UG-C-6004-BCA

2024

Full Marks : 70

Time : 3 hours

Answer from **both** the Groups as directed.

The figures in the right-hand margin indicate marks.

Candidates are required to give their answers in their own words as far as practicable.

GROUP—A

Answer any *four* questions: 10 × 4

1. What do you mean by network security ? Explain the various types of security mechanism used in network security.

2. Define cryptography. State and explain the principles of public key cryptography.

3. Explain RSA algorithm in detail. Perform decryption and encryption using RSA algorithm with $p = 3$, $q = 11$, $e = 7$ and $N = 5$.

(*Turn Over*)

4. What is digital signature ? What are the properties a digital signature should have? Explain the working of digital signature with a neat diagram.

5. Discuss various authentication functions. Explain the format of the X.509 certificate.

6. Describe about SSL/TLS Protocol. Briefly explain the architecture of SSL.

7. Explain the technical details of firewall and describe any three types of firewall with neat diagram.

8. Define intrusion detection and the different types of detection mechanisms, in detail.

GROUP—B

Answer *all* questions: 3 × 10

9. List out the features of SET.

10. Differentiate between symmetric key cryptography and asymmetric key cryptography.

11. Define S/MIME.

12. Name three viruses & describe it.

13. What is Zombie ?

14. Specify the requirements for message authentication.

15. Define Kerberos.

16. Compare stream cipher with block cipher.

17. Differentiate between Active and Passive attack.

18. Define Steganography.

COPYRIGHT RESERVED UG — BCA (C – 604)

2022

Time : 3 hours

Full Marks : 70

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

Answer from both the Groups as directed.

Group – A

Answer any **four** questions of the following :

10×4 = 40

1. Explain the various types of network security mechanism.

2. What do you mean by Cryptography ? Differentiate between Symmetric key and Asymmetric key cryptography.

(Turn over)

3. Draw the block diagram of DES algorithm. Explain briefly.

4. What is Digital Signature ? Explain the working of digital signature with a neat diagram.

5. What is the need of authentication ? Explain various authentication functions.

6. Briefly explain the architecture of SSL.

7. What are the types of Firewall ? Explain each of them in detail.

8. Write short notes on any **two** of the following :

   (a) Virus

   (b) Kerberos

   (c) Worms

   (d) Cryptoanalysis

Group – B

9. Answer **all** questions : 3×10 = 30

   (a) Define Pretty Good Privacy(PGP) protocol.

   (b) Differentiate between monoalphabetic and polyalphabetic cipher.

   (c) Explain the term Integrity.

   (d) Define Block Cipher.

   (e) Compare Substitution and Transposition technique.

   (f) Define Secure Electronic Transaction (SET) protocol.

   (g) Describe how a virus is moved on the internet.

   (h) What is Transport Layer Security (TLS) ?

   (i) Differentiate between Active and Passive attack.

   (j) Define Intruders.

UG — BCA (C – 604)

2019

Time : 3 hours

Full Marks : 70

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

Answer from both the Sections as directed.

Section – A

Answer any **four** questions : 10×4 = 40

1. What do you mean by network security ? Explain network security services.

2. What is Cryptography ? How is data secured electronically ? Explain why encryption alone does not provide integrity of information.

3. What is digital signature ? Explain how it is created by sender and verified by receiver.

4. Explain the role of the different servers in Kerberos protocol. How does the user get authenticated to the different servers ?

5. Explain Secure E-mail protocols and S/MIME.

6. What is IPsec protocol ? Explain, in details, with operation mode. Draw the frame format of IPsec also.

7. What is Firewall ? Explain different types of Firewall.

8. What is the need of SSL ? Explain all phases of SSL Handshake protocol in detail.

Section – B

(Compulsory)

9. Answer all questions : 3×10 = 30

(a) What is Non-repudiation ?

(b) Differentiate between block cipher and stream cipher.

(c) Define and explain Secure Electronic Transaction.

(d) Explain Transport Layer Security Protocol.

(e) Explain Simple Network Management Protocol.

(f) Explain Passive attack.

(g) What do you mean by Intrusion Detection System ?

(h) What do you mean by risk, vulnerability and threats in a network security ?

(i) Explain Key Management in IP security architecture.

(j) What is IP Spoofing ?