<table>
<tr><th rowspan="2">Course Code</th><th rowspan="2">Course Name</th><th colspan="3">Teaching Scheme (Hrs/week)</th><th colspan="4">Credits Assigned</th></tr>
<tr><th>L</th><th>T</th><th>P</th><th>L</th><th>T</th><th>P</th><th>Total</th></tr>
<tr><td rowspan="4"><b>MCAE35A</b></td><td rowspan="4"><b>Network Security</b></td><td><b>3</b></td><td><b>-</b></td><td><b>--</b></td><td><b>3</b></td><td><b>-</b></td><td><b>--</b></td><td><b>3</b></td></tr>
<tr><td colspan="7"><b>Examination Scheme</b></td></tr>
<tr><td colspan="2"><b>ISE</b></td><td colspan="2"><b>MSE</b></td><td colspan="3"><b>ESE</b></td></tr>
<tr><td colspan="2"><b>10</b></td><td colspan="2"><b>30</b></td><td colspan="3"><b>100 (60% Weightage)</b></td></tr>
</table>

Pre-requisite Course Codes	Computer Networks	
Course Outcomes	**CO1**	To understand basics of security and Cryptography
	CO2	To analyze secret and public key cryptography
	CO3	To analyze hash function and message digest
	CO4	To explain authentication and its standards
	CO5	To analyze internet security protocols.
	CO6	To understand IDS, VPN and firewall.

Module No.	**Unit No.**	**Topics**	**Ref.**	**Hrs.**
1		**Introduction**	**2,5**	**3**
	1.1	Types of attacks		
	1.2	Principles of security		
	1.3	Need for security		
	1.4	3 D’s for security		
	1.5	Security Approaches		
2		**Basic of Cryptography**	**1,2**	**4**
	2.1	Introduction		
	2.2	Plain text and Cipher text		
	2.3	Substitution Cipher (Ceaser , playfair cipher)		
	2.4	Transposition Cipher (Columnar transposition, Vernam and Book Cipher)		
	2.5	Encryption and Decryption		
	2.6	Symmetric and Asymmetric Cryptography		
	2.7	Possible types of attacks		
3		**Secret key Cryptography**	**2,4**	**7**
	3.1	DES		
	3.2	IDEA		
	3.3	AES		
	3.4	Blowfish		
	3.5	Schemes to encrypt large messages: ECB, CBC, OFB, CFB, Multiplication Encryption DES.		
4		**Public key Cryptography**	**2,1,4**	**5**
	4.1	RSA		
	4.2	Diffie-Hellmen Key Exchange		
	4.3	Digital Signature		
5		**Hash Functions and Message Digest**	**2,5**	**6**
	5.1	MD2		

	5.2	MD4 &MD5 Comparison		
	5.3	SHA		
	5.4	HMAC		
6		**Authentication and Standards**	**1,2,4**	**6**
	6.1	Types of Authentication (Password, address, cryptographic, smart cards, biometrics, mutual)		
	6.2	KDC working and Multi domain KDC		
	6.3	KerberosV5: names, delegation of rights, ticket lifetime , key version, kerberosV4 vs Kerberos V5		
	6.4	PKI: introduction, PKI trust models, PKI & X.509		
7		**Internet Security Protocols**	**5,1**	**6**
	7.1	SSL		
	7.2	SET		
	7.3	Email Security- PGP, S/MIME		
	7.4	IPSec- AH, ESP		
8		**VPN, IDS and Firewall**	**5,2**	**5**
	8.1	IDS-types and detection models, IDS features, Honeypot		
	8.2	Firewall-Introduction, Types		
	8.3	Virtual Private Network: Introduction, VPN Protocols		
			Total	**42**

References:

[1] William Stallings, “Cryptography and Network Security: Principles and Practice”, 5th edition, Pearson.

[2] Atul Kahate , “Cryptography and Network Security “, 3rd Edition, Tata mc grawhill.

[3] Bernard Menezes , “Network Security and Cryptography”, 2nd edition , Cengage Learning.

[4] Kauffman , “Network Security”, 2nd edition, pearson .

[5] Eric Cole ,“Network Security Bible”, 2nd Edition, Wiley.

[6] Behrouz A. Forouzan , “Cryptography and Network Security”, TMH

[7] Charles P. Pfleeger , “Security in Computing”, Pearson Education.

[8] Matt Bishop, “Computer Security Art and Science” , Addison-Wesley.