Graphic Era Deemed to be University
DEHRADUN

Centre for Distance and Online Education

Name of Student: Deepankar Sharma

Student ID: 23351201

Subject Code: OMC 402B

Subject Name: Cybersecurity Information security

Programme Name: MCA - ODL

Semester: 04

Signature of the Student

Ques (1) a)

Name: Deepankar Sharma
Student ID: 23351213
Course: MCA - ODL
Semester: 04

(1) Confidentiality ensures that the information is accessible only to those authorized to have the access. It is achieved using encryption and access control mechanisms

(2) Integrity guarantees that the data remains accurate, consistent and trustworty and is not altered during the transmission or storage.

(3) Authentication is the process of verifying the identity of a user or a system. It ensures that only legitimate entities can access the resources.

b) Various active attacks are:

(1) Message Modification : changing the content of a message in the transit (altering transaction details in online banking)

(2) Denial of Service (DOS) : over loading a system to make it unavailalele to the users.

(3) Replay Attack : capturing and sending / reusing a valid data transmission (eg. resending a login token from site cookies)

(4) Masquerade Attack : pretending to be another (eg. using your friend's ig to talk to his girlfriend)

(5) Session Hijacking : taking over an active session of someone else, (eg hackers in the movie sending threat)

Name: Deepankar Sharma
Student ID: 23351203
Course: MCA - ODL
Semester: 04

Ques (02) a) Block v/s Stream cipher

Stream cipher	Block cipher
Bit by Bit / Byte by byte data processing	Fixed size blocks (eg 64 bit, 128)
Faster speed & simple	Slower speed & complex
Used in Real Time Data encryption for example RC4	used in file encryption, secure storage, for example AES DES

b) cryptoanalysis

Crypto analysis is the study of analysing and breaking cryptographic systems. It involves techniques to find the weakness in encryption algorithm or protocols.

The goal is to decrypt the information without knowing the key. Multiple types of crypto analysis are:

1. Brute force Attack : try all possible combinations
2. Frequency Analysis : monitor the patterns and appearances.
3. Differential Analysis : try to figure out missing parts by altering
4. Side channel Attack : figure out to bypass.

Name: Deepankar Sharma
Student ID: 23351013
Course: MCA - ODL
Semester: 04

Ques ③

a) Digital signature

A digital signature is a cryptographic technique used to verify the authenticity and integrity of a message or document. It uses the sender's private key to sign the data and public key to verify it.

It ensures that the message is not altered and confirms the sender's identity.

b) RSA algorithm

① Key generation

→ choose two prime numbers, $p=3, q=11$

→ calculate $n = p \times q = 33$ and

$$\varphi(n) = (p-1)(q-1) = (10)(2) = 20$$

→ choose $[1 < e < \varphi(n)$, and $\gcd(e, \varphi(n)) = 1]$

$e = 7$

→ Find $d = 3$ $[(d * e) \bmod \varphi(n) = 1]$

→ Public key = $(e, n) \Rightarrow (7, 33)$

Private key = $(d, n) \Rightarrow (5, 33)$

② Message encryption

$m = 2$, cipher $\Rightarrow 29$ $[C = m^e \bmod n]$

↳ $[2^7 \bmod 33]$

③ Decryption

$m = c^d \bmod n \Rightarrow 29^3 \bmod 33 = 2$

Name: Deepankar Sharma
Student ID: 23351203
Course: MCA - ODL
Semester: 04

Ques ④ a) SHA-1 function

SHA-1 (Secure Hash Algorithm) is a cryptographic hash function that produces a 160 bit (20 byte) hash value from an input message. It's mainly used for verifying the data integrity However SHA-1 is now considered insecure due to vulnerability to collision attacks.

b) Biometric Authentication → uses the unique biological traits such as fingerprints, facial recognition or the iris scans to verify the identity.

certificate based Authentication → uses the digital certificates issued by a trusted certificate authority (CA) to verify the user or the device identity in the network communication.

Name: Deepankar Sharma
Student ID: 23351203
Course: MCA - ODL
Semester: 04

Ques ⑤

a) Pretty Good Privacy (PGP)

PGP is an encryption program that provides cryptographic privacy and authentication.

Key Terms include :

① Public/Private keys used for the encryption & decryption

② Digital Signature verifies the senders identity & message integrity.

③ Web of Trust a decentralized model for key verification

④ Message Digest ensures data integrity using hash functions

b) Email Security Attacks

① Phishing deceptive emails that trick user into revealing the sensitive information.

② Spoofing sending emails with a forged sender address.

③ Spam unsolicited bulk messages that contain possibly malwares.

④ Malware attachments emails with infected files.

⑤ Man In the Middle Attack intercepting emails in the transit.