CLASS : M.Tech **SEMESTER : II**
BRANCH : IS **SESSION :SP /2022**

SUBJECT:IT514 Cryptography

TIME : 2 HOURS **FULL MARKS: 50**

Q1.	(a)	Explain the key principles of security? List and briefly define categories of passive and active security attacks.	[5]
Q1.	(b)	Find the multiplicative inverse of 23 in Z_{100} .	[5]
Q2.	(a)	Use the Play Fair cipher to encipher the message “the key is hidden under the doorpad” The secret key can made by filling the first and part of the second row with the word “GUIDANCE” and filling the rest of the matrix with the rest of the alphabet.	[5]
Q2.	(b)	What are the circumstances which make one prefer AES over TDES for an application?	[5]
Q3.	(a)	Does the number 561 pass the Miller Rabin test? Explain	[5]
Q3.	(b)	Illustrate RSA algorithm with suitable example. Also comment on its strength and weakness.	[5]
Q4.	(a)	Define Hash Function. Differentiate between MAC and Hash Function.	[5]
Q4.	(b)	Why do you carry out the digital signature on the hash value and not on plaintext itself?	[5]
Q5.	(a)	Write a note on Zero Knowledge Protocol in cryptography.	[5]
Q5.	(b)	Describe Rabin Cryptosystem. How it is different than RSA?	[5]

04/05/2022 E