 End Sem (IV) – MCA (XXII)

**2017**

Time : 3 hours

Full Marks: 70

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

The figures in the margin indicate full marks.

Answer from **all** the Groups are directed.

## Group – A

Answer **all** questions.

1. Choose the correct options of the following: 1x15=15
    a. In Asymmetric key cryptography……key is used for enciphering of plain text and ……key is used for deciphering of cipher text.
        i. Private, Public
        ii. Public, Private
        iii. Public, Public
        iv. Private, Private
    b. Depending upon the key length AES (Advance Encryption Standard) algorithm is given various name. which of the following is not a valid AES type depending upon the key length?
        i. AES – 128

ii. AES – 192
iii. AES – 64
iv. AES – 256

c. In asymmetric key cryptography, the private key is kept by:
    i. Sender
    ii. Receiver
    iii. Sender and receiver both
    iv. All the connected devices to the network
d. Digital Signature envelope is decrypted by using…….
    i. Merchant private key
    ii. Payment's private key
    iii. Payment public key
    iv. Merchant's public key
e. ……..is a block cipher.
    i. DES
    ii. IDEA
    iii. AES
    iv. RSA
f. A substitution cipher substitutes one symbol with:
    i. Keys
    ii. Other symbol
    iii. Both (i) and (ii)
    iv. None of these
g. Man-in-the middle attack can endanger security of Diffie-Hellman method if two parties are not:
    i. Authenticated
    ii. Joined
    iii. Submit

iv. Separate

h. RC4, RC5 are examples of:
    i. Block ciphers
    ii. Hashes
    iii. Stream ciphers
    iv. Public key systems
i. The extended Euclidean algorithm is of interest to cryptographers because:
    i. It allows us to quickly factorize large composites
    ii. It provides a mechanism to calculate a multiplicative inverse
    iii. It allows us to quickly check primality of large primes
    iv. None of the above
j. Which of the following issues is not addressed by Kerberos?
    i. Availability
    ii. Privacy
    iii. Integrity
    iv. Authentication
k. The result of $20^{62}$ mod 77 is:
    i. 1
    ii. 12
    iii. 15
    iv. 34
l. Diffusion hides the relationship between:
    i. The ciphertext and the key
    ii. The ciphertext and the plaintext
    iii. Both (i) and (ii)
    iv. None of the above

m. SHA and MD5 are examples of
    i. Symmetric block ciphers
    ii. Asymmetric block ciphers
    iii. Stream ciphers
    iv. Message signing replay attacks
n. The CBC mode of operation used in DES is provided:
    i. To increase diffusion
    ii. To support bidirectional use
    iii. For public keys
    iv. To combat replay attacks
o. A company uses special ink on its checks to prevent forgeries. The techniques used here is:
    i. Steganography
    ii. Cryptography
    iii. Diffusion
    iv. Message digesting

## Group – B

Answer any **five** questions of the following: 4x5=20

2. State Fermat's and Euler's theorem.
3. What are Kerberos? Also explain X.509 authentication service.
4. What is the weakness of DES? Explain.
5. Explain IP Security Architecture.
6. Discuss Intrusion Detection and Approaches of Intrusion Detection.
7. Briefly explain Elliptical Curve Cryptography.
8. Explain RC5.

## Group – C

Answer any **five** questions of the following: 7x5=35

9. How does PGP provides authentication and confidentiality for e-mail services and for file transfer applications? Draw the block diagram and explain the components.
10. Explain the digital signature and how it is used for authentication?
11. Discuss RSA algorithm. Find out the value of the ciphertext C if the plain text M=5, p=3, q=1 and d=7.
12. Discuss the AES cipher.
13. Briefly explain about the Diffie-Hellman Key Exchange.
14. Explain Message Authentication Code(MAC). What is/are the difference(s) between MAC and Modification Detection Code(MDC)?
15. Write short notes on the following:
    a. DDoS attack
    b. E-mail Security

…….*……