Code : 051818

B.Tech. 8th Semester Exam., 2017

Cryptography

Time : 3 hours *Full Marks : 70*

Instructions :

(i) The marks are indicated in the right-hand margin.

*(ii) There are **Nine** questions in this paper.*

*(iii) Attempt **Five** questions in all.*

(iv) Questions No. 1 is compulsory.

1. Choose the correct answer of the following (any seven) 2×7=14

(i) Transposition cipher involves

a) Replacement of blocks of text with other blocks

b) Replacement of characters of text with other characters

c) Strictly row-to-column replacement

d) Some permutation on the input text to produce cipher text

(ii) Cryptanalyst is a person who

a) devises cryptography solutions

b) attempts to break Cryptography solutions

c) none of these

d) both of these

iii) Block ciphers can be used as stream ciphers in

a) ECB mode

b) CBC mode

c) OFB mode

d) CFB & OFB mode

iv) When two different message digests have the same value, it is called as

a) Attack

b) Collision

c) Hash

d) None of these

v) Avalanche Effect in block ciphers means

a) All bits of the ciphertext needs to be independent on the plaintext

b) Small change in plaintext should create significant change in ciphertext

c) Ciphertext only depend on most significant bits of plaintext

d) None of the above

vi) Which of the following is independent malicious program that need not any host program?

a) Trap doors

b) Trojan horse

c) Virus

d) Worm

vii) In RSA, given n=221, e=5, the value of d.is

a) 54

b) 87

c) 77

d) None of the above

viii) While creating Digital Envelop, we encrypt one time session key with

a) Senders private key

b) Sender public key

c) Sender master key

d) Receiver's public key

ix) Kerberos is an authentication protocol which includes

a) Password based authentication

b) Challenge Response based authentication

c) OTP based authentication

d) None of the above

x) The SSL record protocol in SSL provides two services

a) Confidentiality & integrity

b) Integrity and authentication

c) nonrepudiation and confidentiality

d) None of the above

2. (a) Explain the steps involve in first round of AES encryption algorithm showing the changes in states.

(b) What are the weaknesses of DES encryption algorithm? Explain briefly. 7+7

3. (a) Encrypt the message, "The key is hidden under the door pad" using the following ciphers: (Ignore the space between words)

(i) Vigenere cipher with key "HEALTH".

(ii) Playfair cipher with key "GUIDANCE".

(b) Explain four common cryptanalysis attacks used for breaking codes. 7+7

4. (a) What are the various functionalities of IDS in system security?

(b) Explain Firewalls works for the security of an organization. 7+7

5. (a) Explain the differences between symmetric and asymmetric key cryptography.

(b) How Kerberos is used to establish authentication in distributed environment? Explain briefly. 7+7

6. (a) What are the strategies used in Modern Block Ciphers and Stream Ciphers.

(b) Explain details any one stream cipher technology for data protection. 7+7

7. (a) What are the steps involved in hashing techniques. Explain with example.

(b) Explain digital signature algorithm (DSA) for signature generation and verification process. 7+7

8. (a) Draw a diagram to tillustrate the Diffie-Hellman key exchange between Bob and Alice. Explain with example how this protocol cannot prevent the man in the middle attack.

(b) Explain how Chosen Ciphertext attack is possible in RSA based cryptosystem. 7+7

9. (a) What are the differences between classical cryptography and modern cryptography?

(b) Use double transposition ciphering technique with transposition key (31452) to encipher and decipher the following message: 7+7

ATTACK TONIGHT

***