JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2024

B.Tech-7th Semester (CSE/IT)

COURSE CODE (CREDITS): 18B1WCI734 (2) MAX. MARKS: 25

COURSE NAME: Cryptography and Network Security

COURSE INSTRUCTORS: Dr. Pankaj Dhiman MAX. TIME: 1 Hour 30 Minutes

Note: *(a) All questions are compulsory.*

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

Q.No	Question	CO	Marks
Q1	If Alice uses $P = 47$ *and* $G = 2$, with private key a=23, while Bob uses private key b =31, calculate the public keys and shared secret key, and then check if they match with another example where Alice uses a=10 and Bob uses b=15.	**[CO-3]**	5
Q2	Explain Advanced Encryption Standard (AES) and its working?	**[CO-3]**	5
Q3	In the RSA algorithm, let $p = 11$ and $q = 13$. Calculate n, $\varphi(n)$, and the public key (n, e) if you choose e =7. What is the private key d?	**[CO-4]**	5
Q4	Calculate the number of distinct hash values that can be generated by SHA-1, which produces a 160-bit hash.	**[CO-4]**	5
Q5	Consider an HMAC algorithm that combines a 256-bit key with a message of 512 bits. If the final output is a 256-bit HMAC, what is the maximum number of possible distinct HMAC values for the given message?	**[CO-4]**	5