SRN □□□□□□□□□□□□

PES University, Bengaluru
(Established under Karnataka Act No. 16 of 2013)

UE18/19CS314

DECEMBER 2021: END SEMESTER ASSESSMENT (ESA) B. TECH V SEMESTER

UE18/19CS314 – APPLIED CRYPTOGRAPHY

Time: 3 Hrs	Answer All Questions	Max Marks: 100

1	a)	Given the ciphertext and key below, find the plaintext if the Playfair cipher was used. *x* is the special character used for padding and *i* and *j* are treated as the same character.
		C = eiioqoyldc
		K = security
		What is the plaintext hidden behind?
			4

	b)	With suitable diagrams, explain the following with respect to cryptography. i) Cryptanalytic attacks ii) One-time pad encryption scheme	8 + 4
	c)	Consider the shift cipher. For all k ∈ {0,1,...,25}, Pr[K = k] = 1/26 Pr[M = a] = 0.7, Pr[M = z] = 0.3. What is Pr[C = b]?	4
2	a)	What do you mean by Pseudo random numbers? List out the different ways to generate random numbers?	4
	b)	Illustrate the Feistel cipher structure of DES in detail. List the parameters (block size, key size, and the number of rounds) for the three AES versions.	10 + 2
	c)	Define avalanche effect. How is it achieved in AES encryption technique?	4
3	a)	Show the encryption and the decryption diagram for CBC & CTR mode with a brief explanation.	6
	b)	Briefly explain the idea behind the ElGamal cryptosystem. i) What is the trapdoor in this system? ii) Assume Bob is going to send a message to Alice. How does encryption happen in this communication?	1+5
	c)	Let p = 11, q = 13 and e = 11. Find the encryption and decryption keys using RSA algorithm. Show the encryption and decryption for plaintext 7.	8
4	a)	Define zero-knowledge entity authentications. Recall any two pros and cons of zero-knowledge.	4
	b)	How will you convert an input message less than 2^{64} bits to a message digest of 160 bits in length?	12
	c)	State the Random Oracle Model and pigeonhole principle and describe its application in analyzing hash functions.	4

SRN □□□□□□□□□□□□

5	a)	Alice wants to send message M with digital signature Sig(M) to Bob. They have each other's public keys and have agreed on a specific hash function h and a signature algorithm that operates in signature mode S (equivalent to Decryption mode D) or in verification mode V (equivalent to Encryption mode E). Outline the steps that Alice must follow when signing M, and the steps that recipient Bob must follow for verifying and validating the signature Sig(M).	6
	b)	How will you provide integrity, authenticity, and non-repudiation of a document with ECDSS?	10
	c)	Write a short note on CBC-MAC.	4