

**PRAGATI ENGINEERING COLLEGE :SURAMPALEM**  
**(AUTONOMOUS)**  
**III B.Tech II Semester Regular/Supplementary Examinations, April-2024**  
**CRYPTOGRAPHY AND NETWORK SECURITY**  
**(Common to CSE and IT)**

Time: 3hours

Max.Marks:70M

Answer ONE Question from each Unit  
All Questions Carry Equal Marks

Q.No.		Questions	BTL	CO	Marks
<b>UNIT-I</b>					
1.	a)	What are the Security Services? Explain them.	K2	CO1	7M
	b)	Explain about various Security Goals.	K2	CO1	7M
<b>OR</b>					
2.	a)	Determine the security services required to counter various types of Active and Passive attacks.	K2	CO1	7M
	b)	Explain extended Euclidean algorithm with an example.	K2	CO1	7M
<b>UNIT-II</b>					
3.	a)	Difference between a block cipher and a stream cipher	K2	CO2	7M
	b)	Explain about Substitution box, Permutation in DES.	K2	CO2	7M
<b>OR</b>					
4.	a)	Explain any one substitution techniques with suitable examples.	K1	CO2	7M
	b)	Explain about single round of AES.	K2	CO2	7M
<b>UNIT-III</b>					
5.	a)	Write with a neat sketch of RSA algorithm.	K2	CO3	7M
	b)	What is the use of Fermat's theorem?	K2	CO3	7M
<b>OR</b>					
6.	a)	How Asymmetric key cryptography works, mention principles And its applications	K2	CO3	7M
	b)	Explain about Diffie-Hellman algorithm.	K2	CO3	7M
<b>UNIT-IV</b>					
7.	a)	Explain Message digest Algorithm (MD5) in detail.	K2	CO4	7M
	b)	Give the structure of HMAC. Explain the applications of HMAC.	K2	CO4	7M
<b>OR</b>					
8.	a)	What are the Approaches of Message Authentication? Explain them.	K2	CO4	7M
	b)	What are the requirements of cryptographic hash functions?	K2	CO4	7M
<b>UNIT-V</b>					
9.	a)	Explain Pretty Good Privacy (PGP) in detail.	K2	CO5	7M
	b)	Write short notes on S/MIME.	K2	CO5	7M
<b>OR</b>					
10.	a)	Draw and explain fields in AH header.	K2	CO5	7M
	b)	Explain in detail the operation of Secure Socket Layer in detail.	K2	CO5	7M