Name: **Enrolment No:**	UPES UNIVERSITY OF TOMORROW

UPES

End Semester Examination, May 2023

Course: Cryptography and Cryptanalysis **Semester: II**
Program: M.Tech, CSE **Time: 03 hrs.**
Course Code: CSCS7005P **Max. Marks: 100**

Instructions: Attempt all the questions. Q. No. 9 and 11 have internal choices. Calculators are allowed.

SECTION A
(5Qx4M=20Marks)

S. N.		Marks	CO
Q 1	(a) Identify the 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 = _________.	**4**	**CO1**
Q 2	(a) In GF(7), the result of 5 × 4 = _________ and 6 ÷ 5 = _______. (b) Name the three common algebraic structures in Cryptography.	**4**	**CO1**
Q 3	(a) Write two properties of the Feistel block cipher structure. (b) Define confusion and diffusion in the context of block ciphers.	**4**	**CO2**
Q 4	(a) 5^{-1} mod 7 = _____. (b) The number of elements in $\boldsymbol{Z_{15}^*}$ is _____.	**4**	**CO3**
Q 5	(a) If there are ***n*** number of communicators present in a system then _______ number of symmetric keys would be required and ________ number of asymmetric keys would be needed. (b) The number of inputs to a MAC function are ___.	**4**	**CO4**

SECTION B
(4Qx10M= 40 Marks)

Q 6	Explain Cipher Feedback (CFB) mode of block cipher operation. Compare CFB and Counter (CTR) modes of block cipher operation on: (i) Parallel processing capability (ii) Preprocessing of the encryption part (iii) Error propagation (iv) Usage as a stream cipher	**10**	**CO1**

Q 7	Multiply $x^3 + x^2 + x + 1$ by $x^3 + 1$. Use $x^4 + x^3 + 1$ as modulus.	**10**	**CO2**
Q 8	List and brief the requirements of a hash function. Determine the number of rounds to break a MAC key using Brute Force attack, if the key size is 80 bits and the MAC is 32 bits long.	**10**	**CO3**
Q 9	Discuss CMAC with neat diagram.	**10**	**CO4**
	OR		
	Explain Digital Signature Standard (DSS), clearly stating the procedures of key generation, signing and verification.	**10**	**CO4**
SECTION-C (2Qx20M=40 Marks)			
Q 10	(a) Use fast exponentiation algorithm to compute 15^{89} mod 24. (b) Use Extended Euclidean algorithm to find the multiplicative inverse of 15 in $\mathbf{Z}_{26}$.	**10, 10**	**CO2**
Q 11	(a) Explain Modification Detection Code (MDC) and Message Authentication Code (MAC). Discuss the difference between the two. (b) The procedure to generate a simple hash function based on bit by bit exclusive-OR (XOR) defined as: Divide the input message into equal sized blocks of *n*-bits each. Initially set *n*-bit hash value to zero. Process each successive *n*-bit block as follows: - Rotate the current hash value to the left (circular) by one bit. - XOR the block into the hash value Find an 8-bit hash code using this algorithm if the message obtained in the Hex format is 10 2F 1B 08. Justify whether the hash code so generated is preimage resistant.	**10, 10**	**CO3**
	OR		
	(a) Define KDC. Discuss a protocol that involves KDC for the distribution of session keys within the communicating parties. (b) Explain the Diffie-Hellman key exchange procedure. (c) 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 primitive root of 23.	**6, 6, 8**	**CO3**