UPES

UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2021

Course: Cryptography and Network Security	**Semester:** V
Program: BTech-CS-BT	**Time** : 03 hrs.
Course Code: CSEG4001	**Max. Marks: 100**

Instruction: Attempt all questions. Internal choice is given, where ever applicable.

	Section A (5Q x 4M = 20 Marks)		
S. No.		**Marks**	**CO**
Q 1	What do you understand by Session Management in HTTP?	**5**	**CO1**
Q 2	Differentiate between Data masking and Data Erasure. Give Example	**5**	**CO1**
Q 3	Discuss two forms of Input Validation Attacks: Buffer Overflow and Cross-Site-Scripting. Give Examples.	**5**	**CO4**
Q 4	(a)Which elements in the set $\mathbf{Z}_5$={0, 1, 2, 3, 4} are not members of the set $\boldsymbol{Z}_{5*}$? (b) Result of –16 *mod* 13 = _________. (c) State either *true* or *false*: $-3 \equiv 7 \ (mod\ 5)$	**5**	**CO2**
Q 5	Explain the concept of firewalls.	**5**	**CO1**
	Section B (4Q x 10M = 40 Marks)		
Q 1	Differentiate between weak, strong, and complete collision resistant characteristics in hashing algorithm. Is Birthday Paradox helpful in providing a strong hashing algorithm? If yes, discuss briefly.	**10**	**CO2**
Q 2	Discuss Key Management approaches and their importance in real-time scenarios.	**10**	**CO3**
Q 3	What do you understand by Cookie? Why do we use cookies in web applications? List various security threats related to cookies. **OR** List various forms of Malware attacks. How can you protect your computer from malware?	**10**	**CO4**
Q 4	Draw DES Feistel network structure with neat and clean diagram	**10**	**CO2**
	Section C (2Q x 20M = 40 Marks)		
Q 1	(a) State RSA encryption and decryption as a trap-door one-way function. Explain the key generation process in RSA. (b) Perform encryption and decryption using RSA algorithm with input parameters given as p = 3, q =11, e = 7, and M = 5.	**20**	**CO3**

OR			
	(a) Explain the procedure to generate the session key in Diffie-Hellman key exchange algorithm. (b) In a Diffie-Hellman system, prime number *p* and its primitive root *g* are selected as 23 and 7 respectively. Further, Alice and Bob decide their private keys as 3 and 6, respectively. (i) Find the secret shared key. (ii) Show that 7 is a primitive root of 23.	**20**	**CO3**
Q 2	(a) List all the transformations performed in a typical AES round with a brief description of each. Which of the listed operations is skipped in the last AES round? (b) Multiply $x_3 + x_2 + x + 1$ by $x_3 + 1$. Use $x_4 + x_3 + 1$ as modulus.		**CO2**