JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATIONS-2022

B.Tech-VII Semester (CS/IT)

COURSE CODE (CREDITS): 18B1WC1734 MAX. MARKS: 25

COURSE NAME: Cryptography and Network Security

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

---

Note: *All questions are compulsory. Marks are indicated against each question in square brackets.*

Q1. List the main features of SHA-512 cryptographic hash function? What kind of compression function is used in SHA-512? **[CO-3] [3 Marks]**

Q2. Explain Message Authentication Requirements and what are the attacks related to message communication. **[CO-3] [3 Marks]**

Q3. User A & B exchange the key using Diffie Hellman algorithm. Assume á=5 q=11 XA=2 XB=3. Find YA, YB, K. **[CO-3] [4 Marks]**

Q4. Perform encryption and decryption using RSA Alg. For the following P=7; q=11; e=17; M=8. **[CO-4] [3 Marks]**

Q5. What do you mean by one way property in hash function? How Digital signature differs from authentication protocols? **[CO-4] [4 Marks]**

Q6. Let n = pq with p and q being distinct large prime numbers of roughly equal size. Suppose, we know that for any $a < n$ and gcd (a, n) = 1 we have $a^{(p+q)} = a^{(n+1)} \bmod (n)$. Prove that n can be factored in $O(n^{1/4})$ steps with a high probability. **[CO-4] [4 Marks]**

Q7. Suppose $l \geq 2n/m$, what can you say to the attacker to help him in developing an attack against the composed cipher DES? **[CO-3] [4 Marks]**