Total No. of Questions – [3]

Total No. of Printed Pages: 1

G.R. No.	

PAPER CODE	U-321-251B(ESE)

MAY 2022 (ENDSEM) EXAM

T.Y. INFORMATION TECHNOLOGY (SEMESTER - II)

COURSE NAME: INFORMATION AND NETWORK SECURITY

COURSE CODE: ITUA32181B

(PATTERN 2018)

Time: [1Hr] [Max. Marks: 30]

Instructions to candidates:

1) **Figures to the right indicate full marks.**
2) **Use of scientific calculator is allowed**
3) **Use suitable data where ever required**

Q.1	a)	Examine the working of Elgamal Encryption phases.	[4]
	b)	Differentiate between Hash Based Message Authentication Code & Cipher Block Chaining- Message Authentication Code	[6]
		OR	
	b)	Examine the Properties of digital signature and draw the block diagram for digital signature	[6]
Q2	a)	Analyze the working of X.509 authentication service	[4]
	b)	Do you think key management required? Apply the key management technique with example.	[6]
		OR	
	b)	Client machine C wants to communicate with server S. Draw flow diagram by using Kerberos protocol?	[6]
Q.3	a)	Examine the importance of alert protocol and list various warning and fatal error.	[4]
	b)	Create the SQL injection attack on server and discuss the side effects of attack.	[6]
		OR	
	b)	Create Cross site request forgery with real life example.	[6]