



**CB – 482**

**VI Semester B.C.A. Examination, August/September 2023  
(CBCS) (F+R) (2016 – 17 and Onwards)  
COMPUTER SCIENCE  
BCA 603 : Cryptography and Network Security**

Time : 3 Hours

Max. Marks : 100

***Instruction : Answer all the Sections.***

**SECTION – A**

Answer **any ten** questions. **Each** question carries **two** marks.

**(10×2=20)**

1. Define any two network security goals.
2. What is digital signature ?
3. What is a Brute-force attack ?
4. Differentiate between stream cipher and block cipher.
5. List any two properties of cryptographic hash function.
6. What is initialization vector ?
7. Give reasons for certificate revocation.
8. Name the entities involved in a Kerberos authentication process.
9. State the difference between MIME and SMIME.
10. State any two features of SSL architecture.
11. What is security association database ?
12. What are payloads ?

**SECTION – B**

Answer **any five** questions. **Each** question carries **five** marks.

**(5×5=25)**

13. Discuss the classification of security goals.
14. Find the GCD (2322, 654) using Euclidean algorithm.
15. Use the additive cipher with key = 10 to encrypt the message "University".

**P.T.O.**



16. Distinguish between public and private keys in asymmetric key cryptosystem.
17. Explain Fermat's little theorem.
18. Explain the various phases of handshaking process in SSL.
19. Write a note on internet key exchange.
20. Briefly explain Tunnel mode of IPSec.

#### SECTION – C

Answer **any three** questions. **Each** question carries **fifteen** marks. **(3×15=45)**

21. Explain in detail the taxonomy of attacks in relation to security goals. **15**
22. a) Explain AES encryption scheme with a schematic structure. **10**  
b) Discuss any two modes of operation for modern block ciphers. **5**
23. a) Explain RSA algorithm including key generation, encryption and decryption process. **10**  
b) Give the difference between conventional signature and digital signature. **5**
24. a) Explain E-mail architecture. **7**  
b) Write a note on certificate authority. **8**
25. a) Explain the main components of a security policy database. **7**  
b) Differentiate between SSL and TLS. **8**

#### SECTION – D

Answer **any one** question. **Each** question carries **ten** marks. **(1×10=10)**

26. Draw the block diagram of DES algorithm and explain. **10**
  27. Write a note on X.509 certificate. **10**
-