BE-comp/sem-VII/CBSGS/CSS/30/11/2015

QP Code : 5904

(59)

(Time: 3hrs) (Marks 80)

1. Question No 1 is compulsory.
2. Attempt any three out of the remaining five questions.

Q1. (a) Define the following with examples:
i)Substitution cipher ii) Poly-alphabetic cipher iii) Salami attack
iv) Session Hijacking V) **10**

(b) With the help of examples explain non-malicious programming errors. **05**

(c) Define the goals of security and specify mechanisms to achieve each goal. **05**

Q2. (a) In an RSA system the public key (e,n) of user A is defined as (7,119). Calculate **Φn** and private key **d**. What is the cipher text when you encrypt message m=10, using the public key? **10**

(b) Give the format of X 509 digital certificate and explain the use of a digital signature in it. **05**

(c) Encrypt "The key is hidden under the door" using Playfair cipher with keyword "***domestic***". **05**

Q3. (a) Explain how a key is shared between two parties using Diffie Hellman key exchange algorithm. What is the drawback of this algorithm? **10**

(b) Differentiate between i) MD-5 and SHA ii) Firewall and IDS **10**

Q4. (a) Explain working of DES detailing the Fiestel structure **10**

(b) What is a Denial of service attack. What are the different ways in which an attacker can mount a DOS attack on a system? **10**

Q5. (a) List the functions of the different protocols of SSL. Explain the handshake protocol. **05**

(b) How does PGP achieve confidentiality and authentication in emails? **05**

(c) Differentiate between the transport mode and tunnel mode of IPSec and explain how authentication and confidentiality are achieved using IPSec. **10**

Q6. Write in brief about (any four): **20**
i) Operating System Security.
ii) Buffer overflow attack.
iii) IP spoofing
iv) Viruses and their types.
v) Key generation in IDEA.

.....

MUPD15025 ANJUMAN-I-ISLAMS KALSEKAR TECHNICAL CAMPUS, COLLEGE OF ENGINEERING, NEW PANVEL 30-11-2015 09:40:08

Course: B.E. (Sem VII) (REV. -2012) (CBSGS) (Computer Engg.)(Prog T2827)

QP Code: 5904

Correction:

Q 1. (a) v) Cross-site scripting.

Please add above option to Q1 (a)

Query Update time: 30/11/2015 12:50 PM

Block no 10.

1) 45275210

2) 45275206

Sangita JS (Dr. S.S. Mishra) (12.55 pm)

Block no.11

1) 45275228 M. Ubaid

2) 45275232

12:55 p.m

Patel Intekhab.

Block no.12

1) 45275247

2) 45275240

Raheel 30/11/15 JS. (1:04) Raheel Qureshi.

Block 13

1) 45275263

2) 45275260

30/11/15 Datta Kamble (1:05) Rel