BCA(VI) – 602

2010

Candidates are required to give their answers in their own words as far as practicable.
परीक्षार्थी यथासंभव अपने शब्दों में उत्तर दें।

Figures in the margin indicate full marks.
दाहिने ओर किनारे में दिये हुए अंक पूर्णाक निर्दिष्ट करते हैं।

Time – 03 Hours　　　　Full Marks – 80

Candidates are directed to answer in their own words.
Answer any five questions in which Question No.1 is compulsory.

1. Indicate the correct answer:
   (i) Which among the following attack is related to authentication?
   [✓ (a) Interception] (b) Fabrication (c) Modification (d) Interruption.
   (ii) Conversion of plain text into cipher text is known as –
   (a) Encryption (b) Decryption (c) Cryptography (d) Cryptanalyst.
   (iii) If the number of parties involved in a lock-key mechanism is 4, the number of keys needed is - (a) 2 (b) 4 (c) 6 (d) 8
   (iv) In _ _ _ _ one bit of plain text is encrypted at time
   (a) Block cipher [✓ (b) Stream cipher] (c) Both a & b, (d) none of the above.
   (v) DES encrypts blocks of _ _ _ _ _ _ bits.
   (a) 32 (b) 56 [✓ (c) 64] (d) 128
   (vi) To decrypt a message encrypted using RSA, we need the –
   (a) Sender's private key [✓ (b) Sender's public key]
   (c) Receiver's private key (d) Receiver's public key.
   (vii) The _ _ _ _ _ _ _ _standard defines the structure of a digital certificates.
   (a) X.500 (b) TCP / IP (c) ANSI [✓ (d) X.509]
   (viii) Firewall is a specialized form of a –
   (a) Bridge (b) Disk (c) Printer [✓ (d) Router]

2. What is the concept of cryptography and cryptanalysis? Explain how does cryptography help in improving the security of a computer system.
3. What do'you understand by modeler arithmetic? Explain key distribution and traffic confidentially in modelar arithmetic.
4. What is public key cryptography? Discuss RSA and Diffie – Hellman key exchange.
5. What are Substitution, Transposition and Rotal techniques? What are the different types of substitution techniques? Explain.
6. What do you mean by testing of Primality ? State and prove Fermat's and Euler's theorems.
7. What is meant by SSL ? How it works ? Discuss the methods of closing and resuming SSL Connections.
8. What is the concept of IP security ? Discuss its applications and advantages. Also, explain Authentication Header and Encapsulating security payload.
9. What is Firewall? Explain its types and configuration of a Firewall.

*****