Roll No: | | | | | | | | | | | | | |

B. TECH
(SEM VII) THEORY EXAMINATION 2020-21
CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours ***Total Marks: 70***

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. 2 x 7 = 14

		Marks	CO
a.	What do you mean Brute Force Attack?	2	CO1
b.	Define CIA?	2	CO1
c.	Define the concept of confusion and Diffusion?	2	CO2
d.	Find all the primitive roots of 11.	2	CO2
e.	Find gcd (24140, 16762) using Euclid's algorithm?	2	CO1
f.	List out the services provided by the Digital Signature.	2	CO4
g.	What are the five principal services provided by PGP?	2	CO5

SECTION B

2. Attempt any *three* of the following: 7 x 3 = 21

Qno.	Question	Marks	CO
a.	Explain the Security Attacks with Example	7	CO1
b.	Explain the Structure of DES Algorithm and define the role of fiestal cipher in DES in detail.	7	CO2
c.	Explain symmetric and Asymmetric Cryptography with the help of diagrammatic representation. And how-to symmetric cryptography is different from asymmetric Cryptography.	7	CO3
d.	State Chinese remainder theorem and find X for the given set of congruent equations using CRT: X=2(mod3), X=3(mod5), X=2(mod7)	7	CO1
e.	Describe RSA algorithm ,Suppose alice and bob uses a public key cryptosystem using RSA, the two prime no is P=13 and q=17 and e=7 the find out the decryption key d and Perform the encryption and decryption of the message "CRYPTOGRAPHY" Using 00 to 25 for letters A to Z.	7	CO2

SECTION C

3. Attempt any *one* part of the following: 7 x 1 = 7

a.	Explain Block modes of operation and also explain the Electronic Code Book (ECB) mode is not a secured mode of encryption and highlight the problems with this mode.	7	CO2
b.	Give a real-life example where both confidentiality and integrity are needed. Explain why encryption alone does not provide integrity of information.	7	CO1

4. Attempt any *one* part of the following: 7 x 1 = 7

a.	Compare Substitution and Transposition techniques.	7	CO1
b.	Encrypt the following using play fair cipher using the keyword: MONARCHY. "SWARAJ IS MY BIRTH RIGHT". Use X as blank space.	7	CO1

5. Attempt any *one* part of the following: 7 x 1 = 7

a.	Define Primality Test and also explain Miller Rabin Algorithm using base 2 to test whether the number 341 is composite or not?	7	CO2
b.	Explain AES algorithm What is the difference between the AES decryption algorithm and the DES algorithm	7	CO2

6. Attempt any *one* part of the following: 7 x 1 = 7

a.	Explain the Kerberos protocol for key distribution? Explain the functionality of each step.	7	CO4
b.	How does worms and viruses compare? Describe the components of the virus and how does it protect from anti-virus software's?	7	CO4

7. Attempt any *one* part of the following: 7 x 1 = 7

a.	What do you mean by SHA1 algorithm What basic arithmetical and logical functions are used in SHA?	7	CO3
b	Explain in detail about S/MIME and what is difference between S/MIME and PGP.	7	CO5