Krantiguru Shyamji Krishna Verma Kachchh University, Bhuj
Master of Science (Computer Applications & Information Technology)
Semester: VIII

Paper Code: CCCS832		**Total Credit :** 4
Title of Paper: Cryptography		**Total Marks :** 70 **Time :** 3 Hrs
Unit	**Description**	**Weighting**
I	**Introduction** Security Trends, OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, History and Overview of Cryptology	**20%**
II	**Symmetric Ciphers** Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Rotor Machines / Enigma, Steganography Block Ciphers: Principles, Data Encryption Standard/ 3DES, DES Operation, DES Strength, Block Cipher Design Principles	**20%**
III	**Asymmetric Ciphers** Prime Numbers, Principles of Public Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange, Pseudorandom Number Generation, Cryptographic Hash Functions, Secure Hash Algorithm, Message Authentication Codes, Digital Signatures	**20%**
IV	**Network and Internet Security** Key Distribution, X.509 Certificates, Public Key Infrastructure, Web Security Issues, Secure Sockets Layer (SSL), Transport Layer Security (TLS), HTTPS, Secure Shell (SSH), Wireless Network Security Overview, Email Security: PGP, S/MIME, DKIM.	**20%**
V	**Scams and Cyber Laws** DoS and DDoS attacks, CAPTCHA, Spam, Phishing, Ponzi Schemes, Indian IT Act 2000 with Subsequent Amendments.	**20%**
Basic Text & Reference Books :-		
1.	Cryptography and Network Security, William Stallings, Pearson	

Krantiguru Shyamji Krishna Verma Kachchh University, Bhuj
Master of Science (Computer Applications & Information Technology)
Semester: VIII

Paper Code: CCCS832			**Total Credit :** 4 **Total Marks :** 70 **Time :** 3 Hrs
Title of Paper: Cryptography			
Unit	**Description**		**Total Marks**
I	Q.1 (A) Answer the Following. (Definitions, Blanks, Full Forms, True/False, Match the Following)	06	14
	Q.1 (B) Medium / Long Questions. (With Internal Option)	08	
II	Q.2 (A) Answer the Following. (Definitions, Blanks, Full Forms, True/False, Match the Following)	06	14
	Q.2 (B) Medium / Long Questions. (With Internal Option)	08	
III	Q.3 (A) Short / Medium Questions (With Internal Option)	06	14
	Q.3 (B) Medium / Long Questions. (With Internal Option)	08	
IV	Q.4 (A) Short / Medium Questions (With Internal Option)	06	14
	Q.4 (B) Medium / Long Questions. (With Internal Option)	08	
V	Q.5 (A) Short / Medium Questions (With Internal Option)	06	14
	Q.5 (B) Medium / Long Questions. (With Internal Option)	08	