

CS/B.Tech/Even/CSE/8th Sem/CS-801D/2014

2014

Cryptography & Network Security

Time Alloted : 3 Hours

Full Marks : 70

The figure in the margin indicate full marks.
Candidates are required to give their answers in their own words as far as practicable

GROUP - A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for the following:

10x1=10

- i) The process of writing the text as rows and reading it as columns is called as
 a) Vernam Cipher
 b) Caesar Cipher
 c) Columnar Transposition Cipher
 d) Homophonic Substitution Cipher
- ii) The principle of _____ ensures that only the sender and the intended recipients have access to the contents of a message.
 a) Confidentiality
 b) Authentication
 c) Integrity
 d) Access control
- iii) The _____ attack is related to authentication.
 a) Interception
 b) Fabrication
 c) Modification
 d) Interruption

1213

1

[Turn over]

- iv) In IDEA, the key size is _____ bits.
 a) 128 b) 64 c) 256 d) 512
- v) To verify a digital signature, we need the
 a) Sender's private key b) Receiver's private key
 c) Sender's public key d) Receiver's public key
- vi) RSA _____ be used for digital signatures.
 a) Must not b) Cannot
 c) Can d) Should not.
- vii) _____ is a message digest algorithm.
 a) DES b) IDEA c) MD5 d) RSA
- viii) Biometric authentication works on the basis of
 a) Human characteristics b) Passwords
 c) Smart cards d) PINs
- ix) _____ forms the basis for the randomness of an authentication token.
 a) Password b) Seed
 c) User id d) Message digest
- x) Firewall is a specialized form of a _____.
 a) Bridge b) Switch
 c) Network d) Router

GROUP - B

(Short Answer Type Questions)

Answer any three of the following.

3x5=15

2. What is Initializing Vector (IV)? What is its significance? 2+3
3. Distinguish between linear and differential cryptanalysis? What do you mean by 2-factor authentication? 3+2
4. What is the idea behind man-in-the-middle attack? 5

1213

2

5. Distinguish between phishing and pharming. Why is it easy to fall prey to pharming than phishing?
3+2
6. How does digital envelope exploit the advantages of both symmetric and asymmetric key cryptography? Describe the functioning of an MAC?
2+3

GROUP - C**(Long Answer Type Questions)**Answer any *three* of the following. 3x15=45

7. a) Is it Possible to combine symmetric key and asymmetric key cryptography so that better of the two can be combined? 5
b) Write short notes on the following:
i) Digital Signature
ii) Message digest.
[5+(5x2=10)]
8. a) Explain active attack and passive attack with example.
b) Describe briefly DES algorithm.
c) Explain Verman cipher.
(5+7+3)
9. a) What are the key principles of security?
b) What would be the transformation of a message "Happy birthday to you" using Rail Fence technique?
c) For a Verham Cipher do the following:
i) Using pad "TZQ" encode "ARE"
ii) Using pad "ARX" decode "YFR".
d) Explain the differences between asymmetric and symmetric key cryptographies.
What are meant by IP sniffing and IP spoofing?
[4+4+3+(2+2)]

10. What is firewall? What are the different types of firewall? State the limitations of firewall. Explain how NAT works with a example. Given, 2 prime numbers $p=19, q=31$. Find out N,E,D in RSA encryption process.
(2+2+3+3+5)
11. a) Consider the diffie-hellman scheme with a common-prime $q=11$ and primitive root $a=2$.
i) Show that 2 is indeed a generator
ii) If the user A has public key $Y_a=9$, what is A's private key?
iii) If the user B has public key $Y_b=3$, what is the secret key K in between A and B?
- b) What is the difference between block cipher and stream cipher? What are the Different modes of block cipher operation? Explain any one of them.
- c) When an encryption algorithm is said to be computationally secure? What are the different types of attacks on computer and network systems?
[5+(2+1+2)+(2+3)]