GALGOTIAS UNIVERSITY

ADMISSION NUMBER

School of Computing Science and Engineering

Bachelor of Technology in Computer Science and Engineering
Semester End Examination - Jul 2024

Duration : 180 Minutes
Max Marks : 100

Sem VI - R1UC613C - Cryprography and Network Security

General Instructions
Answer to the specific question asked
Draw neat, labelled diagrams wherever necessary
Approved data hand books are allowed subject to verification by the Invigilator

1)	Briefly explain the MD5	K1(2)
2)	Write an algorithm in pseudocode for the Chinese remainder theorem.	K2(4)
3)	Explain the use of Kerberos and name its servers	K2(6)
4)	Apply the row transposition with key {4312567}, to encrypt "Attack postponed until two am". Also decrypt the ciphertext to find the result.	K3(9)
5)	Using the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t. (KL-3, Unit 1) a. 291 and 42 b. 84 and 320 c. 400 and 60	K3(9)
6)	What is a key? "Length of the key is directly proportional to the cipher strength" Defend this statement with example.	K5(10)
7)	In subkey generation in CMAC, it states that the block cipher is applied to the block that consists entirely of 0 bits. The first subkey is derived from the resulting string by a left shift of one bit, and, conditionally, by XORing a constant that depends on the block size. The second subkey is derived in the same manner from the first subkey. Discuss a. What constants are needed for block sizes of 64 and 128 bits? b. Explain how the left shift and XOR accomplishes the desired result.	K4(12)
8)	The first 16 bits of the message digest in a PGP signature are translated in the clear. a. Determine To what extent does this compromise the security of the hash algorithm? b. Determine To what extent does it in fact perform its intended function, namely, to help determine if the correct RSA key was used to decrypt the digest?	K5(15)
9)	With DSS, because the value of k is generated for each signature, even if the same message is signed twice on different occasions, the signatures will differ. This is not true of RSA signatures. What is the practical implication of this difference? Justify.	K5(15)
10)	Elaborate why confusion and diffusion are integral to a cipher's architecture. Based upon this discussion, compare the security of stream and block ciphers.	K6(18)