BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Sc.(ANCS)-Hons-2022
Course Name – Cryptography & Network Security
Course Code - BNCSD502C
(Semester V)

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) Write the process of converting plain text to cipher text.
   a) Decryption b) Authentication
   c) Encryption d) Hashing

(ii) Write an example of a symmetric key encryption algorithm.
   a) RSA b) ECC
   c) AES d) Diffie-Hellman

(iii) Identify the typical key sizes used by AES.
   a) 56 bits, 128 bits, 192 bits b) 64 bits, 128 bits, 256 bits
   c) 128 bits, 192 bits, 256 bits d) 256 bits, 384 bits, 512 bits

(iv) What is the result of a hash function known as?
   a) Key b) Hash Value
   c) Signature d) Ciphertext

(v) Select the protocol considered the more secure successor to SSL.
   a) TLS (Transport Layer Security) b) IPsec
   c) PPTP (Point-to-Point Tunneling Protocol) d) L2TP (Layer 2 Tunneling Protocol)

(vi) An IDS differentiates from an IPS,
   a) IDS monitors and alerts, IPS prevents intrusions b) IDS prevents intrusions, IPS monitors and alerts
   c) IDS encrypts data, IPS decrypts data d) IDS operates at the application layer, IPS at the network layer

(vii) Define the primary concern of authentication in a computer system.
   a) Data encryption b) Verifying identity

c) Preventing malware
d) Managing network traffic

(viii) Select the type of authentication that uses something you know.

a) Token
b) Biometric
c) Password
d) Certificate

(ix) Show which authentication method involves physical or digital objects.

a) Tokens
b) Biometrics
c) Passwords
d) Certificates

(x) Define the access control model that assigns rights based on user identity.

a) Mandatory Access Control (MAC)
b) Discretionary Access Control (DAC)
c) Role-Based Access Control (RBAC)
d) Attribute-Based Access Control (ABAC)

(xi) Show 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

(xii) Write the Unix/Linux tool used for creating user accounts from the command line.

a) useradd
b) usermod
c) userdel
d) usercreate

(xiii) Define what malicious logic refers to.

a) Useful code
b) Malicious software
c) Legal software
d) Open-source software

(xiv) Write what a computer virus attaches itself to.

a) Network packets
b) Host files or boot sectors
c) User passwords
d) IP addresses

(xv) Show how worms spread across networks.

a) Via email
b) By attaching to files
c) By exploiting network vulnerabilities
d) Through physical media

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Describe what the principle of confidentiality ensures. (3)
3. Describe two symmetric encryption algorithms. (3)
4. Define the role of a digital certificate in a Public Key Infrastructure (PKI) system. (3)
5. Describe the key pair usage in asymmetric key cryptography. (3)
6. Evaluate the impact of MIMO technology on 802.11n network performance. (3)

OR

Justify how SSID visibility adjustments could enhance network security. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Compare between digital signatures and end-to-end encryption, for data integrity. (5)
8. Apply multi-factor authentication to enhance system security in a scenario. (5)
9. Compare and contrast the vulnerabilities of WEP and WPA2 in terms of WLAN security. (5)
10. Assess the benefits and challenges of biometric authentication in WLANs. (5)
11. Summarize the effectiveness of Single Sign-On (SSO) in improving WLAN security. (5)
12. Analyze the characteristics of P2P networks, and evaluate their advantages in decentralized communication. (5)

OR

Compare the WebSocket protocol with HTTP, and analyze how their differences affect real-time communication. (5)

****