Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR1E1: Data Security	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:
To impart the knowledge of encryption and decryption techniques and their applications in managing the security of data.

COURSE CONTENT

Unit I : Foundation
Security Taxonomy, Domain of information security, security goals, security approaches, principles of security, security attacks, threats, vulnerabilities, malicious software's, virus, worms, Trojan, spy wares, Applets/Active X, cookies. Security services, mechanisms and security models. Types of attacks, packet sniffing, packet spoofing, IP sniffing, IP spoofing, DNS spoofing attack.

Unit II : Classical Cryptographic Techniques
Cryptography terminologies, classical cryptography: substitution techniques, transposition techniques, playfair cipher, Hill cipher. Mathematics of cryptography: Integer arithmetic, modular arithmetic, Elucid theorem, Concept of symmetric and asymmetric key cryptography, stenography, digital watermarking, key range and size, possible types of attacks. Stream ciphers and Block cipher. Algorithm type and modes. Key distribution, Deffie Hellman key exchange, Man in the middle attack.

Unit III : Symmetric Key Algorithms
Computer based symmetric key cryptographic algorithms: Data Encryption Standard (DES), Double DES, meet in the middle attack, Triple DES, International Data Encryption Algorithm (IDEA), RC5, Blowfish, Advance Encryption Standard (AES).

Unit IV : Asymmetric Key Algorithms
Random number generation, Prime numbers. Fermat's and Euler's theorem. Principles of public key crypto systems. Computer based asymmetric key cryptographic algorithms: RSA algorithm. Principles of public key cryptosystems, symmetric and asymmetric key cryptography together. Concept of Digital Envelope, Digital signatures, message digests and its requirements.

Unit V : Public Key Crptosystems
MD5 Message Digest Algorithm, Message authentic codes, Hash functions, Secure Hash Algorithms, Hash based message authentic code. Elliptical Curve Cryptography (ECC). Problems with the public key exchange.

Text and Reference books:

[1] Douglas R. Stinson;"Cryptography Theory and Practice"; Chapman & Hall/CRC
[2] Williams Stallings; "Cryptography & Network Security"; Pearson Education.
[3] Mathew Bishop; Introduction to computer Security; Addison-Wisley
[4] Atul Kahate; "Cryptography and Network Security"; Tata McGraw-Hill.