SRN

PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

UE18CS314

DECEMBER 2020: END SEMESTER ASSESSMENT (ESA) B TECH 5 SEMESTER

UE18CS314 – Applied cryptography 4 Credits

Time: 3 Hrs | Answer All Questions | Max Marks: 100

1 a) If we have K = {k1,k2,k3} and M={a,b,c,d} with Pr[K = k1] =1/4, pr[K=k2]=1/2 and pr[K=k3]=1/4 for each k ∈K. Pr[M = a] = 1/4, Pr[M = b] = 3/10, Pr[M=c]=3/20 and Pr[M=d]=3/10 and encryption Matrix M is given as 8

M=

	a	b	c	d
k_1	3	4	2	1
k_2	3	1	4	2
k_3	4	3	1	2

What is the conditional probability distribution Pr[C=2 | M=d] ?

b) A person X gains access to a system under another user's account and changes the Salary field of an employee record from $20,000 to $25,000. What type of attack does X perform on data. Discuss how this can be avoided using cryptographic Algorithm. 4

c) Explain the different types of digital Steganography. 4

d) Define cryptanalysis. EVE gets access to channel and gets to know ciphertext "HLOECMTCYTGAHELWLOEORPORPY" by some other means he came to know that the cipher system used is rail fence. can eve find the plaintext? 4

2 a) The input/output in a s-box is shown in following table. derive the table for the inverse s-box 6

Input: right bits

Input: left bits		0	1
	1	01	11
	0	10	00

b) Explain DES Mangler function 8

c) Explain AES key expansion algorithm 6

3 a) Describe a man-in-the-middle attack on the Diffie–Hellman protocol. 6

SRN □□□□□□□□□□□

	b)	In an RSA cryptosystem, A uses two prime numbers p = 13 and q =17 generate her public and private keys. If A wants to send message =5 to B what is ciphertext generated by A? How B gets the original plaintext message from ciphertext.	8
	c)	Find primitive root for prime number 7.	4
	d)	Using Fermat little theorem find the value for 2^{17} mod 15.	2
4	a)	Describe the working of Fiat- Shamir protocol.	8
	b)	Explain Kerberos KDC authentication process.	8
	c)	If your message size is ℓ=49 and if authentication method used is SHA1 find padding bits.	4
5	a)	Describe elliptical curve group operation equation. If elliptical curve is defined by the equation $y^2 = x^3 + Ax + B$. Can A=-3 and B=5 be used for this curve. If A=-3 and b=5 is used then will point (25,28) satisfy the curve equation.	6
	b)	List and define DSA Domain Parameters	6
	c)	Explain with a diagram point addition and point multiplication of elliptic curve.	8