Introduction to Cyber Crime

* Define Cyber Crime and Information Security.

=) Cyber Crime :

Cyber Crime is refers to criminal activities which is use computer as a tool or target.

Cyber Crime encompasses a wide range of illegal action using the computer network or digital devices.

Cyber Crime include activities such as hacking, spreading malware attacks.

=) Information Security :

Information Security involves the protecting information from the unauthorized access.

Information security protect the computer network from the unauthorized access.

* Classification of Cyber Crime:

=) Here are the main classification of Cyber Crime, according to its nature of the offenses.

1 Email Spoofing:

=) Work:

In this Cyber crime, Attacker creates an email with a fake sender address.

This Fake email may contain the link or malware attachments.

The attacker may pretend to be someone trusted user to elicit sensitive information.

-> Impact:

Email Spoofing can be stolen Personal or Financial information of the user

Systems can be infected with malware which leading to the Further attacks.

Unauthorized user can be get all the sensitive information of individuals or organization.

-> Solution:

Use robust anti-malware solutions to scan the Email attachments.

Alwayes keep software and systems updated to patch vulnerabilities.

Use Email Authentication, for identify the sender information or verify sender identity.

2. Spamming:

=> Work:

In this Cyber Crime, Attacker is also use email to get the sensitive information.

Attacker sending unsolicited emails to a large number of recipients which is often used for promote products or services.

This email may contains links to phishing sites which is designed to get sensitive information.

-> Impact:

This attack may Overloads the email server which lead to slow performance or crashes system.

Also lead to Financial losses due to the scams email and Fraudulent transactions.

-> Solution:

Use Advanced spam Filtering technology to block the unsolicited emails on email server

Implements email authentication protocol to verify and indentify the legitimate senders.

3 Internet Time Theft:

=> Work:

In this type of Cyber Attack, Attacker

gains access to someone's internet service without permission.

The attacker use the victim's internet connection for personal gain.

Using Victim's internet connection, attacker try to get the ~~capt~~ login details of the user.

-> Impact:

When attacker use victim's internet connection, than victim may receive unexpected high internet bills.

Sometime Victim's bandwidth slowing down and victim can not use its own internet for its personal work.

If Attacker use victim's internet in any illegal activities, then Victim may be faces legal issues.

-> Solution:

Victim have to use strong, unique password for its internet service accounts.

Victim have to regular monitor the internet usage For any unusual activity.

or

Victim have to use Employ network security tools to detect and prevent unauthorized access.

4 Salami Attack:

=) Work:

In this cyber attack Attacker makes very small, unnoticed, deductions From victim accounts.

Attacker transFer small amount in the victim accounts, that will add up to significant sum over time.

-> Impact:

Victims lose small amounts of money that accmulate into large sums.

Attackers small size of each theft makes detection difficult and slow in the victims accounts.

In Victims accounts, tracking and investigating numerous small transaction can be complex.

-> Solution:

Victim have to implement robust Fraud detection systems to identify unusual patterns.

Provide customers with real-time alerts for transactions.

Victim's accounts should enforce strong security practices and regular monitoring.

5 Data Hacking:

=> Work:

In this Cyber Attack, Attacker use the systems vulnerabilities or security weakness.

Using Systems Vulnerabilities, Attacker try to gain access to sensitive data without authorized user permission.

Attacker steal or alter data For malicious purposes without user permission.

-> Impact:

Attacker get the all the sensitive data without user permission which data can be any type of personal or financial information.

This Sensitive data can lead to significant financial losses for any individuals or organization.

Due to the data loss victim can be loss trust and credibility for its organization.

-> Solution:

Victim have to conduct regular security assessments and vulnerability scans for the system.

Keep systems and software up-to-date with the latest security patches.

Victim have to use encrypt sensitive data for protect the unauthorized access of user.

6 Credit Card Frauds:

=) Work:

In this cyber attack, Attacker use credit card details from ATMs or payment terminals.

Attacker obtaining card details through hacking the victim databases.

Also use fake website to capture credit card information during victim perform the transactions.

-> Impact:

Victims may suffer significant financial losses due to attacker unauthorized transactions.

Attackers fraudlent activities can negatively impact the victim's credit score.

-> Solution :

Victim have to alwayes use secure payment method and verify the security of website before making transactions.

User have to regularly check the credit card statements for check unauthorized transaction.

User have to use two factor authentication for online transaction.

7 Identity Theft:

=> Work:

In this cyber attack, Attacker collect the user personal information through phising, hacking or social engineering.

Using user's personal information attacker try to create a false identity.

Using this false identity attacker

conduct transaction or access authorized services.

-> Impact:

Because Attacker use False identity, victim may incur debts they did not authorized.

Victim may Face legal issues or complication From the Fraudulent activities of attacker.

Due to the False identity, Victim may suffer from a credit score.

-> Solution:

Every user have to cautious about sharing personal information in online or offline.

User have to implement security Feature like credit Freezes or Fraud alerts.

User have to regularly check credit reports For any unauthorized activities.

8 Password Sniffing:

=> Work:

In this cyber attack, Attackers monitor network traffic to capture passwords.

Attacker use Sniffing tools or software to intercept and record login credentials.

Attacker use unsecured network connection to obtain passwords.

-> Impact:

Using this Attack, Attacker gain access to accounts and try to get authorized sensitive information.

Victim can loss of trust if the breach affects a business or organization.

This attack can lead to data breach and exposure of confidential information.

-) Solution :

User have to use encrypted connection to protect data ~~t~~ during transmission of any information.

User have to Use complex, unique passwords for different accounts.

User have to implement two-factor authentication for additional security ~~and~~ and Use anti-malware tools to detect sniffing.

9 Software Piaracy :

=) Work :

In this Cyber Attack, Attackers Makes illegal copies of software without proper licenses.

Using this Software, Attacker Remove or bypass all the software protection Mechanisms.

=) Impact :

Software developers and companies lose revenue due to piracy of software.

Organization or Individuals can Face legal penalties For software piracy and this software may contain malware or vulnerabilities.

=> Solution:

Organization or Individual ensure that all software used is properly licensed.

Implement anti-piracy technologies and protection in software.

10 Web Jacking:

=> Working:

In this Cyber Attack, Attacker takes a control over the website by using the vulnerabilities.

Attacker stealing login credentials to gain access to the website administration.

=) Impact:

Organization or Individuals can loss the sensitive data on the website.

E-commerce sites can lose revenue due to downtime or redirected traffic.

=) Solution:

Organization or Individuals have to conduct regular security audits to identify and fix the vulnerabilities of website.

Use strong and multi-layer authentication for website administration.

11 Forgery:

=) Working:

In this cyber attack, Attacker create the fake documents or manipulate digital documents or signatures.

Using this document, attacker can conduct the transaction.

=> Impact:

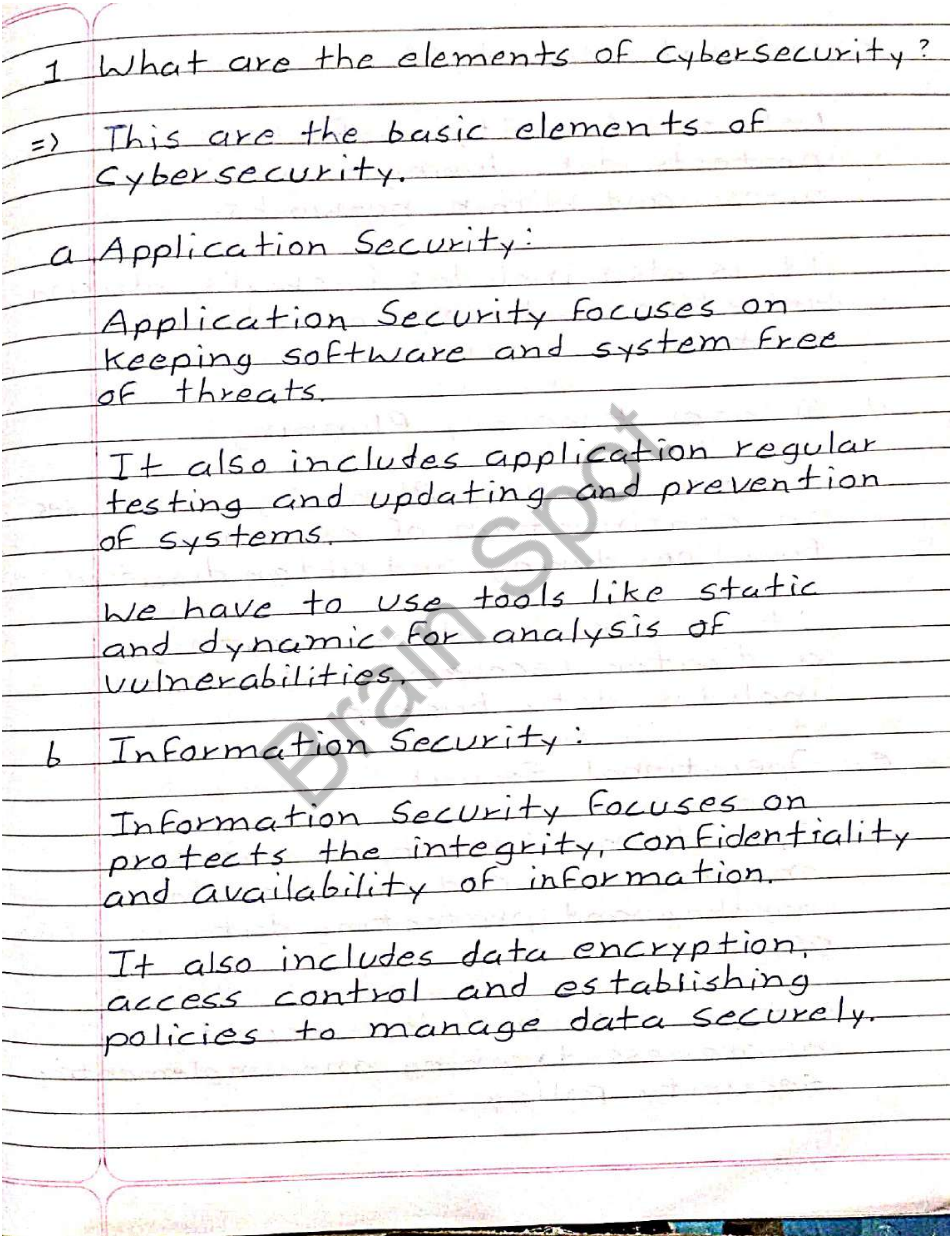
Organization or Individual can faces the legal action and it can be lead to significant Financial losses.

Organization can loss the trust and credibility of businesses.

=> ~~Ka~~ Solution:

Organization have to implement verification system to detect the fake document.

Use digital signatures and certificates to secure digital documents.



1 What are the elements of cybersecurity?

=> This are the basic elements of cybersecurity.

a Application Security:

Application Security focuses on keeping software and system free of threats.

It also includes application regular testing and updating and prevention of systems.

We have to use tools like static and dynamic for analysis of vulnerabilities.

b Information Security:

Information Security focuses on protects the integrity, confidentiality and availability of information.

It also includes data encryption, access control and establishing policies to manage data securely.

c Network Security:

Network Security is Focuses on protects data during transmission across and within networks.

It is also includes Firewalls, intrusion detection and secure networks protocols.

d Disater Recovery Planning:

Disater Recovery Planning is Focuses on continuation of essential Functions during and after disater.

It is also involves creating a disater recovery plant that includes data backup.

e Operational Security:

Operational Security is Focuses on processes and decisions for handling and protecting data assets.

It is also includes security awareness training and implementing security policy.

F End-user Security:

End-User Security is Focuses on educating and protecting the end users who interact with the system and data.

It also ensures users understand the importance of security measures, to avoid common threats.

2 What are the advantages of cyber security?

=> This are the Advantages of Cyber Security.

(i) Protection of Data:

Ensures the confidentiality, integrity and availability of sensitive information from authorized and unauthorized user or system.

(ii) Prevents Unauthorized Access:

Protects systems and networks from unauthorized users, system and potential attackers.

(iii) Mitigates Financial Loss:

Reduces the risk of Financial losses due to cyber attack, data breaches and Fraud.

(iv) Enhances Customer Trust:

Builds trust with customer by demonstrating a commitment to protecting the user data.

(v) Improves Productivity:

Reduces downtime caused by cyber attack and ensures that employees can work efficiently without interruption.

(vi) Mitigates Risks:

Identifies and addresses vulnerabilities and threats before that can be explotied in the system.

(vii) Supports Safe Digital Transformation:

Enables organizations to adopt new technologies and digital initiatives securely.

(viii) Reduces Computer Crash :

Cyber security protect the computer crash and freezing screen of computer while working with technology.

(ix) System availability :

Due to the Cyber Security. System is free from the Threats and it can boost the effectiveness of system.

(x) Handles data management :

Cyber security training helps in managing and preventing access loss of data in the system.

3 What is Cybersecurity ?

=) Cybersecurity is the practice of protecting systems, networks and data.

Cybersecurity prevents system from digital attacks, unauthorized access, damage or theft.

It ensures that sensitive information is not accessed, altered or destroyed by unauthorized parties.

It also involves data encryption, access controls and secure data storage practices.

Cybersecurity ensures that software applications are free from the vulnerabilities.

It also involves detecting, responding to and recovering from cyber incidents.

also involves backup solutions, recovery plan and regular testing of this plan and system.

Cybersecurity provides Security Awarness Training which edcates employees and users about cyber threats.

Involves secure coding practies, regular testing and the use of security tools to detect and fix issues.

Also manages user identities and regulates access to systems and data.

4 What are the difference between SSL and TLS?

=>

	SSL	TLS
1	SSL stands for Secure Sockets Layer.	TLS stands for Transport Layer Security.
2	Supports older and less secure ~~Eg~~ cryptographic algorithm.	Supports morder and more secure cryptographic algorithm.
3	Less Secure	More Secure.
4	Uses the SSL record protocol.	Uses the TLS record protocol.
5	Provides fewer, less detailed alerts.	Provides more detailed and descriptive alert message.
6	Less secure renegotiation Process.	Secure Renegotiation process.
7	Less optimized and slower performance.	Better Performance and protocol optimizations.

5 Explain the brute Force attack.

=> A Brute Force Attack is a method used by attackers to gain Unauthorized access to the system.

In this Attack, Attacker trying all possible combination of password or encryption keys.

Attacker try the combination until the correct one password or encryption keys are found.

A Brute Force Attack work on trial and error manner.

Attackers use software tools to automate the process of guessing passwords by attempting every possible combination.

Attackers use previously stolen username-password pairs.

Attackers start with known password and attempt to find a matching username by systematically trying different usernames.

=) How to Prevent it?

=) This are the method to prevent the system from Brute Force Attack.

(i) Use Strong Passwords:

Ensure passwords are long, complex and unique, combining Uppercase and lowercase letters, numbers and special symbol.

(ii) Use Multi-Factor Authentication:

User have to use Multi-Layer or Two Layer authentication For Login.

(iii) Rate Limiting:

Limit the number of login attempts From a single IP address or user account within a specific username.

(iv) Use Captcha:

Implement Captcha to distiguish between human Users and automated brute Force tools.

(v) Password Hashing:

Store Password using strong hashing algorithms for protect from brute force attack.

(vi) Educate Users:

Informs users about the importance of choosing strong, unique password and multi-layer authentication.

6 What are Black Hat Hackers ?

=> Black Hat Hacker are individuals who use their knowledge of computer system, network and software to conduct malicious activities.

Black Hat Hacker has knowledge about the computer system with its Vulnerabilities.

This Hacker operate with malicious intent and exploit vulnerabilities of system for personal gain.

This Hacker has intent to hack the system for financial profit or to cause harm.

This Hacker gain unauthorized access to computer system, network without permission.

-> Preventing:

(i) Implement Strong Security Measures:

Use Firewalls, intrusion detection/ prevention system to protect the computer system or network.

(ii) Regular Security Audits and Assessments:

Conduct regular security testing and Vulnerability scans to identify and address weekness.

(iii) Data Encryption:

Encrpt sensitive data to protect from unauthorized access using secure encryption algorithm.

(iv) Access Controls:

Implement strict access controls

and monitor user activities to prevent unauthorized access.

7 How to reset a password-protected BIOS configuration?

=> This are the comman method to Reset password.

a. Using a BIOS Password Reset Jumper

Power off the Computer and Open the computer access for motherboard.

Locate the BIOS password reset jumper and Move the jumper from default position to reset position.

Wait For few second and close computer case.

b. Removing the CMOS Battery:

Power off to computer and open computer case for access motheboard.

Locate the CMOS Battery and Carefully remove the CMOS Battery and Wait For 10-15 minutes.

Reinsert the CMOS Battery and Close compute case.

c. Using BIOS Backdoor Passwords:

Some BIOS include a backdoor password, that can be used to access the BIOS if user password is forgotten.

You can try comman password like admin and 1234 or Create new password.

d. Using Manufacture-Specific Tools:

Some Manufacture provide tools or utilities to reset the BIOS password.

Check the Manufacture website or contact their support for tools.

e Contacting Technical Support:

If the above methods do not work or if you are uncomfortable performing this steps, then contanct service provider which provide service to reset the BIOS password.

8 Difference Between Asymmetric and Symmetric Encryption.

=>	Symmetric Encryption	Asymmetric Encryption
1	Uses the Same Key For encryption and Decryption.	Use Public key for encryption and Private key for decryption.
2	Faster Due to simple Algorithm.	Slower due to complex algorithm.
3	Use 128 or 256 bits key For encryption	Use 2048 or 4096 bits key.
4	More efficient For working.	Less efficient For working.
5	Require less Computational Power.	Require More Computational Power.
6	Simple Process due to single key use.	More Complex Process due to Two key use.
7	Less Scalable.	More Scalable
8	AES, DES	RSA, DSA

9 Explain Vulnerabilities in Network Security.

=> Vulnerabilities in network security are weakness or flaws within Network.

Vulnerabilities are the network or system's weakness, which is Used by Attacker to Attack or Hack the system or network.

Using this Vulnerabilities Attacker, try to gain access to the system or network.

Always System or Network's weakness are use by Attacker to access Authorized system without permission.

=> Comman Vulnerabilities:

a Weak Passwords:

Simple, easily guessable password make it easy for attacker to gain unauthorized access.

b Misconfigured Network Devices:

Incorrect Configured routers,

Firewalls and switches can create security gap.

c Insufficient Encryption:

Data transmitted without encryption can be read and intercepted by attacker.

d Poor Access Control:

Inadequate user access control can allow unauthorized ~~allow~~ ~~unauthorized~~ users to access system.

e Vulnerable Network Protocols:

Some network protocol have inherent security weakness that can be exploited.

=> Preventing Network:

a Regular Updates and Patch Management.

b Strong Password Policies

c Proper Configuration Managment.

d Robust Encryption

e Access Control and Management

F Backup and Disater Recovery Planning

10 List out some of common Cyber-attack, write any three attack with an example.

=) Common CyberAttack:

- Email Spoofing
- Spamming
- Internet Time Theft
- Salami Attack
- Data Hacking
- Credit Card Frauds
- Identity Theft
- Password Sniffing
- Software Piracy
- Web Jacking
- Forgery
- Online Frauds

1 Email Spoofing:

In this Cyber crime, Attacker create an email with a Fake sender address.

This fake email may contain the link or malware attachment.

Email Spoofing Can be stolen Personal or Financial information of the user.

Unauthorized user can be get all the sensitive information of individuals or organization.

We have to use Robust anti-malware solutions to scan the email attachment.

2 Salami Attack:

In this Cyberattack, Attacker makes very small, unnoticed, deductions from victim accounts.

Attacker transfer small amount in the victim accounts, that will add up to significant sum over time.

Victims lose small amounts of money that accmulate into large sums.

3 Data Hacking:

In this Cyber Attack, Attacker use the systems vulnerabilities or security weakness.

Using systems vulnerabilities, Attacker try to gain access to sensitive data without authorized user permission.

This sensitive data can lead to significant Financial losses for any individuals or organization.

Victim have to keep system and software up-to-date with the latest security patches.

11 What is MAC ? What is its Use ?

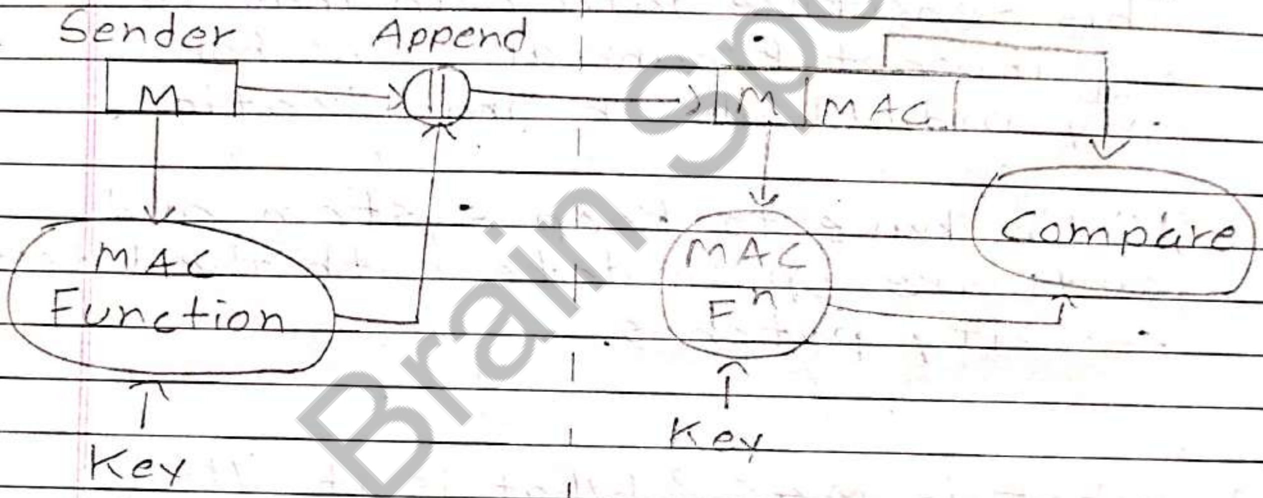
=> MAC is stands For Message Authentication code is a cryptographic checksum.

A MAC ensures that the message has not been altered and verifies the sender's identity.

In this, we have to use secret key to generate a small fixed size block of data called MAC.

Calculation of MAC is
MAC = C(K, M)

where, M = Input data
C = MAC Function
K = Shared Secret Key



Sender Side | Receiver Side

=> Sender Side :

Sender have to passed this message into MAC Function.

MAC Function is generate output which is known as MAC.

After that MAC output and

Original message is append.

=) Receiver Side:

At Receiver Side, We will separate the part of Message from (Message + MAC).

The message is passed in MAC Function which is create Fixed size of block using the secret key.

After the MAC output and MAC will be compare and. So, it is known as authentication.

12 Explain Information Classification Process in brief.

=) Information Classification is the process of categorizing data based on its sensitivity, importance and the level of protection it requires.

This process helps Organizations manage and secure their information assets effectively.

=> Information Classification Process :

1 Identify Information Assets

Identify all information assets within the organization including documents, database, emails and other form of data.

Create an Inventory of information assets.

2 Define Classification Levels :

Establish a set of classification level based on the sensitivity and criticality of the information.

Common Classification Levels :

- Public
- Internal
- Confidential
- Highly Confidential

3 Classify Information :

Assign each information assets to a classification level based on predefined criteria.

4 Implement Controls:

Implement security control and policies appropriate to each classification level to protect the information.

5 Monitor and Review:

Continuously monitor the effectiveness of the classification scheme and make adjustments.

6 Communicate and Train:

Ensure that all employees are aware of the classification scheme and Understand their roles.

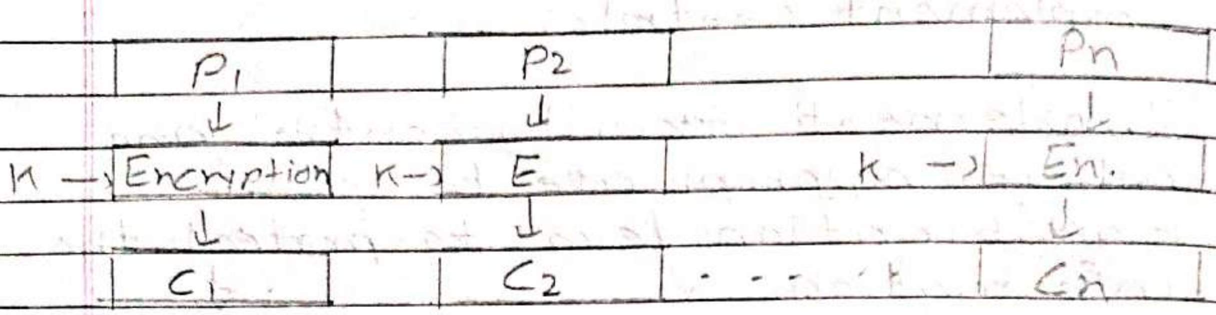
13 Describe various block cipher operating modes in brief.

=) This are the several modes of operation of a block cipher.

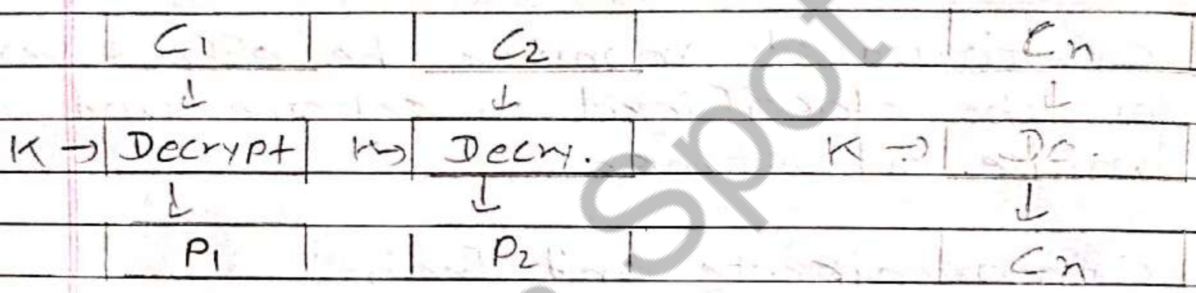
(1) Electronic Code Book:

Electronic Code Book is the easiest mode because of direct encryption of each block of plaintext to encrypted ciphertext.

Encryption :



Decryption:

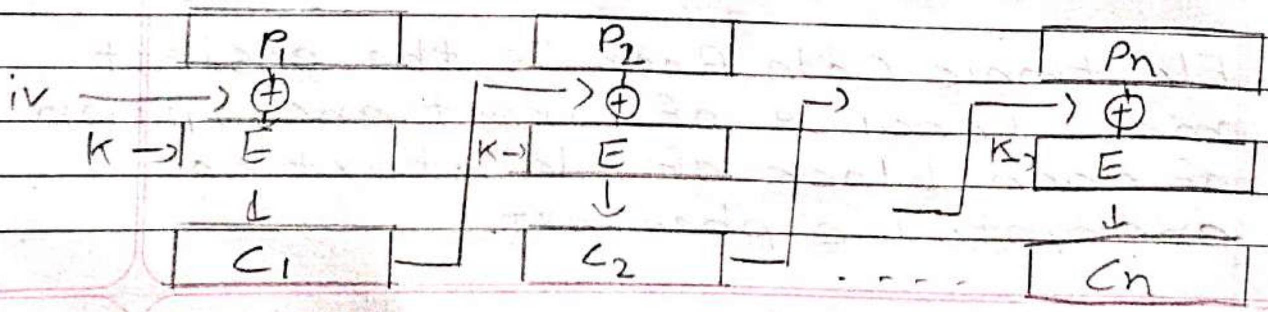


(2) Cipher Block Chaining :

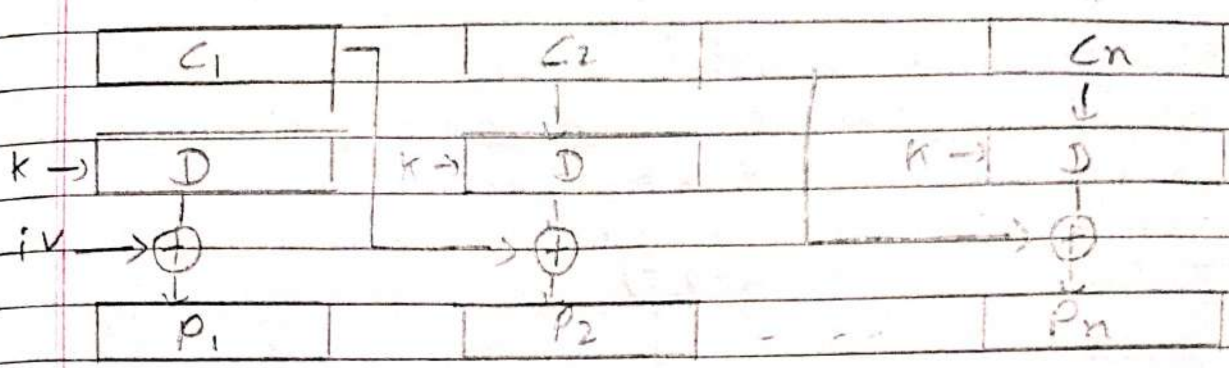
CBC is advancement made on ECB.

In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block.

Encryption:



Decryption:



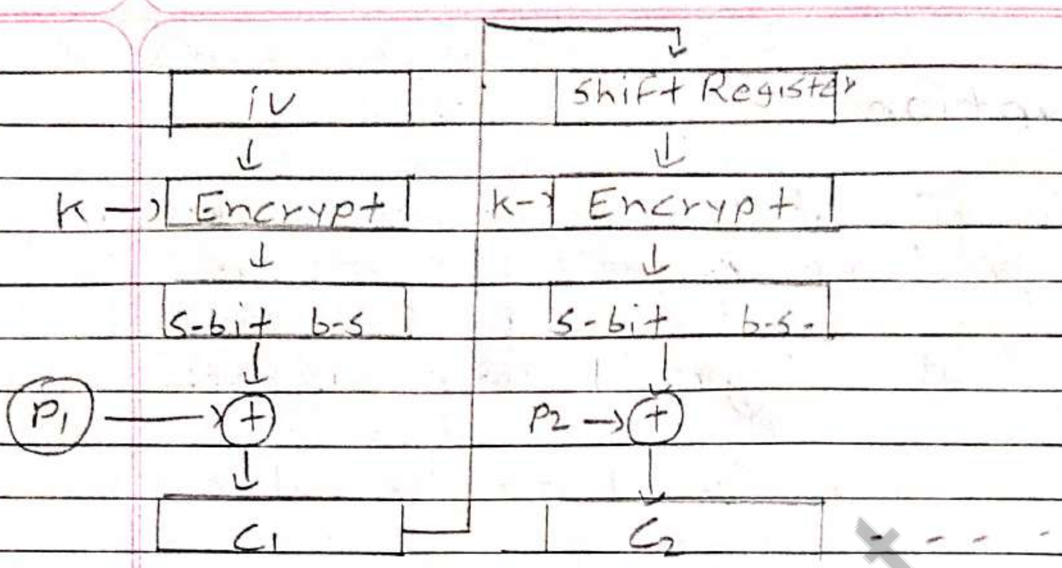
(3) Cipher ~~Fed~~ Feedback Mode:

In this mode, the cipher is given as feedback to the next block of encryption.

First an inital vector vi is used for First encryption and output bits are divided as a set of s and b-s bits.

The left-hand side s-bits are selected along with plaintext bits to which an XOR operation is applied.

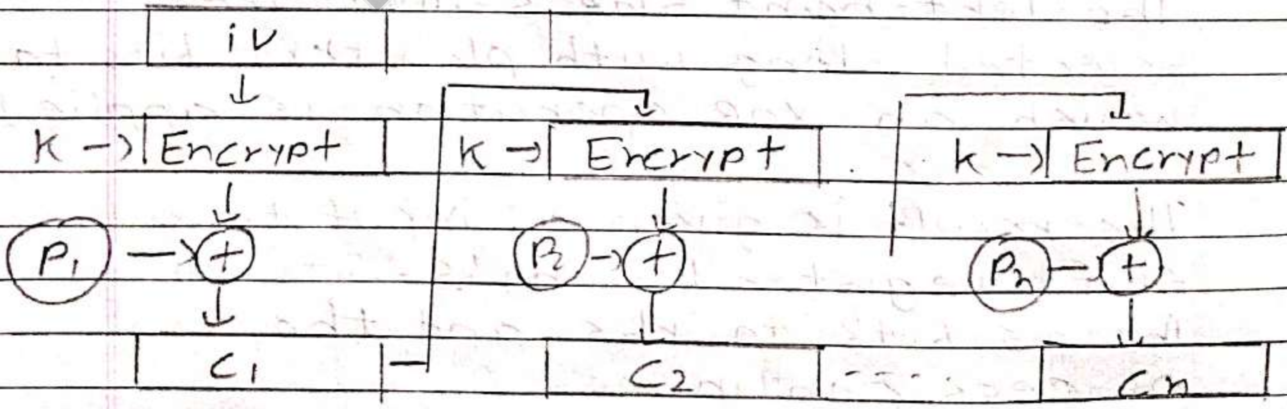
The result is given as input to a shift register having b-s-bits to lhs, s-bits to rhs and the process continues.

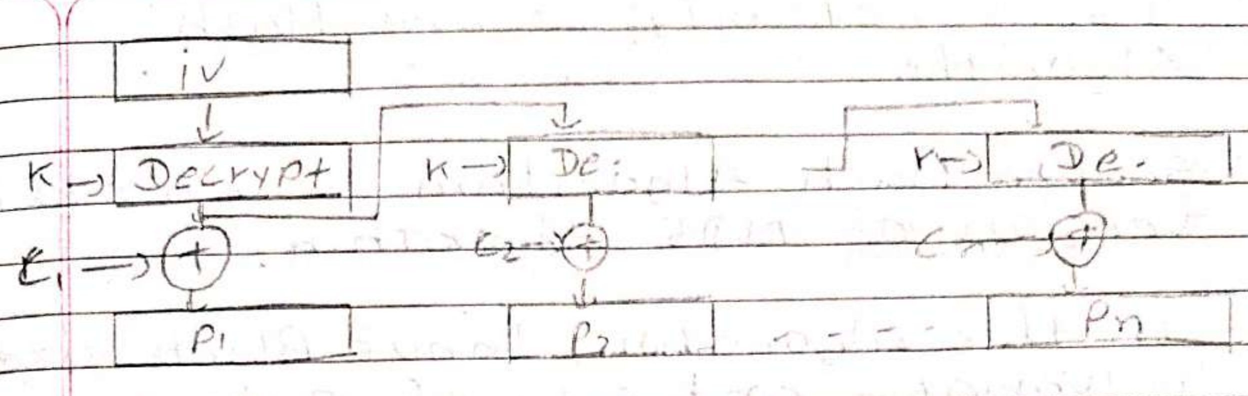


(4) Output Feedback Mode:

It sends the encrypted output as Feedback instead of the actual cipher which is XOR output.

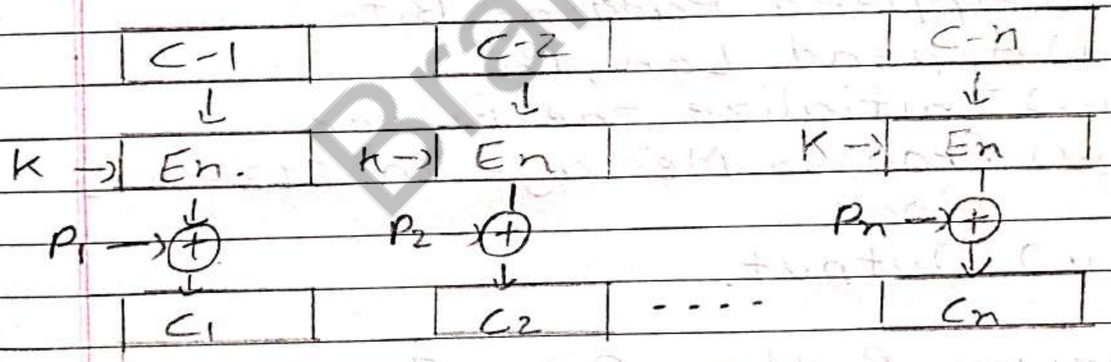
In this output Feedback mode, all bits of the block are sent instead of sending s bits.

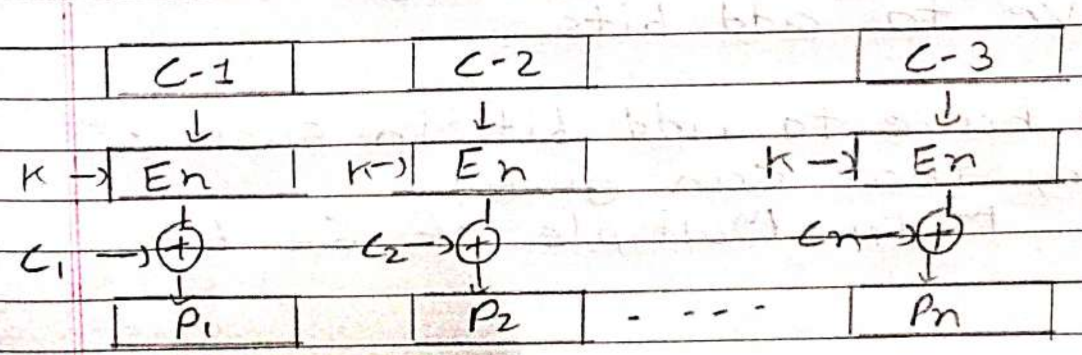




(5) Counter Mode:

CTR mode is a simple counter-based block cipher, every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in cipher block.





14 Discuss clearly Secure Hash Algorithm.

=> Secure Hash Algorithm is a modified version of MD5 Algorithm.

In this algorithm, Input Block size is variable and size of output block is 160 bits.

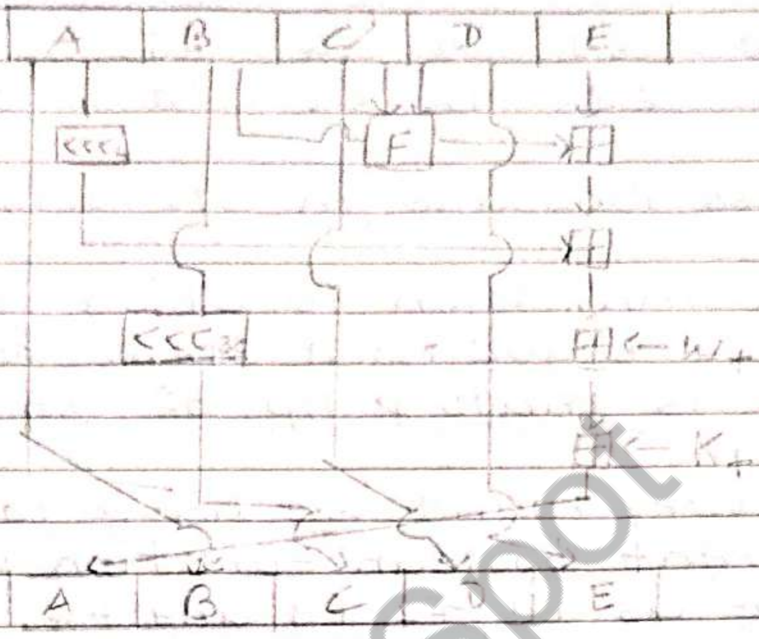
Secure Hash Algorithm 1 is a hash function which takes an input and produces 160 bits hash value.

There are Five Steps in SHA:

(i) Append Padding Bits
(ii) Append Length
(iii) Initialize the Buffer
(iv) Process Message in 512-bits block
(v) Output.

(i) Append Padding Bits: In SHA, According to MD5 algorithm we have to add bits.

~~(ii)~~ We have to add bit in such a way that can gives, ~~Mutp~~ Multiple of 64 bits.



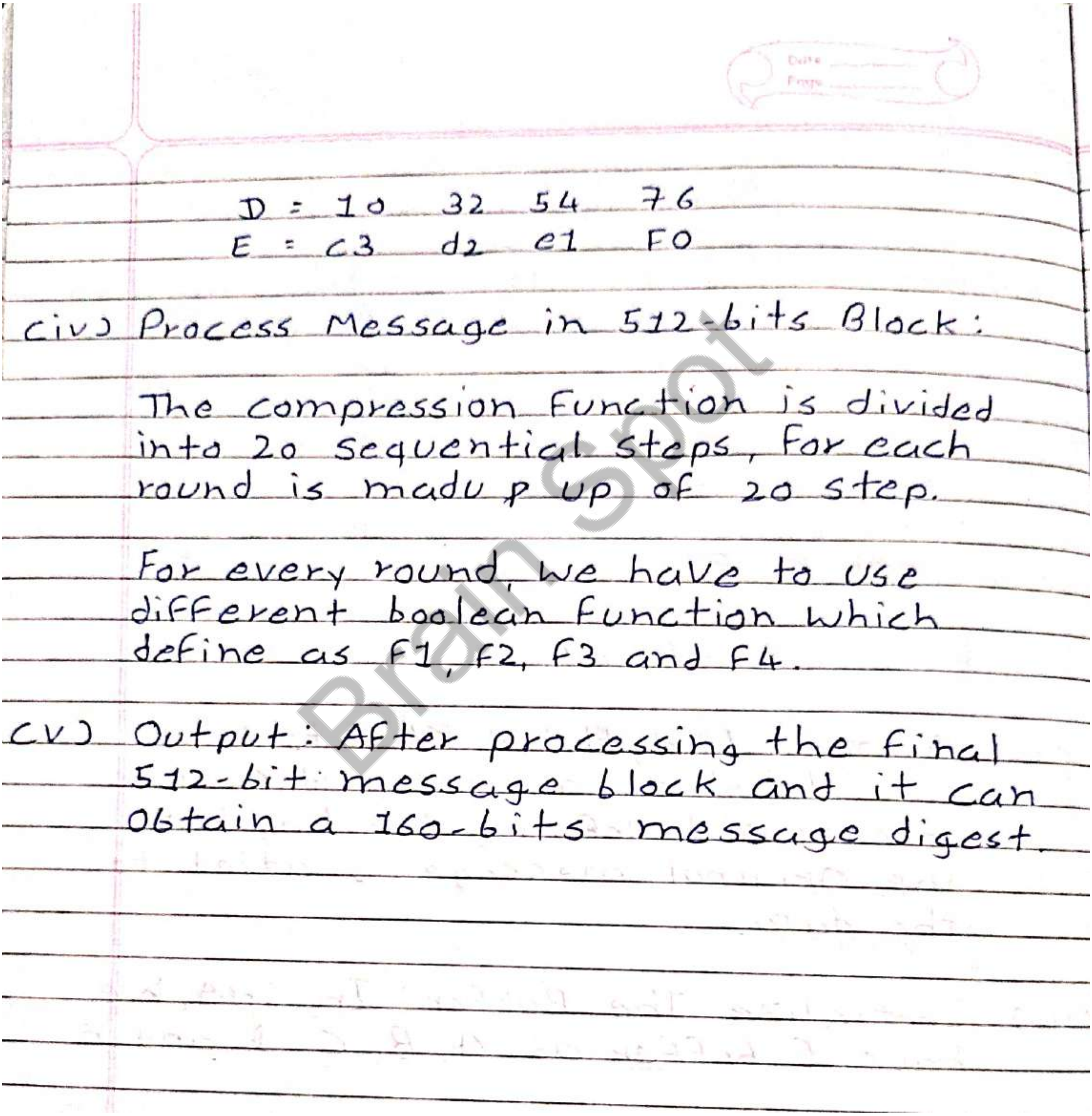
(ii) Append Length: A 64-bits block considered as an unsigned 64-bit integer and defining the length of the Original message is added to the data.

(iii) Initialize The BuFFer: In SHA, We have 5 buffer as A, B, C, D and E.

The BuFFer includes 5 registers of 32-bits which gives 160-bits of output.

This Five register are initialized to the Following 32-bits integers.

A = 67 45 23 01
B = ef cd ab 89
C = 98 ba dc Fe



D = 10 32 54 76
E = c3 d2 e1 F0

(iv) Process Message in 512-bits Block:

The compression Function is divided into 20 sequential steps, For each round is madu p up of 20 step.

For every round, we have to use different boolean function which define as F1, F2, F3 and F4.

(v) Output: After processing the final 512-bit message block and it can obtain a 160-bits message digest.