Reg.No. _____

Karunya UNIVERSITY

(Karunya Institute of Technology & Sciences)
(Declared as Deemed-to-be University under Sec.3 of the UGC Act, 1956)

End Semester Examination – Nov/Dec – 2016

Code : 14CS2008 **Semester : 2016-17 ODD**
Sub. Name : Cryptography and Network Security **Duration : 3hrs**
Max. marks : 100

ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)

Q. No	Sub Div.	Questions	Course Outcome	Marks
1.	a.	Discuss the strengths of DES.	CO2	**5**
	b.	Explain with details the AES transformation functions.	CO2	**15**
		(OR)		
2.	a.	Draw and explain single round of DES operation.	CO1	**10**
	b.	Illustrate the AES key expansion with a suitable diagram.	CO1	**10**
3.	a.	Perform encryption and decryption using the RSA algorithm for the following: p = 3; q = 11, e = 7;M = 5	CO3	**15**
	b.	Describe the techniques used for the distribution of public keys.	CO2	**5**
		(OR)		
4.	a.	Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root 7. i. If user A has private key 5, what is A's public key? ii. If user B has private key 12, what is B's public key? iii. What is the shared secret key?	CO1	**10**
	b.	Summarize the steps involved in ElGamal cryptosystem to encrypt and decrypt the given message.	CO3	**10**
5.	a.	With necessary sketch, explain HMAC algorithm.	CO2	**10**
	b.	Draw and explain the single round of SHA-512 operation.	CO1	**10**
		(OR)		
6.		Demonstrate the signing and verification process in DSS using the values given. p=23; q=11; h=16; x=7; k=5; H(M)=10	CO1	**20**
7.	a.	Compare and contrast Kerberos v4 and v5 dialogs	CO2	**10**
	b.	Describe the process of obtaining and revoking X.509 certificate?	CO3	**10**
		(OR)		
8.	a.	Explain with adequate diagram the transmission and reception of PGP messages.	CO2	**10**
	b.	Describe the various types of firewalls.	CO3	**10**
		Compulsory:		
9.	a.	Explain the various kinds of security attacks on systems and networks; also discuss the possible countermeasures.	CO3	**10**
	b.	Encrypt the message "meet me at central library" using playfair cipher. (Hint: use the key "victory"	CO1	**10**

ALL THE BEST