GALGOTIAS UNIVERSITY

ADMISSION NUMBER

School of Computing Science and Engineering

Bachelor of Technology in Computer Science and Engineering
Semester End Examination - Jun 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)	Define a statistical attack.	K1(2)
2)	Define X.509 and explain its purpose.	K2(4)
3)	Calculate additive inverse of 8 in Z10	K2(6)
4)	Identify the changes that are required in HMAC to replace one underlying hash function with another?	K3(9)
5)	How can you construct a better and secure MAC for post quantum world.	K3(9)
6)	It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible? Explain	K5(10)
7)	Alice uses Bob's RSA public key (e = 7, n = 143) to send the plaintext P = 8 encrypted as ciphertext C = 57. Simplify how Eve can use the chosen-ciphertext attack if she has access to Bob's computer to find the plaintext.	K4(12)
8)	Prove (using example) the following: a. a ≡ b (mod n) implies b≡ a (mod n) b. a ≡ b (mod n) and b ≡ c (mod n) implies a ≡ c (mod n)	K5(15)
9)	Differentiate between public key encryption and private key encryption. Also compare their security.	K5(15)
10)	When tunnel mode is used, a new outer IP header is constructed. For both IPv4 and IPv6, indicate the relationship of each outer IP header field and each extension header in the outer packet to the corresponding field or extension header of the inner IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values. Estimate.	K6(18)