NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI.

B.Tech END SEMESTER EXAMINATION

CSPC 63 Principles of Cryptography

Date : 30/05/25 **Time: 3 hours**

ANSWER ALL THE QUESTIONS

MAX: 50 Marks

S NO	QUESTION	MARKS
1(a)	Distinguish between Z, Z_n, and Z_n^* citing examples.	(5)
(b)	With examples, explain how an Extended Euclidean algorithm can be used to find the multiplicative inverse of an integer .	(5)
2(a)	List the security mechanism(s) provided in each of the following cases:	
(i)	A school demands student identification and a password to let students log into the school server	(2)
(ii)	A professor refuses to send students their grades by email unless they provide student identification that were preassigned by the professor	(2)
(iii)	*A bank requires a customer's signature for a withdrawal.*	(2)
(b)	*Discuss in detail about the non-cryptanalytic attacks and the methods to prevent these attacks.*	(4)
3.(a)	*With a neat block diagram, explain how key generation is done in DES cipher.*	(5)
(b)	For the multiplicative group G =<Z_6^*,*>,	
(i)	Prove that it is an abelian group	(3)
(ii)	Find the result of 5 * 1 and 1 ÷ 5	(2)
4(a)	Alice uses Bob's RSA public key (e = 7, n = 143) to send the plaintext P = 8 encrypted as ciphertext C = 57. Show how Eve can use the chosen-ciphertext attack if she has access to Bob's	(5)

P.T.O

	computer to find the plaintext. Assume that Alice uses Bob's ElGamal public key (e1 = 2 and e2 = 8) to send two messages P = 17 and P′ = 37 using the same random integer r = 9. Eve intercepts the ciphertext and somehow, she finds the value of P = 17. Show how Eve can use a known-plaintext attack to find the value of P′.	
(b)	With diagrams, explain the working of a Diffie Hellman cryptosystem. What are the limitations of this system? How can it be rectified?	(5)
5.(a)	Using RSA scheme, let p = 809, q= 751 and d = 23. Calculate the public key e. Then	
(i)	*Sign and verify a message with* $M_1 = 100$. Let it be signature S_1	(1.5)
(ii)	*Sign and verify a message with* M2 = 50. Let it be signature *S2*	(1.5)
(iii)	*Show that if* $M = M_1 * M_2 = 5000$, then $S = S_1 * S_2$	(2)
(b)	*With appropriate diagrams, explain the computation of HMAC and state how HMAC is useful.*	(5)

****