SGSITS

Name	SHIKHAR MAHAJAN
Enrollment No.	0801CS171077
Subject Code	CO44701
Subject Nomenclature	Information and Network security.
Gsuite id:	gs0801CS171077@sgsitsindore.in
Mobile No.	9131817212
Course	B. Tech
Branch	Computer Science (CSE)
Pages	14
Signature	Shikhar.
Date	20, April, 2021

SCSITS 2/14

20/4/21

Q 1

(a)

Ans => There are 3 main security goals. These are 3 pillars of network security are often represented as CIA triangle.

① Confidentiality: The function of confidentiality is to protect precious business data from unauthorised persons. Confidentiality part of Network security makes sure that the data is available only to the intended and authorized goals.

② Integrity: This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make data reliable and is not changed by unauthorized persons

③ Availability: The function of availability in NS is to make sure that the data, network resources/services are continiously available to the legitimate users.

0801CS171077

Shikhar

SCSITS 3/10

20/4/21

Q1

(b)

Ans= Decline the request and remind your project guide that it is against SCSITS policy.

Justification: As sharing personal credentials over an attack prone network is very dangerous. Moreover, their is no need of personal password to be known by anyone else. Therefore, asking the instructor directly about requesting such data and declining the request is the appropriate thing to do.

(c)

Ans) Cryptoanalytic attacks are those attacks which try to exploit mathematical weakness in the algorithms.

The various types of cryptoanalytic attacks are:-

① Known plain text analysis: Some plain text cipher text pairs are already known

0801CS171077

Shikhar

SCSITS 4/16

20/4/21

The maps is done to find encryption key. ex ⇒ Linear crypto analysis

(2) Chosen plain text analysis: The attacker chooses random plain texts and corresponding cipher text to find encryption key.
ex = Adaptive choosen plain text analysis

(3) Differential cryptanalysis: It is a chosen plain text analysis that analysis text pairs on block ciphers to get key

(4) Man in the middle analysis - Attackers can acquire the keys after find way to insert - themselves in secure channel.

0801CS171077

Shikhar

SGSITS 5/14 20/4/21

Q2
(d)

Ans: SHA 512 is a cryptographic has function completed with 64-bit words. It is based on Merkle-Damaged scheme.
for the creation of message digest in SHA-512 first, the message is divided in blocks of size 1024. The augmented ~~image~~ message consists of the original message, padding and length of original message.

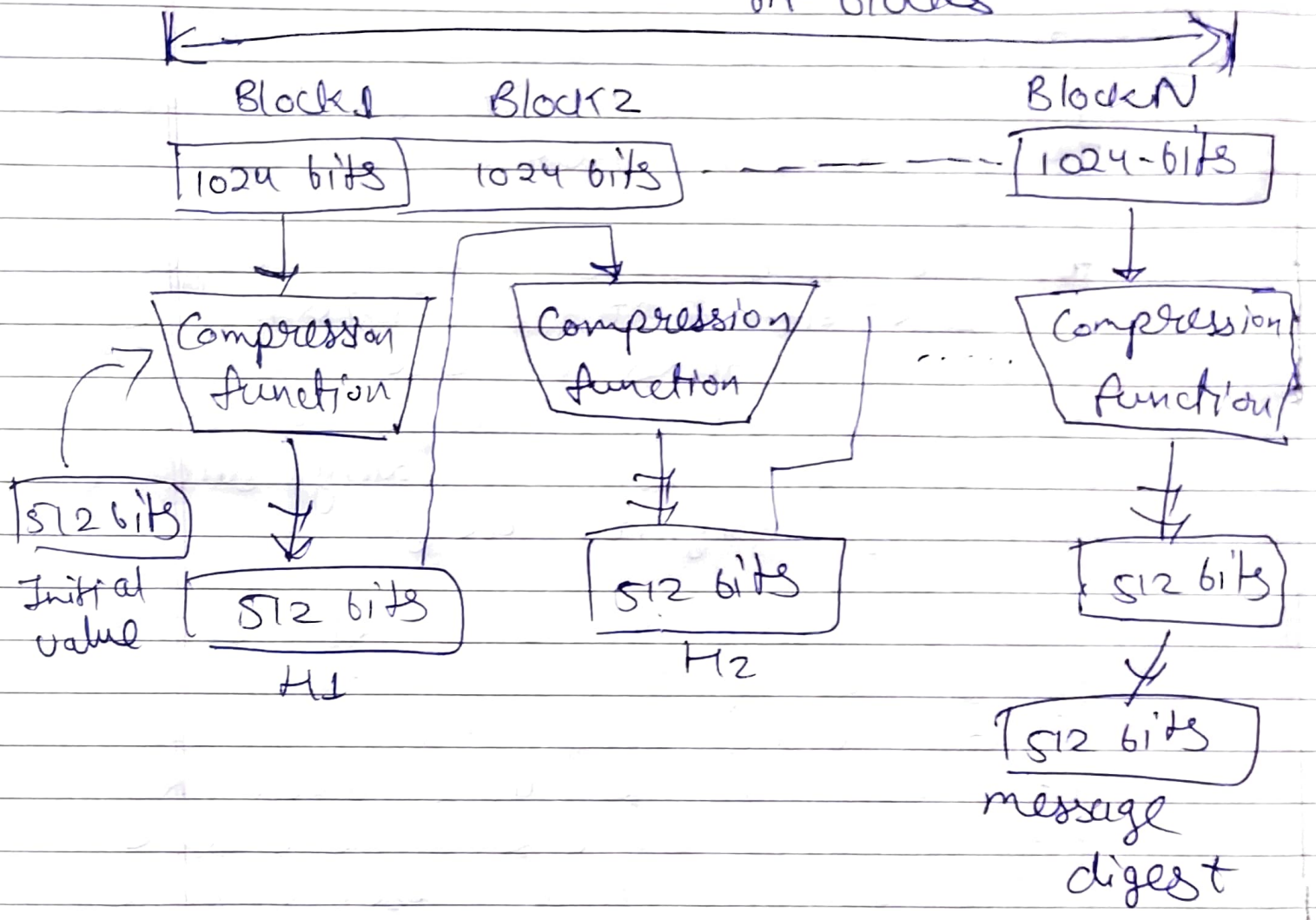
Each of these blocks is then used as one of the inputs for compression function along with the compressed value from the previous block. An initial value of 512 bits is used the 1st block. The final message digest of size 512 bits is the one obtained from the last block of the message.

P.T.O.

0801CS171077 Shikhar

SCSITS 6/14 20/4/11

Augmented message : multiple of 1024 bit blocks



Q2

(e) $\phi(1990) = ?$

$1990 = 2 \times 5 \times 199$

$\Rightarrow \phi(1990) = \phi(2) \times \phi(5) \times \phi(199)$

$\because \phi(m \times n) = \phi(m) \times \phi(n)$

08013171077 Sukhes

SGSITS

7/14

20/4/11

$= (2-1) \times (5-1) \times (199-1)$

$= 1 \times 4 \times 198$

$= 792$

Ans ⇒ $\boxed{\phi(1990) = 792}$

(*) $5^{12} \bmod 11$

$= (5^{11} \times 5) \bmod 11$

$= (5^{11} \bmod 11 \times 5 \bmod 11) \bmod 11$

$\boxed{a^p = a \bmod p}$

$= (5 \bmod 11 \times 5 \bmod 11) \bmod 11$

$= (5 \times 5) \bmod 11$

$= 25 \bmod 11 \quad = 3$

Ans $\boxed{5^{12} \bmod 11 = 3}$

0801CS171077

Smitha

SQSITS 8/14 20/4/21

Q3.

(a)

Ans It is the term used for protecting email account from unauthorized access or from spreading malware or from phishing attack.

(b)	PGP	S/MIME
(i)	It is designed for processing the plain text	It is designed to process email as well as many multimedia files.
(ii)	It is good for personal or office use	It is good for industrial use.
(iii)	It is less efficient	It is more efficient than PGP.
(iv)	It uses diffie hellman digital signature	It uses Elgomal digital signature.

0801CS171077

Shikhar

SGSITS 9/14 20/4/21

Q3

(c) Email services can be secured as:-

(1) Avoid clicking on links or downloading attachments.

(2) Test your SMTP server

(3) Make use of SMTP ssl/TLS ports

(4) Deploy End-to-End Encryption for maximum email security

(5) Use TLS with IMAP and POP3

(6) Maintain IP blacklists to block Targeted spams

(7) Use Restrictive Main Relay options.

(8) Set up reverse DNS lookup to block IPs on when authentication fails

(9) Limit the number of connections to your SMTP server

(10) Learn to inspect message headers

08015171077 Shilchar

SCSITS

10/14

20/4/21

Q 4

Ans=4

(a) A firewall is a software or hardware that prevents unauthorized access to the network

(b)

Ans= The 3 design ~~mod~~ goals of firewall are as follows.

① > Any traffic going outside the system and moving into the system must pass through firewall

② > Only local security policy authorized traffic will be able to get into and out of the firewall.

③ > Internal threats are often at bay as the firewall alert of a possible malware threat

0801CS171077

Siddhi

SQ SITS

11/14

(c) The techniques used by a firewall to control access are:-

1. Service Control: This control determines the type of service that are allowed to access from the network. Traffic are controlled by filtering traffic-based on their IP address, port number or protocol used

2. Direction control: It determines the direction in which the particular service requests are allowed to flow through the firewall.

3. User control: Access to different services are provided according to the user level. Services are provided according to the user type and their level. Generally, this feature is applied inside the local network.

4. Behaviour control: It controls how particular services are used in network. They keep track of particular service in order to find any malicious activity in that service.

080ICS171077

Shikhar

SGSITS

12/14

Q5
(d)

Ans⇒ All systems have assets and security is about protecting assets. The first thing is to know your assets and their value. The second thing is to know what threats are putting your assets at risk. These includes things such as power failure and employee fraud. Threats are partly hypothetical, always changing and always be imperfectly known.

Database security encompases a range of security controls designed to protect the DBMS. The type of database security measures your business should use include protecting the underlying infrastructure that houses the database such as network and server securly configuring the DBMS and the access to the data itself.

It is the collective measures used to protect and secure database software from illegitimate use and malicious cyber threats and attacks.

080CS171077

Shridhar.

SGSITS

13/14

Q5

(e) The different threats to database are—

1. Unauthorised modification
2. Loss of availability
3. Commercial sensitivity
4. Computer misuse
5. Unauthorised disclose
6. Personal privacy and data protection

A security model establishes the external criteria for the examination of security issues in general, and provides the context for database considerations including implementation and operation.
There are 2 database security models

(1) Authentication: The client has to establish the identity of the server and the server has to establish the identity of the client. This is done by means of shared secrets.

0801CS171077

Shikhar.

It can also be achieved by a system of higher authority which has previously established authentication. Authentication is a pre-requisite for authorisation.

(2) Authorization: It relates to the permission granted to an authorised user to carry out particular transactions and hence to change the state of the database or receive data from the database. The result of authorisation, which needs to be on a transactional basis, is a vector:
There is an issue of a server to server security and a problem with amplification as the authorsation is transmitted from system to system.