BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Sc.(ANCS)-Hons-2023
Course Name – Cryptography and Network Security
Course Code - BNC60206
(Semester VI)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) What does the principle of confidentiality ensure?
   a) Data is accurate and complete
   b) Data is accessible only to authorized users
   c) Systems are available when needed
   d) Data can be changed by any user

(ii) Which algorithm is an example of asymmetric key cryptography?
   a) DES
   b) 3DES
   c) AES
   d) RSA

(iii) Explain the concept of key distribution in cryptography:
   a) The process of hiding keys within data
   b) The method of sharing encryption keys securely
   c) The technique of generating encryption keys
   d) The act of encrypting keys

(iv) Which entity issues digital certificates in a PKI system?
   a) RA
   b) CA
   c) KDC
   d) HSM

(v) Identify the correct description of Blom's Scheme.
   a) A key pre-distribution scheme ensuring any two nodes can establish a shared key
   b) A method for encrypting large data sets
   c) A protocol for user authentication
   d) A standard for digital signatures

(vi) Choose the type of firewall inspects packets and blocks them based on source and destination addresses.
   a) Proxy Firewall
   b) Packet-Filtering Firewall
   c) Stateful Inspection Firewall
   d) Next-Generation Firewall

(vii) In VPNs, trace what IPsec primarily provides.
   a) Only encryption
   b) Confidentiality, integrity, and authentication
   c) Only authentication
   d) Only integrity

(viii) What is the main advantage of stateful inspection firewalls over packet-filtering firewalls?

a) Faster performance
b) Context-aware decision making
c) Simpler configuration
d) Greater application support

(ix) Determine the protocol which enables real-time, full-duplex communication channels over a single TCP connection.

a) HTTP
b) WebSocket
c) FTP
d) SMTP

(x) Select a common library for implementing WebSockets in Node.js.

a) socket.io
b) ws
c) websocket
d) both socket.io and ws

(xi) Identify the protocol, designed to provide strong authentication for client-server applications.

a) HTTP
b) SSL
c) IPsec
d) Kerberos

(xii) How does SSL/TLS contribute to authentication on the web?

a) Authentication protocols
b) Secure web communications
c) Token management
d) Network routing

(xiii) What is the primary difference between authentication and authorization?

a) Authentication verifies identity; authorization determines permissions
b) Authorization verifies identity; authentication determines permissions
c) Both verify identity
d) Both determine permissions

(xiv) Explain "Default Deny" mean in firewall rules.

a) All traffic is allowed except what is explicitly blocked
b) All traffic is blocked except what is explicitly allowed
c) All traffic is allowed
d) All traffic is blocked

(xv) Which protocol is commonly used by IAS for remote user authentication and accounting?

a) RADIUS
b) LDAP
c) HTTPS
d) FTP

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Discuss the importance of private key management. (3)
3. How does the Registration Authority (RA) function in PKI? (3)
4. Illustrate IPsec and its main purpose. (3)
5. What is the purpose of multi-factor authentication (MFA)? (3)
6. Explain the key pair usage in asymmetric key cryptography. (3)

OR

Explain what is phishing. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Describe the process of encryption and decryption and differentiate between symmetric and asymmetric key cryptography. (5)
8. Explain the roles and functions of the different types of firewalls. (5)
9. Report the role of hashing algorithms in password storage and their importance. (5)
10. Explain the authentication process in the Kerberos protocol and its key features. (5)
11. Recommend the role and effectiveness of Intrusion Detection Systems (IDS) in cybersecurity. (5)
12. Explain the RSA Cryptography Standard (PKCS#1) and its importance. (5)

OR

In a RSA cryptosystem, a participant A uses two prime numbers p = 3 and q = 11 to generate her public and private keys. If the public key of A is 7, then calculate the private key of A. (5)