COPYRIGHT RESERVED BCA(VI) — 602

2011

Crypto

Time : 3 hours

Full Marks : 80

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

The questions are of equal value.

Answer any five questions in which Q. No. 1 is compulsory.

1. Indicate the correct answer of the following :

   (i) Homophonic substitution Cipher is ________ to break as compared to Mono-alphabetic Cipher.

   (a) Easier

   (c) Difficult

   [✓ (d) Easier or same ✓]

   (ii) There are ________ rounds in DES.

   (a) 8

(b) 10

(c) 14

[✓ (d) 16]

(e) 32

(iii) Symmetric key cryptography is ________ asymmetric key cryptography.

(a) Always slower than

(b) Of the same speed as

[✓ (c) Faster than]

(d) Usually slower than

(iv) SSL layer is located between ________ and ________.

(a) Transport layer, network layer

[✓ (b) Application layer, transport layer]

(c) Data link layer, physical layer

(d) Network layer, link layer

(v) A ________ is used to verify the integrity of a message.

[✓ (a) Message digest]

(b) Decryption algorithm

(c) Digital envelope

(d) None of the above

(vi) RSA __________ be used for digital signatures.

- (a) Must not
- (b) Can not
- [✓ (c) Can]
- (d) Should not

(vii) The CA with the highest authority is called as __________ CA.

- [✓ (a) Root]
- (b) Head
- (c) Main
- (d) Chief

(viii) The __________ protocol is similar to SSL.

- (a) HTTP
- (b) HTTPS
- [✓ (c) TLS]
- (d) SHTTP

2. What are the key principles of security ? Why is confidentiality an important principle of security ?

3. Distinguish between Symmetric and Asymmetric key cryptography. Explain Diffie-Hellman key exchange algorithm.

115

4. What is the difference between modular arithmetic and ordinary arithmetic ? Explain Chinese Remainder Theorem with an example.

5. List the characteristics of a good firewall implementation. What are its limitations ? What are the three main actions of a packet filter ?

6. What are the typical contents of a digital certificate ? Explain the four key steps in the creation of a digital certificate.

7. Distinguish between stream and block ciphers. Explain MDS digest algorithm.

8. Write short notes on the following : two :—

(a) Steganography

(b) Differential and Linear Cryptanalysis

(c) RIPEMID – 160