Sub Code: RCAE21

Paper Id: 214503 Roll No: | | | | | | | | | | | | | |

MCA
(SEM V) THEORY EXAMINATION 2019-20
CRYPTOGRAPHY& NETWORKW SECURITY

Time: 3 Hours ***Total Marks: 70***

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. 2 x 7 = 14

a.	Using extended Euclid algorithm, find GCD (150, 9).
b.	Why the concept of Avalanche effect is required?
c.	Show 2 is the primitive root of 11
d.	Which type of encryption uses only one shared key to encrypt and decrypt?
e.	Define Euler's theorem and its' application.
f.	Between symmetric and asymmetric encryption which method is more convenient and why?
g.	Using playfair Cipher and the keyword **'KINGDOM'**, encrypt the plain text **'HELLO WORLD'.**

www.aktuonline.com

SECTION B

2. Attempt any *three* of the following: 7 x 3 = 21

a.	How Block Cipher Modes Of Operation in DES helps and compare the CFB and OFB mode of operations..
b.	How email security is provided through PGP? Also describe the PGP message generation and PGP message reception
c.	In a public key system using RSA, if the Cipher Text C = 10, public key e=5, n =35, what is the plain text corresponding to the Cipher Text C?
d.	What do you understand by Feistel cipher structure? Illustrate by some example.
e.	Find all Primitive roots of 25.

SECTION C

3. Attempt any *one* part of the following: 7 x 1 = 7

(a)	What basic arithmetical and logical functions are used in MD5? Explain SHA-1 logic. Compare SHA-1 and MD5
(b)	What services does IPSec provide? What is the difference between transport mode and tunnel mode?

4. Attempt any *one* part of the following: 7 x 1 = 7

(a)	State Chinese Remainder theorem. Use it to solve the following congruence to obtain value of x:- X≡1 mod 3; X≡2 mod 5; X≡3 mod 7
(b)	For a Deffie-Hellman scheme with common prime q = 11, and primitive root α = 2, generate a set of public key and private key pairs between two users A and B. Make your own assumptions.

http://www.aktuonline.com

Sub Code: RCAE21

Paper Id: 214503 Roll No: | | | | | | | | | | | | | |

5. Attempt any *one* part of the following: 7 x 1 = 7

(a)	How symmetric keys can be distributed? Describe a key distribution scenario between users A, B and KDC. Assume that users A and B share a unique master key with KDC.
(b)	What do you understand by Digital signature? What is the difference between direct and arbitrated digital signature?

6. Attempt any *one* part of the following: 7 x 1 = 7

(a)	Identify the requirements for a Hash function? What is Birthday attack on Hash codes? Also explain the Weak collision resistance and strong collision resistance?
(b)	What do you mean by test of primality of a number? Explain.

7. Attempt any *one* part of the following: 7 x 1 = 7

(a)	Write down short notes on any three of following: -- i. HTTPS ii. Digital certificates
(b)	What is Kerberos? Explain the role of Authentication Server (AS) and Ticket Granting Server (TGS) in Kerberos authentication Protocol.

www.aktuonline.com

http://www.aktuonline.com