password has been compromised.

Unauthorized users shouldn't be able to access your personal information. The attacker might attempt to obtain your information by capturing the data with various online tools.

The use of different encryption techniques to protect our data is one of the main ways to prevent confidentiality, Because Encryption techniques prevent the attacker from being able to decrypt it, even if they manage to obtain access to it.



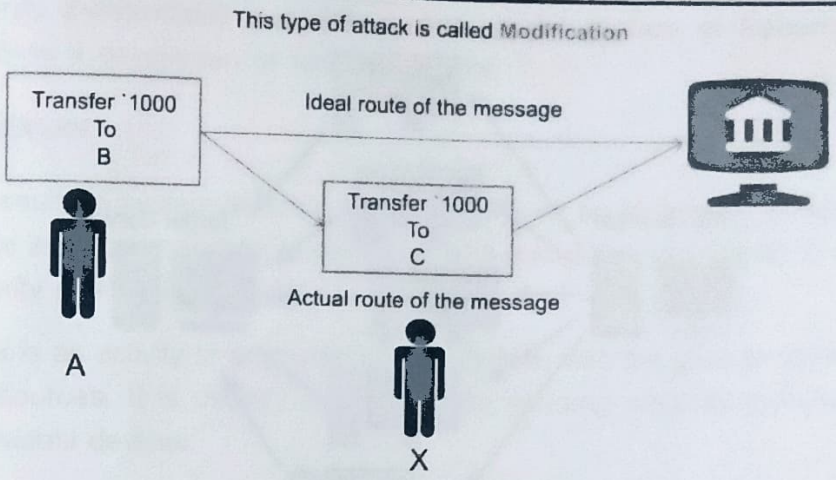
[Fig. 1.2 : Confidentiality using Encryption]

AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two examples of encryption standards.

Integrity

The next CIA component for discussion is integrity. *The **Integrity** refers to make sure that data has not been modified by unauthorised party.*

To check whether our data has been modified or not, we can use hash functions. Two common types of hash functions are : SHA (Secure Hash Algorithm) and MD5 (Message Direct 5).

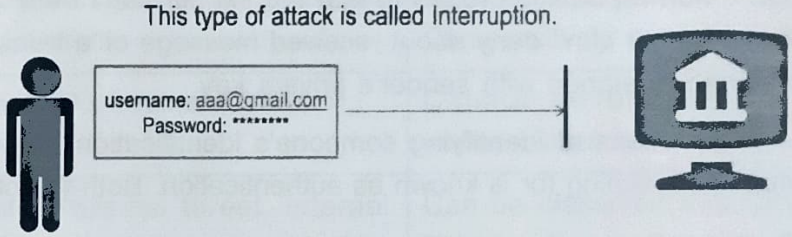


[Fig. 1.3 : Integrity : Types of Modification Attack]

Let's assume Sender 'A' wants to send data to Receiver 'B' with maintaining data integrity. A hash function will run over the data and produce an arbitrary hash value which is then attached to the data. When receiver 'B' receives the packet, it runs the same hash function over the data which gives a hash value. Now, if sender hash value = Receiver hash value, then it means that the data's integrity has been maintained and the contents were not modified.

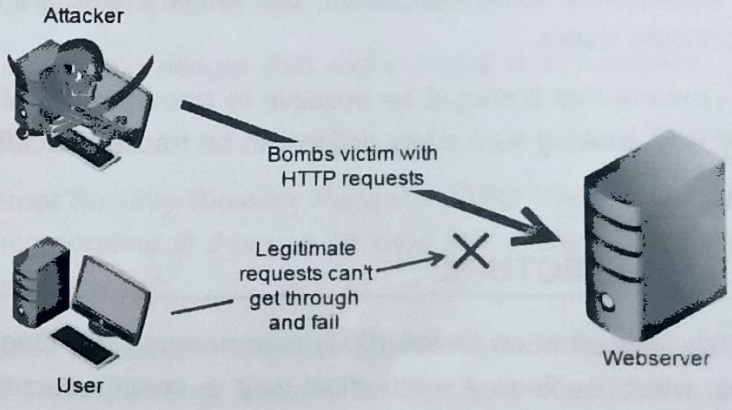
Availability

Availability *refers to ensure that, the system or network is timely and reliably available to its authorised users*. This applies to systems as well as data. Attacks such as DoS (Denial of Services or DDoS(Distributed Denial of Services) may render a network unavailable as the resources of the network get exhausted.

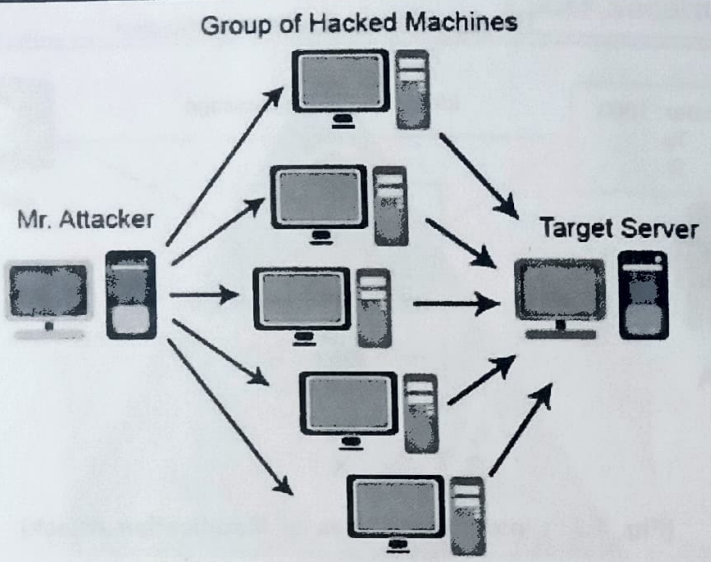


[Fig. 1.4 : Availability : Type of Interruption Attack]

To make the resources like systems, networks, or web servers unavailable to its legitimate users, attackers apply attacks like Denial of Services (DOS) and Distributed Denial of Services (DDOS).



[Fig. 1.5 : DOS Attack to Make Resource Unavailable]



[Fig. 1.6 : DDOS Attack to Make Resource Unavailable]

To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.

Apart from these three TRIAD objectives, there are some other principles which governs information security.

These principles are as under :

- **Non repudiation** – non repudiation refers to that the sender can't deny about sent message or a transaction and receiver can't deny about received message or a transaction.This is achieved through digital signature signed with sender's private key
- **Authenticity** – The process of identifying someone's identification by confirming that they are similar to as what it is claiming for is known as authentication. Both the client and the server can use it.

  When someone needs to access the data, the server utilizes authentication since it needs to know who is gaining access. When the client needs to verify that the server is who it says it is, it uses it. The username and password are usually used by the server to complete the authentication process. Cards, fingerprints, voice recognition, and retinal scans are some more ways that the server can authenticate users.
- **Accountability** – means that it should be possible to trace actions of an entity uniquely to that entity. By another way, making sure every action can be tracked back to a single person, not just a group.

1.3 OSI SECURITY ARCHITECTURE

The International Telecommunication Union (ITU) recommends the Open System Interconnection (OSI) security architecture, which outlines a methodical way to specify security needs and methods to satisfy those criteria.

The OSI security architecture provides a general description of Security Services, Security mechanisms, as well as a description of security attacks.

1.3.1 Security Attacks :

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.

A security attack is an activity or act made upon a system with the goal to obtain unauthorized access to information or resources. It is usually carried out by evading security policies that are in place in organizations or individual devices.

Thus, any action that compromises the security of information owned by an organization.

Security attacks can be classified in two types : Active attack and Passive attack.

Difference between threats and attacks :

THREAT	ATTACK
Threat can be intentional or unintentional	Attack is intentional
May or may not be malicious	Attack is malicious
Circumstance that has the ability to cause damage	Objective is to cause damage
Information may or may not be altered or damaged	Chance for information alteration and damage is very high
Comparatively hard to detect	Comparatively easy to detect
Can be blocked by control of vulnerabilities	Cannot be blocked by just controlling the vulnerabilities
Can be classified into Physical threat, internal threat, external threat, human threat, and non-physical threat.	Can be classified into Virus, Spyware, Phishing, Worms, Spam, Botnets, DoS attacks, Ransom-ware, Breaches.

Threats : 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 a vulnerability.

1.3.2 Security Mechanism :

According to the Internet Security Glossary Version 2 (RFC 4949), a security mechanism is *"A method or process (or a device incorporating it) that can be used in a system to implement a security service that is provided by or within the system".*

Some of the examples of security mechanism are authentication exchange, checksum, digital signature, encryption, and traffic padding. Security mechanisms described in the OSI security architecture are as under :

- Specific Security Mechanisms
  - Encipherment
  - Digital Signature mechanisms
  - Access Control
  - Data Integrity
  - Authentication Exchange
  - Traffic Padding
  - Routing Control
  - Notarization
- Pervasive Security Mechanisms
  - Trusted Functionality
  - Security Label
  - Event Detection
  - Security Audit Trail
  - Security Recovery

1.3.3 Security Services :

According to the Internet Security Glossary Version 2 (RFC 4949), a security service is

"A processing or communication service that is provided by a system to give a specific kind of protection to system resources".

The OSI security architecture classifies security services as follows:

- Authentication
- Access Control Service
- Data Confidentiality
- Data integrity
- Non-repudiation

1.4 CRYPTOGRAPHY AND CRYPTOGRAPHIC TECHNIQUES

1.4.1 Basic Cryptographic Terms :

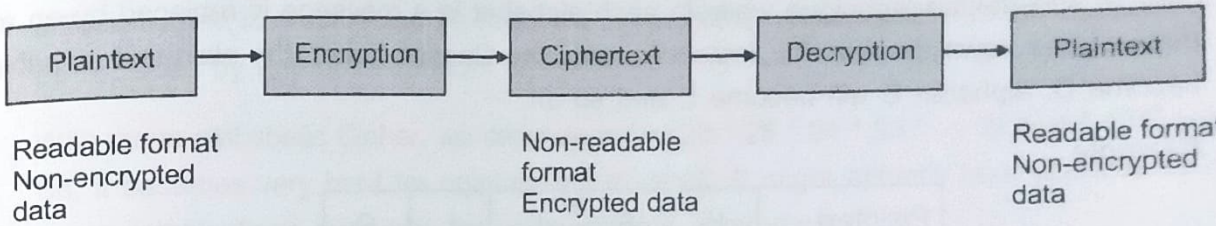
Cryptography - *"Cryptography is the art of achieving security by encoding messages to make them non-readable."*

Cryptanalysis - *"Cryptanalysis is the technique of decoding messages from a non-readable format back to a readable format without knowing how they were initially converted from readable format to nonreadable format."*

In other words, it is like breaking a code. These concepts are shown in Fig. 1.7.

Cryptology - *"Cryptology is a combination of cryptography and cryptanalysis."*

Cryptography + Cryptanalysis = Cryptology



[Fig. 1.7 : Elements of Cryptography Process]

Plaintext or Clear text - "Any original message that can be readable and understandable by the sender, the recipient, and also by anyone else who gets access to that message."

Cipher text - When any original plain-text message is codified using any suitable scheme into the form which is not understandable by other than the sender and the recipient, then such resulting message is called cipher text.

Encryption - The process of encoding plaintext messages into cipher text messages is called encryption.

Decryption -The reverse process of transforming cipher-text messages back to plain text messages is called decryption.

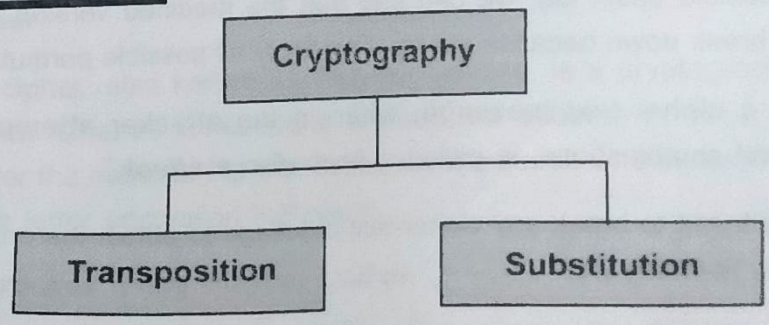
Every encryption and decryption process has two aspects : the algorithm and the key used for encryption and decryption.

1.4.2 Cryptographic techniques :

As shown in Fig. 1.8, there are two primary ways in which a plain-text message can be codified to obtain the corresponding cipher text :

A. Substitution Techniques

B. Transposition Techniques



[Fig. 1.8 : Types of Classical Cryptographic Techniques]

[A] Substitution techniques :

In the substitution-cipher technique, the characters of a plain-text message are replaced(substituted) by other characters, numbers or symbols. Some of the substitution techniques are discussed below.

- **Caesar Cipher**

Caesar cipher was the first and simplest example of substitution cipher technique. It was first proposed by Julius Caesar, and so is termed as Caesar cipher. The Caesar cipher is a special case of substitution technique wherein each alphabet in a message is replaced by an alphabet three places down the line. For instance, using the Caesar cipher, the plain-text alphabet A will become D, alphabet B will become E and so on.

Example :

Plaintext	H	E	L	L	O
Ciphertext	K	H	O	O	R

[Converting plain text into ciphertext]

The Caesar cipher is considered as a very weak scheme of cryptography. To get the original plain text message, we required to just reverse of the Caesar cipher process - i.e. replace each alphabet in a cipher-text message produced by Caesar cipher with the alphabet that is three places up the line.

Ciphertext	K	H	O	O	R
Plaintext	H	E	L	L	O

[Converting Cipher text into Plain text]

- **Modified Version of Caesar Cipher**

As we discussed, the Caesar cipher is very simple to implement but it is the weakest technique to break down. How can we complicate a Caesar cipher a bit more? Now instead of replacing each character of plaintext message by an alphabet three places down the line, we replace it with any of the remaining 25 alphabets. Once the replacement technique has been determined then it will be applied to all other alphabets in that message.

We can see that to convert the cipher text into plaintext we need to apply 25 different attempts in the worst possible case. So, we can say that the modified version of Caesar cipher more complicated to break down because we have to apply all possible permutation and combinations.

"An attack on a cipher-text message, wherein the attacker attempts to use all possible permutations and combinations, is called a ***brute-force attack.***"

"The process of trying to break any cipher-text message to obtain the original plain-text message itself is called ***cryptanalysis.***"

"The person attempting a cryptanalysis is called a ***cryptanalyst.***"

- **Mono-alphabetic Cipher**

The primary limitation of the Caesar cipher is its predictability. Once we determined to replace an alphabet in the original plain text with an alphabet which is k positions up or down order, we use the same scheme (same k position) for all the alphabets. Due to this cryptanalyst has to try only 25 possibilities to crack the ciphertext.

In mono alphabetic cipher instead of using uniform pattern, we replace alphabet each time differently that is each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any other random alphabet (A or C through Z), and so on.

With mono alphabetic Cipher, we can now have (26 * 25 * 24 * 23 * ... 2) or $4 * 10^{26}$ possibilities! So, it becomes very hard for cryptanalyst to crack. It might actually take years to try out these many combinations even with the most modern computers.

- **Homophonic Substitution Cipher**

This technique is very similar to mono-alphabetic cipher. But, the difference between the two techniques is that replacement alphabet set in case of the simple substitution techniques is fixed (e.g. replace A with D, B with E, etc.), in the case of homophonic substitution cipher, one plain-text alphabet can be replaced with alphabet from chosen set. For example, A can be replaced by E, G, I, K; B can be replaced by F, H, J, L, etc.

- **Polygram Substitution Cipher**

In the PolyGram substitution cipher technique, instead of replacing alphabets one by one at a time, a block of alphabets is replaced with another block. For example, HELLO could be replaced by DKNNW, but HELL could be replaced by a totally different cipher text block TLEF.

HELLO ----------> DKNNW

HELL ----------> TLEF

(Plaintext) (ciphertext)

This shows that in the Polygram substitution cipher, the replacement of plain text happens block by block, rather than character by character.

- **Playfair Cipher**

The Playfair cipher, also known as **Playfair square**, is a cryptographic method for manually encrypting data. Charles Wheatstone created this scheme in 1854, but it eventually gained popularity under the name of Playfair, Wheatstone's friend, who became the scheme's public face. It is a multiple letter encryption technique.

Encryption process using Playfair Cipher

1. Construct 5 * 5 matrix and fill it up with characters without repeating from the given keyword.

Example :

Keyword : MONARCHY

M	O	N	A	R
C	H	Y		

2. Fill all remaining places in the Playfair square using letters from alphabet without repeating.

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

Note : In English alphabets there are 26 letters, but we have only 5 * 5 (Total 25) places. So, I and J are placed in the same box.

3. Create Digrams by combining two-two alphabets from the given plain text message.

Example :

Plaintext : ATTACK

Diagram : AT TA CK

(A) If there is a singlecharacter in the last Diagram, then use filler character X.

Example :

Plaintext : NESO ACADEMY

Diagram : NE SO AC AD EM Y

New Diagram : NE SO AC AD EM YX

(B) If there is repeating character in the Diagram, use filler character as under.

Example :

Plaintext : BALLOON

Diagram : BA LL OO N

New Diagram : BA LX LO ON

4. Check each character of the Diagram in the matrix, and replace as per below rules.

(A) if both characters are in the same column, replace them with one downward character.

(B) if both characters are in the same row, replace them with one right side character.

(C) if characters are in different row and different column, replace with last character in the same row.

Example - 1

Plaintext	ATTACK		
Diagram	AT	TA	CK
Ciphertext	RS	SR	DE
Process step	4C	4C	4C

Example – 2

Plaintext	MOSQUE		
Diagram	MO	SQ	UE
Ciphertext	ON	TS	ML
Process step	4B	4B	4A

[B] Transposition techniques :

In contrast to the substitution techniques, Transposition techniques perform some permutation over the plain text, instead of replacing one alphabet with another alphabet. For example, if given plaintext is HELLO, then Ciphertext may be LHELO. Here we can observe that In ciphertext, letters are same as plain text but placed at different position.

Some of the common transposition techniques are discussed as under.

- **Rail-Fence Technique**

  Rail-fence technique is the simplest transposition technique which work with algorithm as written below.

  Step 1. Write alternate letters of the given plaintext into first line.

  Step 2. Write remaining letters of the given plaintext into second line.

  Step3. Read the first line and then read the second line. Output of the step 3 is Ciphertext of the given plaintext.

Example

Plaintext : YOU ARE BEST FRIEND

Plaintext	YOU ARE BEST FRIEND
Step 1	YURBSFIN
Step 2	OAEETRED
Step 3	YURBSFINOAEETRED

Plaintext : YOU ARE BEST FRIEND

Ciphertext : YURBSFINOAEETRED

- **Simple Columnar Transposition Technique**

Columnar transposition technique is similar like simple rail fence technique with minor change in processing method. There are two types of columnar transposition techniques.

(1) Basic Simple Columnar Transposition Technique

Basic Simple Columnar Transposition Technique works with algorithm as written below.

Step 1. Write the letters of given plain text row by row into table with predefined size.

Step2. Read the letter from the table column wise. No need to read columns in sequence. (columns 1, 2, 3...). You are allowed to read columns randomly like column 3, 1, 2 etc...

Step 3. The output of the step 2 is Ciphertext.

Example

Plaintext : YOU ARE MY BEST FRIEND

Step 1. Consider table of five columns and write letters of plaintext row wise as below.

Column 1	Column 2	Column 3	Column 4	Column 5
Y	O	U	A	R
E	M	Y	B	E
S	T	F	R	I
E	N	D		

Step 2. Now decide the sequence of column as column 2, 4, 1, 3, 5. Read the letters from the table as the sequence decided.

Step 3. The output ciphertext would be : OMTNABRYESEUYFDREI

(2) Transposition Technique with Multiple round

To increase the complexity, the Basic Columnar Transposition Technique is carried out with multiple rounds. The basic process is as the case of Basic Columnar Transposition technique.

The basic algorithm for transposition technique with multiple rounds is as under.

Step 1. Write the letters of given plain text row by row into table with predefined size.

Step 2. Read the letter from the table column wise. No need to read columns in sequence. (columns 1, 2, 3...). You are allowed to read columns randomly like column 3, 1, 2 etc...

Step 3. The output of the step 3 is Ciphertext with round 1.

Step 4. Repeat steps 1 to 3 as many times as you decided.

Example

Plaintext : YOU ARE MY BEST FRIEND

Step 1. Consider table of five columns and write letters of plaintext row wise as below.

Column 1	Column 2	Column 3	Column 4	Column 5
Y	O	U	A	R
E	M	Y	B	E
S	T	F	R	I
E	N	D		

Step 2. Now decide the sequence of column as column 2, 4, 1, 3, 5. Read the letters from the table as the sequence decided.

Step 3. The output ciphertext would be : OMTNABRYESEUYFDREI

Step 4. Repeat step 1 to 3 for the ciphertext : OMTNABRYESEUYFDREI so the new table representation will be as below.

Column 1	Column 2	Column 3	Column 4	Column 5
O	M	T	N	A
B	R	Y	E	S
E	U	Y	F	D
R	E	I		

Step 5. Now decide the sequence of column as column 2, 4, 1, 3, 5. Read the letters from the table as the sequence decided.

Step 6. The output ciphertext would be : MRUENEFOBERTYYIASD

- **Vernam Cipher (One-Time Pad)**

The Vernam cipher, uses a random set of non-repeating characters as the input cipher text. This technique uses such input ciphertext to convert plain text into ciphertext. Here it is never repeated so-called one-time pad. The length of the input cipher text is equal to the length of the original plain text. The algorithm used in the Vernam cipher is as under.

Step 1. Assign each letter in the plaintext with number i.e. A = 0, B = 2, ... Z = 25.

Step 2. Assign each letter in the input ciphertext with the number same as step 1.

Step 3. Add corresponding plaintext alphabet number with the input ciphertext number.

Step 4. If the sum is greater than 25, subtract 26 from the sum.

Step 5. Translate each number of sums back to the corresponding letter.

Example

Plaintext : HOW ARE YOU

Plaintext	H	O	W	A	R	E	Y	O	U
Corresponding Number	7	14	22	0	17	4	24	14	20
Input Ciphertext	N	W	Z	Q	R	P	V	B	D
Corresponding Number	13	22	25	16	17	15	21	1	3
Sum of corresponding No.	20	36	47	16	34	19	45	15	23
Subtract 26, if sum > 25	20	10	21	16	8	19	19	15	23
convert into corresponding letter, called ciphertext	U	K	V	Q	I	T	T	P	X

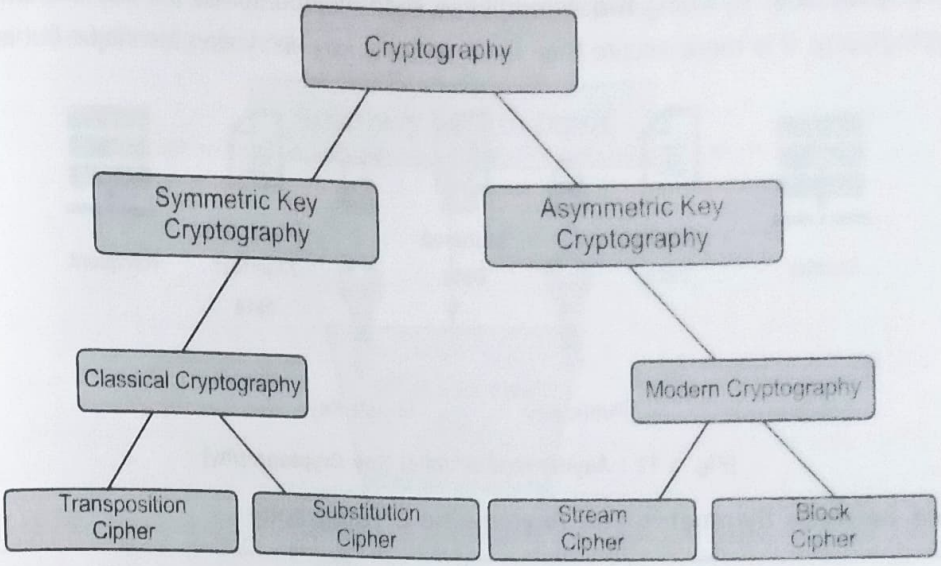
In this technique, one-time pad is discarded after a single use, so this technique is highly secure and suitable for small plain-text message, but this technique is impractical for large messages.

- **Book Cipher/Running-Key Cipher**

A portion of text from a book is used to produce cipher text; this text acts as a one-time pad, and characters from the book are added to the input plain-text message in a manner similar to the Vernam cipher. This basic idea behind the book cipher, also incorrectly called running-key cipher, is quite simple.

1.4.3 Private and Public key cryptography :

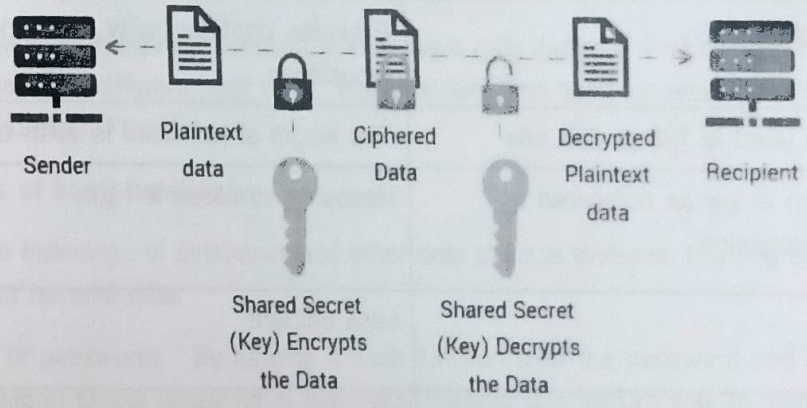
Encryption is the process of converting the original message called plaintext into unintelligible message called ciphertext by the sender. For such conversion sender uses two important components namely **an algorithm** and **the key.** Cryptography can be classified in to two categories as depicted in fig. 1.9.



[Fig. 1.9 : Classification of Cryptographic Techniques]

(1) Symmetric Key Cryptography

In Symmetric-key encryption the message is encrypted by using a key at the sender side and the same key is used to decrypt the message at the receiver side. Such kind of cryptography uses a same key for encryption as well as decryption. In this method of cryptography, key should be kept secret for sender and receiver. Such key is called secret or private key and the method is called symmetric key cryptography or private key cryptography. This method is easy to use but less secure because it requires a safe method to transfer the key from sender to receiver.



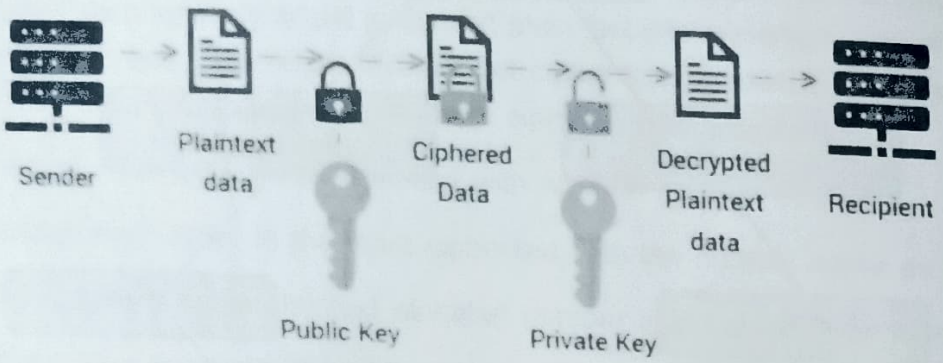
[Fig. 1.10 : Symmetric (Shared) Key Cryptography]

In the above figure 1.10, we can see that same key is used for encryption (sender side) as well as for decryption (receiver side). Symmetric key cryptography emerges the key exchange problem. Symmetric key cryptography is also known as Common Key Cryptography because both the sender and receiver use the same key.

(2) Asymmetric Key Cryptography

One of the major problems with the symmetric key cryptography is how safely transfer the key from sender side to receiver side. This problem is called **key exchange problem**. Asymmetric Key cryptography uses two different keys : one is public key for encryption at sender side and another is private key for

decryption at receiver side. By using two different key such method solves the key exchange problem of symmetric cryptography. It is more secure than the symmetric key encryption technique but is much slower



[Fig. 1.11 : Asymmetric (Public) Key Cryptography]

Difference between Symmetric and Asymmetric cryptography

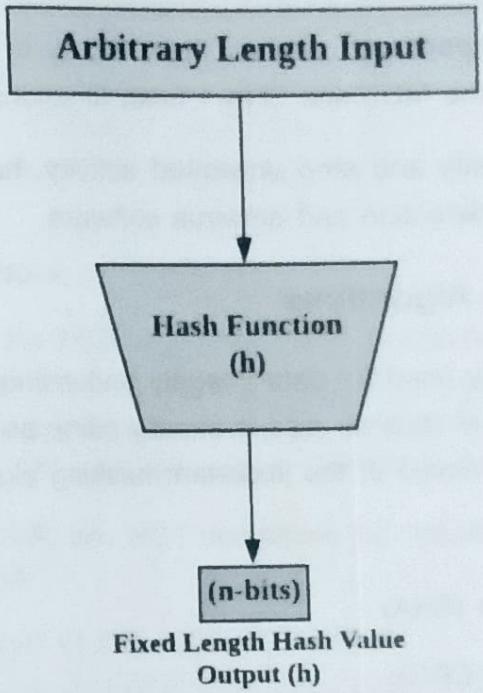
Symmetric Key Encryption (Private Key Cryptography)	Asymmetric Key Encryption (Public Key Cryptography)
Single key for both Encryption and Decryption.	A public key is used for Encryption and a private key used for Decryption.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
Used to transfer large amount of data.	Used to transfer small amounts of data.
Only provides confidentiality.	Provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
Resource utilization is low as compared to asymmetric key encryption.	Resource utilization is high.
More efficient	Less efficient.
Less secure because uses same key.	More secure as two keys are used here- one for encryption and the other for decryption.
Examples : 3DES, AES, DES and RC4	Examples : Diffie-Hellman, ECC, El Gamal, DSA and RSA

1.5 MESSAGE DIGESTING, HASHING AND SHA

1.5.1 Hashing

Hashing is the process of generating a fixed-size output value from variable length block of data as an input. The fixed size output value is called hash value and the algorithm used for such conversion is

alled hash function. Hash function is nothing but a mathematical formula. The working flow of hashing as depicted in the below figure 1.12.



[Fig. 1.12 : Working Flow of Hashing Function]

E.g. if our input value is "hello" then "5d41510abc4b2a76b9719d911017c592" is the output value after applying hashing. Similarly, the output value for the input value "God is Great" is "5ee878141e0cb782e0729066a7d88852". From these two examples we can observe that even though both the inputs with different length, both the output of the hashing function with the same length.

The main objective of the hash function is to achieve data integrity. The change in any bit or bits of the message will generate different hash value. The hash functions used for security applications is referred to as Cryptographic Hash Function.

Applications of hash functions.

- *Database indexing* : In databases and other data storage systems, hashing is used to efficiently index and retrieve data.
- *Storage of passwords* : By running a hash function over the password and saving the hashed result instead of the password in plain text, hashing is a secure way to save passwords.
- *Data compression* : To efficiently encode data, hashing is employed in data compression methods like the Huffman coding scheme.
- *Cryptography* : Digital signatures, Message Authentication Codes (MACs), and key derivation functions are all produced via hashing.
- *Load balancing* : Hashing is used to distribute requests among servers in a network via load-balancing techniques like consistent hashing.
- *Blockchain* : The proof-of-work algorithm, which is a component of blockchain technology, uses hashing to protect the consensus and integrity of the blockchain.

- *Image processing* : Perceptual hashing is one application of hashing used in image processing to identify and stop image duplication and alteration.
- *File comparison* : To compare and confirm the integrity of files, hashing is employed in file comparison methods like the MD5 and SHA-1 hash functions.
- *Fraud detection* : To identify and stop unwanted activity, hashing is utilized in cybersecurity applications like intrusion detection and antivirus software.

1.5.2 Cryptographic Hashing Algorithms

Hashing functions are generally used for data integrity and authentication of sender. Data integrity assures that the message received at receiver side is exactly same as sent by sender. Authentication is achieved through Digital Signature. Some of the important hashing algorithms are :

- Message Digest (MD 5)
- Secured Hashing Algorithm (SHA)
- Cyclic Redundancy Check (CRC)

[A] Message Digest (MD 5)

A message of any length can be entered into the MD5 cryptographic hash function method, which converts it into a fixed-length message of 16 bytes (128 Bits). The message-digest algorithm is known as the MD5 algorithm. MD5 was created with enhanced security features to replace MD4. MD5 always produces a digest size output of 128 bits. Ronald Rivest created MD5 in 1991.

Working of MD5

The MD5 algorithm proceeds as follows :

1. **Append Padding Bits :**

   In the first step, we modify the original message by adding padding bits so that the message's overall length is 64 bits shorter than multiple of 512.

   E.g. Assume a 1000-bit message is sent to us. We now need to append padding bits to the original message. Here, the original message will be appended with 472 padding bits. The output of the first step will have a size of 1472 once the padding bits are added, which is 64 bits less than an exact multiple of 512 (512*3 = 1536).

   Thus Length (original message + padding bits) = 512 * i – 64 where i = 1,2,3 . . .

2. **Padding Length**

   To make your final string a multiple of 512, you must add a few more characters. To accomplish this, take the first input's length and express it as 64 bits. Thus prepare final data to be hashed in multiple of 512 bits.

3. Initialize MD buffer :

we use the 4 buffers i.e. J, K, L, and M. The size of each buffer is 32 bits.

J = 01 23 45 67

K = 89 ab cd ef

L = fe dc ba 98

M= 76 54 32 10

4. Process Each 512-bit Block :

This step is the core of the MD5 algorithm. Here, 4 rounds carried out and in each round 16 operations are performed. Thus, during this a total of 64 operations are performed in 4 rounds. We apply a different function on each round i.e. for the 1st round we apply the F function, for the 2ndround G function, 3rdround H function, and 4th round I function.

We perform OR, AND, XOR, and NOT operations for calculating functions. We use 3 buffers for each function i.e. K, L, M.

- F(K,L,M) = (K AND L) OR (NOT K AND M)
- G(K,L,M) = (K AND L) OR (L AND NOT M)
- H(K,L,M) = K XOR L XOR M
- I(K,L,M) = L XOR (K OR NOT M)

After all, rounds have been performed, the buffer J, K, L, and M contains the MD5 output starting with the lower bit J and ending with Higher bits M.

Advantages of using MD5

- The MD5 algorithm has the advantages of being quicker and easier to comprehend.
- The MD5 method produces a 16-byte strong password. The MD5 algorithm is used by all developers, including web developers, to safeguard user passwords.
- The MD5 method requires comparatively little memory to incorporate.

Disadvantages of using MD5

- MD5 generates the same hash function for different inputs.
- MD5 provides poor security over other advanced algorithms.
- MD5 is neither a symmetric nor asymmetric algorithm.

[B] Secure Hashing Algorithm (SHA)

Secure Hashing Algorithm (SHA) is designed on the base of MD4. It produces a 512-bit message digest.

The input message is divided into number of blocks where each contains 1024 bits. The SHA algorithm is carried out with below steps.

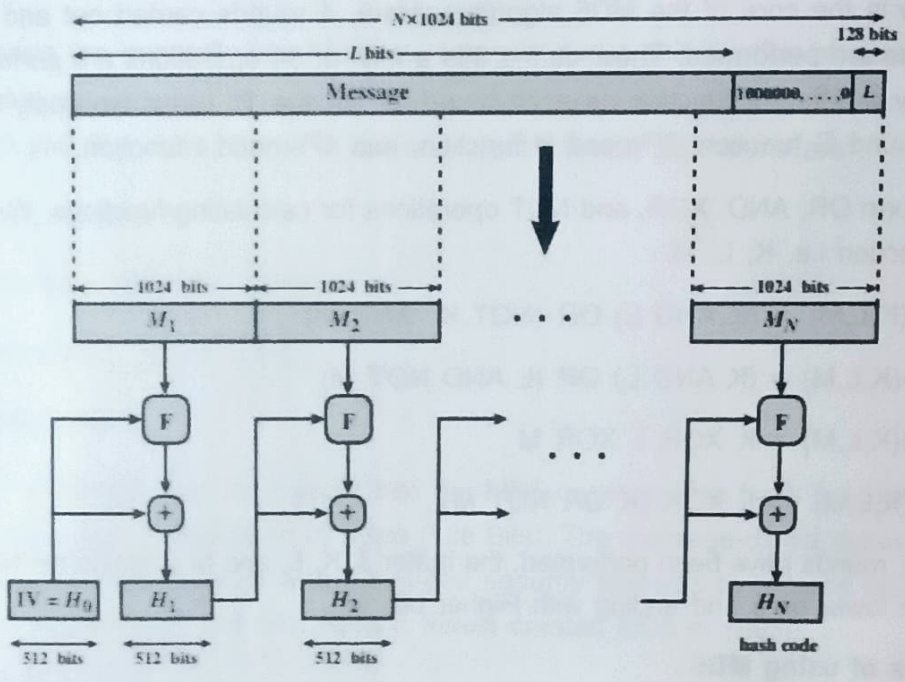
Step 1. Append padding bits.

The message is appended with padding bits so the message is congruent to 896 modulo 1024. The padding bits consists of all o with leading 1.

Step 2. Append Length.

A block of 128 bits is appended to the message. This block contains the length of the original message (before the padding). The message is now integer multiple of 1024 bits in length.

In the below figure 1.13, message is represented as the sequence of 1024 bit blocks M1, M2...Mn the total length of the expanded message is n × 1024 bits.



[Fig. 1.13 : Secure Hashing Message Digesting Process]

Step. 3 Initialise Hash buffer.

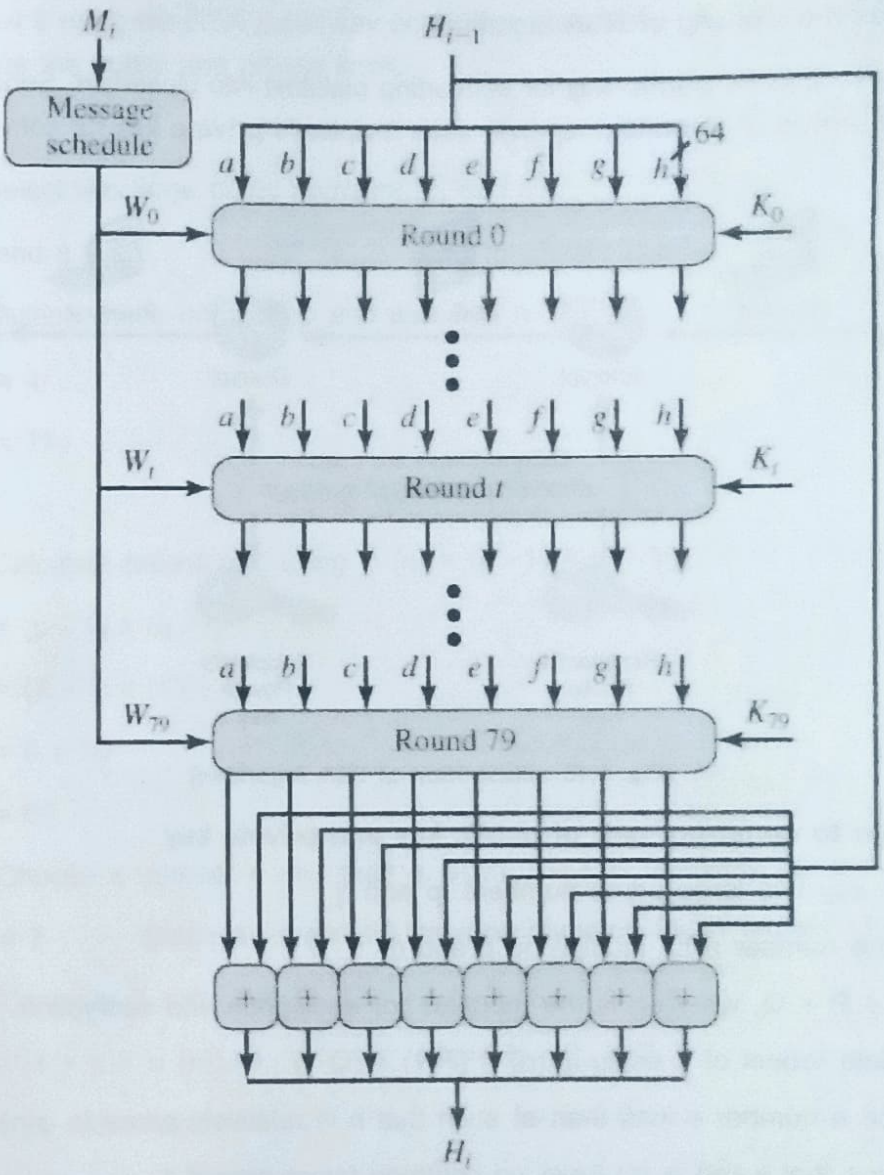
A buffer with capacity of 512 bits can be used to store intermediate as well as final result of the hash function.This Buffer is represented as the collection of eight 64 bits registers namely a, b, c, d, e, f, g, h. these registers are initialised to the 64-bit registers(Hexadecimal values) obtained by taking the first sixty-four bits of the fractional parts of the square roots of the first eight prime numbers.

Step. 4 Process message in 1024 – bit (128 word) blocks

The core part of this algorithm is the module F which is also known as round function. This function consists of 80 rounds. Each round takes input :

- 512-bit buffer value (H_{i-1})
- 64-bit words W_t obtained from the current data block by message schedule.
- Additive constant K_t which represents the first sixty-four bits of the fractional parts of the cube roots of the first eighty prime numbers.

The buffer content is updated after each round completion.



[Fig. 1.14 : Secure Hashing Algorithm (SHA)]

Step. 5 Output

The core part of this algorithm is the module F which is also known as round function. This function consists

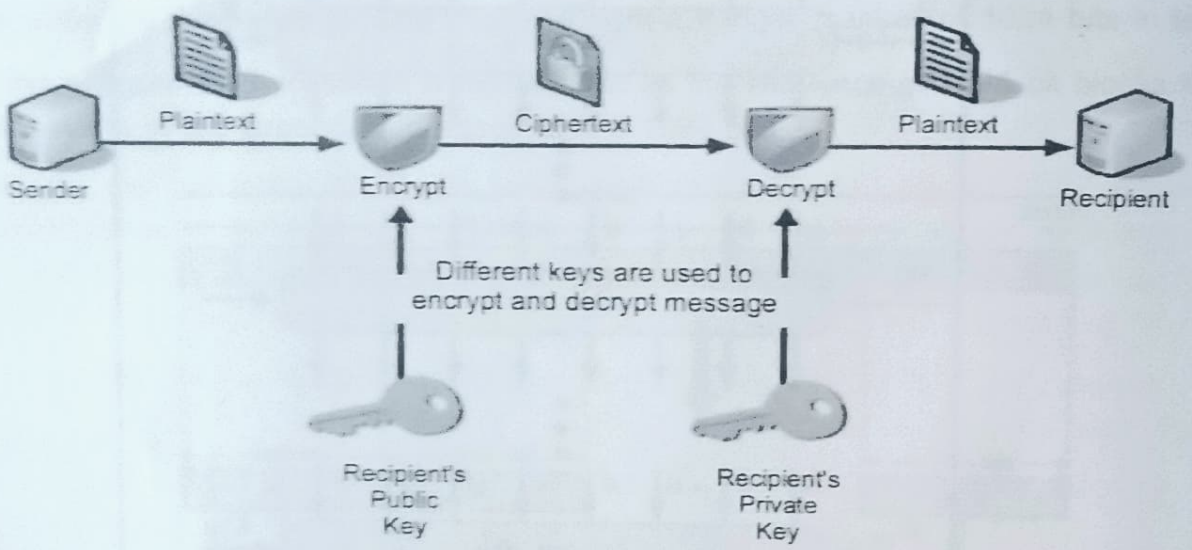
After all the N blocks (1024 bits) have been processed, the output from the Nth stage is the 512-bit message digest.

[C] RSA Algorithm

RSA algorithm was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm. It is an asymmetric cryptography algorithm. Asymmetric cryptography algorithm uses a linked pair of two different keys (public key, private key). The two keys are linked, but the

private key can not be derived from the public key. The Public Key is given to everyone and the Private key is kept private. This algorithm is also known as public key encryption algorithm. The below figure illustrates the working of RSA algorithm.

Sender uses a recipient's **public key** for converting plaintext into ciphertext. Sender sends ciphertext to receiver. On arrival of ciphertext receiver uses recipient's **private key** for converting the ciphertext into plaintext.



[Fig. 1.15 : Illustration of RSA Algorithm]

RSA Algorithm to construct pair of public key and private key

Step 1. Select any two large prime numbers, p and q

Step 2. Find the number n by multiplying p and q.

$n = P \times Q$, where n is the modulus for encryption and decryption.

Step 3. Calculate totient of n using $\varphi(n) = (P-1) \times (Q-1)$

Step 4. Choose a number **e** less than **n**, such that n is relatively prime to $\varphi(n)$.

It means that **e** and $\varphi(n)$ have no common factor except 1.

Step 5. Compute d such that $d \times e = 1 \bmod \varphi(n)$

$\Rightarrow d = e^{-1} \bmod \varphi(n)$

$\Rightarrow$ or $d = (1 + k \cdot \varphi(n)) / e$ where k = 0, 1, 2...

Step 6. Construct pair of public key and private key as under

Public key PU = {e, n}

Private ke PR = {d, n}

Step 7. Compute ciphertext C from plaintext M using public key PU as below. (Encryption)

$C = M^e \bmod n$

Step 8. Compute plaintext M from ciphertext C using Private key PR as below. (Decryption)

$M = C^d \bmod n$

Example :

Encrypt plaintext 9 using the RSA public-key encryption algorithm. This example uses prime numbers 7 and 11 to generate the public and private keys.

Solution :

Step 1 : Select two large prime numbers, p, and q.

$p = 7$ and $q = 11$

Step 2 : Multiply these numbers p and q to find n.

$n = p \times q$

$n = 7 \times 11$

$n = 77$

Step 3 : Calculate totient of n using $\varphi(n) = (P - 1) \times (Q - 1)$

$\varphi(n) = (p - 1) \times (q - 1)$

$\varphi(n) = (7 - 1) \times (11 - 1)$

$\varphi(n) = 6 \times 10$

$\varphi(n) = 60$

Step 4 : Choose a number e less than **n**, such that e is relatively prime to $\varphi(n)$.

Let e = 7 [Because 7 and 60 have no common factor except 1]

Step 5 : Compute d such that

$d = (1 + k \times \varphi(n)) / e$ where k = 0, 1, 2...

$\Rightarrow d = (1 + 0 \times 60) / 7$ for k = 0

$= 1/7$

$\Rightarrow d = (1 + 1 \times 60) / 7$ for k = 1

$= 1/7$

$\Rightarrow$ continue until we get integer result.

$\Rightarrow d = (1 + 5 \times 60) / 7$ for k = 5

$= 301/7$

$d = 43$

Step 6 : Construct pair of public key and private key as under

Public key PU = {e, n} = {7,77}

Private key PR = {d, n} = {43, 77}

Step 7 : Compute ciphertext C from plaintext M using public key PU. (Encryption)

$C = M^e \bmod n$

$= 9^7 \bmod 77$

$= 37$

Step 8 : Compute plaintext M from ciphertext C using Private key PR. (Decryption)

$M = C^d \bmod n$

$= 37^{43} \bmod 77$

$= 9$

In the above example plaintext M = 9 and cipher text C = 37.

Self - Assessment

Q. 1 Answer the below short questions :

(1) Why we need to secure Information ?

(2) What is Information security ?

(3) List out various goals of Information security.

(4) List out basic components of the OSI Security Architecture.

(5) Define the terms : Confidentiality, Integrity, Availability, Nonrepudiation, accountability, Authenticity

(6) Define the terms : Plaintext, Ciphertext, Cryptography, Cryptanalysis, Encryption, Decryption, Algorithm, Cryptology

(7) Differentiate : Attack and threat.

(8) List out different Substitution encryption techniques.

(9) List out different Transposition encryption techniques.

(10) What do you mean by brute-force attack? Explain with simple example.

Q. 2 Explain the below questions :

(1) Explain fundamental goals of Information Security.

(2) Explain OSI Security Architecture in brief.

(3) Short note on : Cryptography

(4) What do you mean by Substitution technique ? Explain with one simple technique.

(5) Explain Play fair cipher technique with suitable example.

(6) What do you mean by Transposition technique ? Explain with simple example.

(7) Explain Basic simple columnar transposition technique.

(8) Explain Vernam Cipher technique with suitable example.

(9) Differentiate : Symmetric Cryptography V/s Asymmetric Cryptography.

(10) Explain hashing with suitable example and working diagram.

(11) Explain hashing with its applications.

(12) Explain Message Digest 5 with its working, advantages and disadvantages.

(13) Explain Secure Hashing Algorithm in brief.

(14) Explain RSA Algorithm with suitable example.

* * *