2017

(5th Semester)

BACHELOR OF COMPUTER APPLICATION

Paper No : BCA-5E2

(Computer Network Security)

Full Marks : 75

Time : 3 hours

(PART : B—DESCRIPTIVE)

(*Marks* : 50)

The figures in the margin indicate full marks for the questions

1. *(a)* Explain a model of Internetwork Security with diagram. 6

(b) What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why? 4

Or

(c) Describe the six services provided by network security. 6

(d) Explain how man-in-the-middle attacks work. 4

2. *(a)* Write notes on AES and DES. 6

(b) Using transposition cipher, encrypt and decrypt the message "I LOVE YOU" with the following key : 4

Plain text : 2 4 1 3 Ciphertext : 1 2 3 4

Or

(c) Explain the procedure of Diffie-Hellman cryptosystem. 6

(d) What are the keys used in cryptography? In what types of cryptography the keys are used? 4

3. *(a)* What is Kerberos? Explain the principles involving in Kerberos protocol. 6

(b) What is password? What are the advantages and disadvantages of using long passwords? 4

Or

(c) Explain the procedure of SHA-1 hash algorithm. 6

(d) Why is Certification Authority so important in network security? 4

4. *(a)* Define IPSec. Explain the two modes of IP Security. 5

(b) What is VPN? Why do we need to use VPN? 5

Or

(c) Describe the protocol of SSL (Secure Sockets Layer). 5

(d) What is firewall? Explain the function of packet filter firewall. 5

5. *(a)* Why do we need to use IDPS? Explain the different types of intrusion detection and prevention system detection methods. 10

Or

(b) Explain any *five* of the following : 2×5=10

(i) Port scanner

(ii) Firewall analysis

(iii) Operating system detection tools

(iv) Vulnerability scanners

(v) Packet sniffers

(vi) Wireless software

★★★

Subject Code : V/BCA/5E2

Booklet No. A

Date Stamp .....

.....

To be filled in by the Candidate

DEGREE 5th Semester
(Arts / Science / Commerce / .....) Exam., **2017**

Subject .....
Paper .....

INSTRUCTIONS TO CANDIDATES

1. **The Booklet No. of this script should be quoted in the answer script meant for descriptive type questions and vice versa.**
2. **This paper should be ANSWERED FIRST and submitted within 1 (one) Hour of the commencement of the Examination.**
3. **While answering the questions of this booklet, any cutting, erasing, over-writing or furnishing more than one answer is prohibited. Any rough work, if required, should be done only on the main Answer Book. Instructions given in each question should be followed for answering that question only.**

To be filled in by the Candidate

DEGREE 5th Semester
(Arts / Science / Commerce / .....) Exam., **2017**

Roll No. .....
Regn. No. .....

Subject .....
Paper .....

Descriptive Type
Booklet No. B .....

Signature of Scrutiniser(s)

Signature of Examiner(s)

Signature of Invigilator(s)

/277

2017

(5th Semester)

BACHELOR OF COMPUTER APPLICATION

Paper No : BCA-5E2

(Computer Network Security)

(PART : A—OBJECTIVE)

(*Marks* : 25)

The figures in the margin indicate full marks for the questions

SECTION—I

(*Marks* : 15)

1. Tick (✓) the correct answer in the brackets provided : 1×10=10

(a) The use of fraudulent e-mails or instant messages to trick users is called

(i) spoofing ( )

(ii) sniffing ( )

(iii) phishing ( )

(iv) mailbombing ( )

(b) Malicious software that looks like a legitimate software is called

(i) Virus ( )

(ii) Worm ( )

(iii) Trojan horse ( )

(iv) DOS ( )

(c) Digital signature provides

(i) confidentiality ( )

(ii) integrity ( )

(iii) non-repudiation ( )

(iv) authentication ( )

(d) Pretty Good Privacy (PGP) is used in

(i) browser security ( )

(ii) e-mail security ( )

(iii) FTP security ( )

(iv) None of the above ( )

(e) ____ is a network that allows authorized access from outside users.

(i) Intranet ( )

(ii) Internet ( )

(iii) Extranet ( )

(iv) None of the above ( )

(f) In a/an ____ cipher, the same key is used by both the sender and receiver.

(i) symmetric key ( )

(ii) asymmetric key ( )

(iii) Either *(i)* or *(ii)* ( )

(iv) Neither *(i)* nor *(ii)* ( )

(g) SHA-1 has a message digest of

(i) 160 bits ( )

(ii) 512 bits ( )

(iii) 628 bits ( )

(iv) 820 bits ( )

(h) A session symmetric key between two parties is used

(i) only once ( )

(ii) twice ( )

(iii) multiple times ( )

(iv) Depends on situation ( )

(i) WPA2 is used for security in

(i) Ethernet ( )

(ii) Bluetooth ( )

(iii) Wi-Fi ( )

(iv) None of the above ( )

(j) Which of the following is antivirus program?

(i) Norton ( )

(ii) K7 ( )

(iii) Quick Heal ( )

(iv) All of the above ( )

2. State whether the following statements are *True* (*T*) *or False* (*F*) in the brackets provided : 1×5=5

(a) A one-time password makes eavesdropping and stealing useless.

( )

(b) In transposition cipher, the locations of characters are changed instead of substitute.

( )

(c) SSL was developed by Microsoft.

( )

(d) A virus is a malicious code that can survive on its own.

( )

(e) A proxy firewall filters at the network layer.

( )

SECTION—II

(*Marks* : 10)

3. Answer the following questions : 2×5=10

(a) Use the Shift cipher with key = 13 to encrypt the message "VIRUS".

(b) Differentiate between conventional signature and digital signature.

(c) What capabilities should a wireless security toolkit include?

(d) What are the two categories of cryptography?

(e) What is the purpose of a firewall?

★★★