	from the academic SEMESTER -		
Course Code	18CS744	CIE Marks	40
Number of Contact Hours/Week	3:0:0	SEE Marks	60
Total Number of Contact Hours	40	Exam Hours	03
	CREDITS -		
Course Learning Objectives: This cou		enable students to:	
 Define cryptography and its print 			
 Explain Cryptography algorithm 			
Illustrate Public and Private key			
 Explain Key management, distri- 		ation	
Explain authentication protocols	s		
• Tell about IPSec			
Module – 1			Contac
Classical Encryption Techniques Sym	metric Cinhar Mad	al Countages has Count	Hours
and Brute-Force Attack, Substitution T	echniques Caesar (Ci, Cryptograpny, Cryptai	nalysis 08
Playfair Cipher, Hill Cipher, Polyalphab	etic Cipher, One Ti	ne Pad. Block Ciphers at	nd the
data encryption standard: Traditional	block Cipher struc	ture, stream Ciphers and	block
Ciphers, Motivation for the feistel Ciphers	er structure, the feis	tel Cipher, The data encr	votion
standard, DES encryption, DES decrypt	ion, A DES example	e, results, the avalanche	effect
the strength of DES, the use of 56-Bi	t Keys, the nature	of the DES algorithm, t	timing
attacks, Block cipher design principles	c number of roun		
cchadula algorithm	s, number of found	ds, design of function F	F, key
schedule algorithm	s, number of found	ds, design of function F	, key
rextbook 1: Ch. 2.1,2.2, Ch. 3	s, number of found	ds, design of function F	, key
Schedule algorithm Textbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2	s, number of four	ds, design of function F	, key
Textbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2			
Restriction of the Restriction o	Principles of public-	key cryptosystems. Publi	ic-key 08
Public-Key Cryptography and RSA: I	Principles of public- key cryptosystems	key cryptosystems. Publi	ic-key 08
ryptosystems. Applications for public-ryptosystems. public-key cryptography and RSA: I	Principles of public- key cryptosystems The RSA algorith	key cryptosystems. Publi	ic-key 08
Public-Key Cryptography and RSA: I cryptosystems. Applications for public-ryptosystems. public-key cryptanalysis. omputational aspects, the security of RS	Principles of public- key cryptosystems The RSA algorithm	key cryptosystems. Publi , requirements for publi n, desription of the algor	ic-key 08
Public-Key Cryptography and RSA: I cryptosystems. Applications for public-ryptosystems. Applications for public-ryptosystems. Applications for public-ryptosystems. Applications for public-ryptosystems. Displayed the security of RS of the Public-Key Cryptosystems: Displayed the public-Key Cryptosystems the public-Key Cryptosys	Principles of public- key cryptosystems The RSA algorithm A.	key cryptosystems. Publi , requirements for publi n, desription of the algor xchange. The algorithm	ic-key 08
Public-Key Cryptography and RSA: I cryptosystems. Applications for public-ryptosystems. public-key cryptanalysis. omputational aspects, the security of RS other Public-Key Cryptosystems: Dixchange protocols, man in the middle att	Principles of public- key cryptosystems The RSA algorithm A.	key cryptosystems. Publi , requirements for publi n, desription of the algor xchange. The algorithm	ic-key 08
Public-Key Cryptography and RSA: I cryptosystems. Applications for public-ryptosystems. Public-key cryptosystems. Other Public-Key Cryptosystems: Dixchange protocols, man in the middle atterthook 1: Ch. 9, Ch. 10.1,10.2	Principles of public- key cryptosystems The RSA algorithm A.	key cryptosystems. Publi , requirements for publi n, desription of the algor xchange. The algorithm	ic-key 08
Public-Key Cryptography and RSA: I ryptosystems. Applications for public-ryptosystems. Applications for public-ryptosystems. Diversity of RSD of the Public-Key Cryptosystems: Diversity of RSD of t	Principles of public- key cryptosystems The RSA algorithm A.	key cryptosystems. Publi , requirements for publi n, desription of the algor xchange. The algorithm	ic-key 08
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I cryptosystems. Applications for publicaryptosystems. public-key cryptanalysis. omputational aspects, the security of RSD ther Public-Key Cryptosystems: Dixchange protocols, man in the middle attention of the cryptosystems of the crypto	Principles of public- key cryptosystems The RSA algorithm A. Iffie-hellman key etack, Elgamal Crypto	key cryptosystems. Public, requirements for public, not the algorate and the second se	ic-key 08 ic-key rithm,
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I ryptosystems. Applications for public ryptosystems. public-key cryptanalysis. omputational aspects, the security of RS Other Public-Key Cryptosystems: Dixchange protocols, man in the middle att rextbook 1: Ch. 9, Ch. 10.1,10.2 RBT: L1, L2 Iodule – 3 Iliptic curve arithmetic, abelian groups,	Principles of public- key cryptosystems The RSA algorithm A. offie-hellman key etack, Elgamal Crypto elliptic curves ove	key cryptosystems. Publi, requirements for publin, description of the algorithm, xchange, The algorithm, graphic systems	ic-key 08 ic-key rithm, , key
Public-Key Cryptography and RSA: I cryptosystems. Applications for public-ryptosystems. Applications for public-ryptosystems. public-key cryptanalysis. omputational aspects, the security of RSD ther Public-Key Cryptosystems: Dixchange protocols, man in the middle attractional aspects. The man in the middle attractional aspects, as a man in the middle attractional aspects. The man in the middle attractional aspects are man in the middle attractional aspects. The man in the middle attractional aspects are man in the middle attractional aspects. The man in the middle attractional aspects are man in the middle attractional aspects are man in the middle attractional aspects. The man in the middle attractional aspects are man in the middle attractional aspects are man in the middle attractional aspects. The man in the middle attractional aspects are man in the middle attractional aspects are man in the middle attractional aspects. The man in the middle attractional aspects are man in the middle attractional aspects are man in the middle attractional aspects. The man in the middle attractional aspects are man in the middle attractional aspects are man in the middle attractional aspects. The man in the middle attractional aspects are man in the middl	Principles of public- key cryptosystems The RSA algorithm A. Iffie-hellman key etack, Elgamal Crypto elliptic curves ove	key cryptosystems. Public, requirements for public, requirements for public, description of the algorithm, systems. Treal numbers, elliptic copply, Analog of Diffie-hel	ic-key 08 ic-key rithm, key 08
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I ryptosystems. Applications for public-ryptosystems. public-key cryptanalysis. omputational aspects, the security of RSD ther Public-Key Cryptosystems: Dixchange protocols, man in the middle attentional aspects. The man in the middle attention of the computation o	Principles of public- key cryptosystems The RSA algorithman A. Iffie-hellman key etack, Elgamal Crypto elliptic curves ove ptic curve cryptogra decryption, security	key cryptosystems. Public, requirements for public, requirements for public, requirements for public m, description of the algorithm, exchange, The algorithm, agraphic systems real numbers, elliptic cophy, Analog of Diffie-hele of Elliptic curve cryptogra	urves 08
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I cryptosystems. Applications for public-tryptosystems. public-key cryptanalysis. omputational aspects, the security of RSD ther Public-Key Cryptosystems: Dixchange protocols, man in the middle attractional aspects. Cryptosystems: Dixchange protocols, man in the middle attractional aspects. L1, L2 Indule – 3 Iliptic curve arithmetic, abelian groups, wer Zp, elliptic curves overGF(2m), Elliptic curve encryption/desendorandom number generation based of the control of the control of the curve and the curve encryption of the curve and the curve encryption of the curve encryption of the curve and the curve encryption of the curve encryp	Principles of publication-less of publication-	key cryptosystems. Public, requirements for public, requirements for public, requirements for public m, description of the algorithm, exchange, The algorithm, agraphic systems real numbers, elliptic cophy, Analog of Diffie-help of Elliptic curve cryptographer, PRNG based on RSA	urves 08 lman aphy, A.
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I cryptosystems. Applications for publicaryptosystems. public-key cryptanalysis. computational aspects, the security of RSD ther Public-Key Cryptosystems: Diexchange protocols, man in the middle attractional aspects. Cryptosystems: Diexchange protocols, man in the middle attractional aspects. Cryptosystems: Diexchange protocols, man in the middle attractional aspects. Cryptosystems: Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attractional cryption of the cryptosystems. Diexchange protocols, man in the middle attraction cryption of the cryptosystems. Diexchange protocols, man in the middle attraction cryption of the cryptosystems. Diexchange protocols, man in the middle attraction cryption	Principles of public- key cryptosystems The RSA algorithm A. Iffie-hellman key etack, Elgamal Crypto elliptic curves ove ptic curve cryptogra decryption, security on an asymmetric cip	key cryptosystems. Public, requirements for public, requirements for public, requirements for public, requirements for public and the algorithm, agraphic systems. The real numbers, elliptic couphy, Analog of Diffie-help of Elliptic curve cryptographer, PRNG based on RSA distribution using Symmetric Symmetric Course Symmetric Symmetric Course	urves 08 lman aphy, A.
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I ryptosystems. Applications for publicaryptosystems. public-key cryptanalysis. omputational aspects, the security of RSD ther Public-Key Cryptosystems: Dixchange protocols, man in the middle attractional aspects. Ch. 9, Ch. 10.1,10.2 RBT: L1, L2 Iodule – 3 Illiptic curve arithmetic, abelian groups, wer Zp, elliptic curves overGF(2m), Ellipty exchange, Elliptic curve encryption/diseudorandom number generation based of the Management and Distribution: acryption, A key distribution scenario,	Principles of public- key cryptosystems The RSA algorithm A. Iffie-hellman key estack, Elgamal Crypto elliptic curves ove ptic curve cryptogra decryption, security on an asymmetric cip Symmetric key deliverarchical key co	key cryptosystems. Public, requirements for public, requirements for public, requirements for public, requirements for public and the algorithm, which is the systems for real numbers, elliptic curphy, Analog of Diffie-help of Elliptic curve cryptographer, PRNG based on RSA distribution using Symmontrol, session key lifeting	urves O8 lman aphy, A. netric
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I ryptosystems. Applications for publicaryptosystems. public-key cryptanalysis. computational aspects, the security of RSD ther Public-Key Cryptosystems: Dixchange protocols, man in the middle attractional aspects. Ch. 9, Ch. 10.1,10.2 RBT: L1, L2 Iodule – 3 Illiptic curve arithmetic, abelian groups, wer Zp, elliptic curves overGF(2m), Elliptic curve arithmetic, abelian groups, wer Zp, elliptic curves overGF(2m), Elliptic curve and Distribution: acception, A key distribution scenario, ansparent key control scheme, Dece	Principles of public- key cryptosystems The RSA algorithm A. Iffie-hellman key estack, Elgamal Crypto elliptic curves over ptic curve cryptogra lecryption, security on an asymmetric cip Symmetric key de Hierarchical key contralized key con	key cryptosystems. Public, requirements for public, not description of the algorithm, description of the algorithm, agraphic systems Treal numbers, elliptic comply, Analog of Diffie-help of Elliptic curve cryptographer, PRNG based on RSA distribution using Symmontrol, session key lifeting trol, controlling key us	urves land aphy, A. hetric ne, a sage
rextbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2 Module – 2 Public-Key Cryptography and RSA: I ryptosystems. Applications for publicaryptosystems. public-key cryptanalysis. omputational aspects, the security of RSD ther Public-Key Cryptosystems: Dixchange protocols, man in the middle attractional aspects. Ch. 9, Ch. 10.1,10.2 RBT: L1, L2 Iodule – 3 Illiptic curve arithmetic, abelian groups, wer Zp, elliptic curves overGF(2m), Ellipty exchange, Elliptic curve encryption/diseudorandom number generation based of the Management and Distribution: acryption, A key distribution scenario,	Principles of public- key cryptosystems The RSA algorithm A. Iffie-hellman key estack, Elgamal Crypto elliptic curves over ptic curve cryptogra decryption, security on an asymmetric cip Symmetric key de Hierarchical key contralized key contralized key contestric encryption, si	key cryptosystems. Public, requirements for public, not description of the algorithm, description of the algorithm, seraphic systems. Treal numbers, elliptic comply, Analog of Diffie-help of Elliptic curve cryptographer, PRNG based on RSA distribution using Symmontrol, session key lifeting trol, controlling key usimple secret key distribution.	urves O8 lman aphy, A. netric ne, a sage, tion

authority, public keys certificates. Textbook 1: Ch. 10.3-10.5, Ch.14.1 to 14.3 RBT: L1, L2 Module - 4 X-509 certificates. Certificates, X-509 version 3, public key infrastructure .User Authentication: Remote user Authentication principles, Mutual Authentication, one wayAuthentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one way Authentication, Kerberos, Motivation, Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one way Authentication. Electronic Mail Security: Pretty good privacy, notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing, enhanced security services, Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow. Textbook 1: Ch. 14.4, Ch. 15.1 to 15.4, Ch.19 **RBT: L1, L2** Module - 5 IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing 08 applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service Transport and tunnel modes, combining security associations, authentication plus confidentiality, basic combinations of security associations, internet key exchange, key determinations protocol, header and payload formats, cryptographic suits. Textbook 1: Ch. 20.1 to 20.3 RBT: L1, L2 Course outcomes: The students should be able to: Define cryptography and its principles Explain Cryptography algorithms Illustrate Public and Private key cryptography Explain Key management, distribution and ceritification Explain authentication protocols Tell about IPSec Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module. Text Books: 1. William Stallings: Cryptography and Network Security, Pearson 6th edition. Reference Books: 1. V K Pachghare: Cryptography and Information Security, PHI 2nd Edition.

> Dept. Of Computer Science & Engineering Alva's Institute of Engg. & Technology Mijar, MOODBIDRI - 574 225