Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–V • EXAMINATION – SUMMER - 2016

Subject Code: 2650002 Date:06/05/ 2016

Subject Name: Network Security (NS)

Time:10.30 AM TO 01.00 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)** Write any SEVEN **07**

1. A student reading a question paper of university from paper setter's communication with university is an example of which attack?
2. A student modifying university mark sheet from the university database is an example of which attack?
3. When an attacker can have ciphertext that he can decide and a plaintext associated with it, it is known as which type of attack?
4. How DES is used in constructing a 3DES encryption? Write the process in one sentence.
5. Write the full form of MAC
6. An encrypted hash of a message is a type of _____
7. The server in Kerberos which contains information about all users is known as _____
8. The encrypted data by key shared between a client and a TGS which is used to access some service from some server is known as _____
9. Collection of all machines managed by a single Kerberos server is known as _____

(b) Write any SEVEN **07**

1. What is the first step in AES round?
2. RC4 is an example of _____
3. In cipher feedback mode decryption is done exactly as _____
4. The power of counter mode is _____
5. When both encryption and authentication is done together in a cipher mode, it is known as _____
6. A random number in key exchange is popularly known as ___
7. Secret key algorithms are also known as _____
8. When a secret key is used, before processing _____ is a must
9. In Diffie Hellman algorithm when $b = a^i \bmod n$ is calculated where a is a primitive root for prime number n, the value i is known as _____

Q.2 **(a)** Write any SEVEN **07**

1. For error reporting, SSL uses _____ protocol
2. SSH is a protocol for _____
3. Extended service set is _____
4. 802.1x deploys _____ protocol
5. 4 way handshake is used in 802.11i for _____
6. How key exchange is done in PGP?
7. The place where public keys of all other contacts is stored is known as _____ in PGP
8. The certification method used in PGP is known as _____
9. The encrypted content in SMIME is sent using _____

(b) Write any seven **07**

1. A cryptographic algorithm for public key encryption which is competing with RSA uses a type of curve in calculation. Name it.
2. The SSL negotiations begins with _____ protocol
3. ITU-T recommendation for public key certificate is popularly known as _____
4. The bodies which are authorized to provide public key certificates are known as _____
5. The method which IPsec uses for providing encryption as well as authentication together is known as _____
6. The security related information (encryption key, IV etc) is stored in IPsec database known as _____
7. To catch duplicate packets, IPsec implements _____
8. A legitimate user who tries to escalate his rights is known as _____
9. An IDS method which decides the action based on user's behavioral pattern over a period of time is known as _____

OR

(b) Write any seven **07**

1. What is the fundamental tool which records intrusion related information?
2. 'Users must not write to other user's files' is an example of _____
3. When coordination and cooperation is asked for in IDS from different networks, it is known as _____
4. When a system responds back with the strength of the password at the time of entry, it is known as _____ method
5. The firewall service which determines which type of Internet services are accessed, is known as _____
6. A firewall which applies set of rules to each incoming and outgoing packets is known as _____
7. A firewall which remembers the TCP state the connection is in, is known as _____
8. SOCKS is an example of _____
9. A firewall to secure an individual host is known as _____

Q.3 **(a)** Write any two **07**

1. Give one example of each of the three building blocks of security, i.e. security attack, service and mechanism. Show relation between them
2. Give three examples of active attacks
3. Differentiate between peer entity and data origin authentication

(b) Write any two **07**

1. What is feistel cipher structure? Give an example
2. What are dimensions of classifying cryptographic systems?
3. Write at least four advantages of counter mode

OR

Q.3 **(a)** Write any two **07**

1. Write three advantages of using message authentication without encryption
2. Differentiate between weak and strong collision resistance
3. Explain the processing of CMAC

(b) Write any two **07**

1. Write any three requirements of public key cryptography
2. Authenticator is defined as E(Kc, [IDc||ADc||TS]). Explain each field in the context of the function of authenticator
3. What is the purpose of fields subject public key information, issuer unique identifier and subject unique identifier in public key certificate?

Q.4 **(a)** Write any two **07**

1. What is subject alternate name in extension 3 in X.509? why was that needed?
2. What is the job of registrar in PKI?
3. Provide any three reasons for increased web security considerations

(b) Write any two **07**

1. What is the job of SSL Record Protocol?
2. Write any three important differences between SSL and TLS
3. Explain the difference between local and remote port forwarding with respect to SSH

OR

Q.4 **(a)** Write any two **07**

1. Explain the discovery phase of 802.11i
2. Explain the authentication phase of 802.11i
3. Explain the key management phase of 802.11i

(b) Write any two **07**

1. Explain security services of WAP architecture
2. Write at least three differences between WTLS and TLS
3. Why compression happens before signature generation in PGP? Give both reasons

Q.5 **(a)** Write any two **07**

1. How Key legitimacy field, owner trust field and signature trust field are calculated in Web of Trust model in PGP?
2. What is the difference between a clear signed and signed data in S/MIME?
3. Write and explain any three applications of IPsec

(b) Write any two **07**

1. Write any three parameters of SA database and explain their need
2. Explain how outbound packets are processed in IPsec.
3. How security associations are combined in IPsec? Give appropriate examples.

OR

Q.5 **(a)** Write any two **07**

1. How rule based intrusion detection is performed? Give an example
2. How Unix system manages passwords?
3. How a system can detect a bad password in real time? Explain any one method.

(b) Write any two **07**

1. Write and explain any three techniques Firewall uses to enforce control.
2. Explain the functioning of Application proxy firewall
3. Differentiate between application level gateway and circuit level gateway

****