Seat No.: ________ Enrolment No.______________

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA – SEMESTER V - EXAMINATION –SUMMER-2021

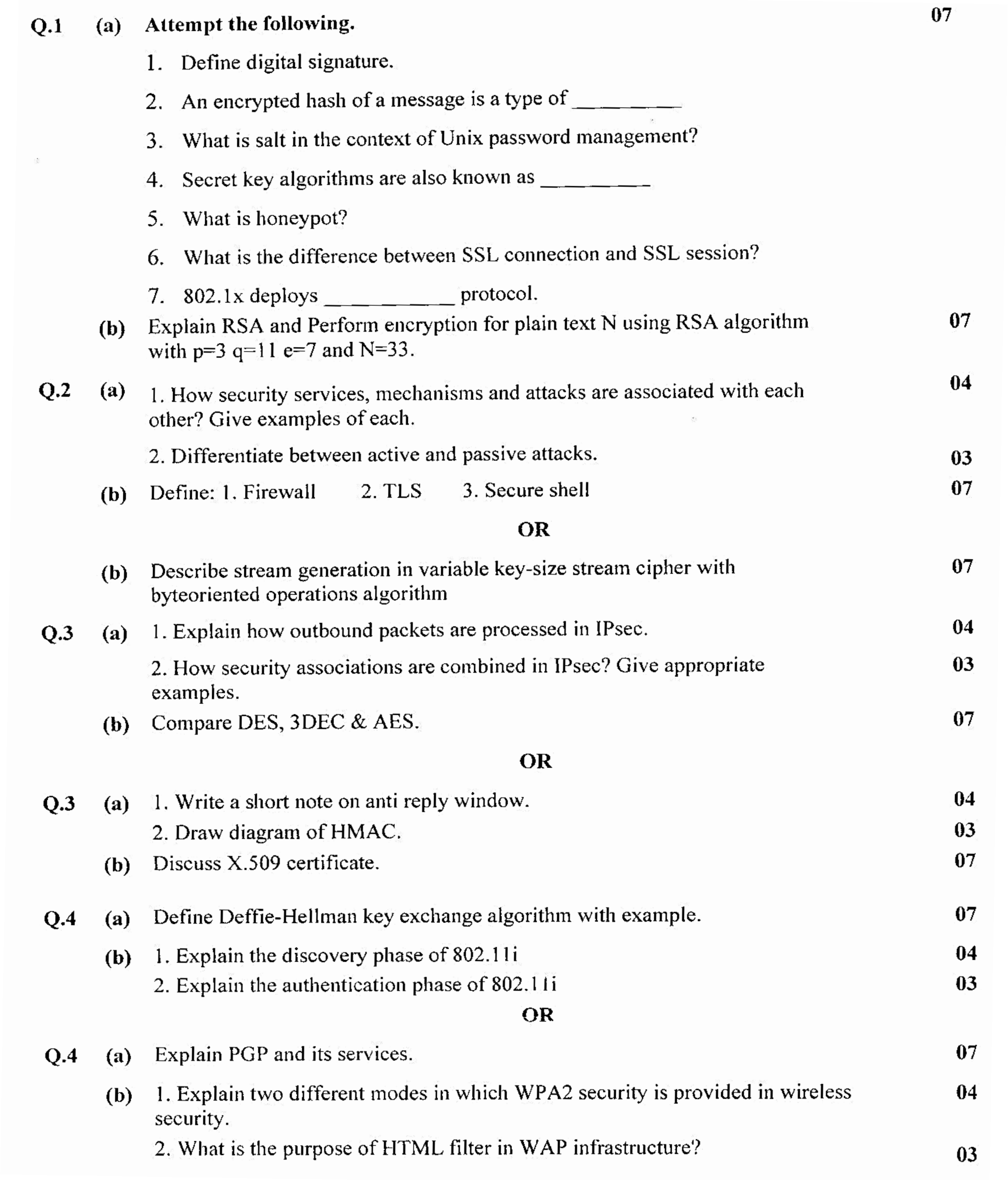
Subject Code: 2650002 **Date: 04-08-2021**

Subject Name: Network Security (NS)

Time: 02:30 PM to 05:00 PM **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make Suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**



Q.1 (a) **Attempt the following.** 07

1. Define digital signature.
2. An encrypted hash of a message is a type of _________
3. What is salt in the context of Unix password management?
4. Secret key algorithms are also known as _________
5. What is honeypot?
6. What is the difference between SSL connection and SSL session?
7. 802.1x deploys ___________ protocol.

(b) Explain RSA and Perform encryption for plain text N using RSA algorithm with p=3 q=11 e=7 and N=33. 07

Q.2 (a) 1. How security services, mechanisms and attacks are associated with each other? Give examples of each. 04

2. Differentiate between active and passive attacks. 03

(b) Define: 1. Firewall 2. TLS 3. Secure shell 07

OR

(b) Describe stream generation in variable key-size stream cipher with byteoriented operations algorithm 07

Q.3 (a) 1. Explain how outbound packets are processed in IPsec. 04

2. How security associations are combined in IPsec? Give appropriate examples. 03

(b) Compare DES, 3DEC & AES. 07

OR

Q.3 (a) 1. Write a short note on anti reply window. 04

2. Draw diagram of HMAC. 03

(b) Discuss X.509 certificate. 07

Q.4 (a) Define Deffie-Hellman key exchange algorithm with example. 07

(b) 1. Explain the discovery phase of 802.11i 04

2. Explain the authentication phase of 802.11i 03

OR

Q.4 (a) Explain PGP and its services. 07

(b) 1. Explain two different modes in which WPA2 security is provided in wireless security. 04

2. What is the purpose of HTML filter in WAP infrastructure? 03

Q.5 **(a)** Explain IEEE 802.11 Wireless LAN. **07**

(b) Discuss Kerberos and its versions. **07**

OR

Q.5 **(a)** Explain Firewall and its types. **07**

(b) Discuss Intrusion and its detection techniques. **07**

****