Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP3G2: Applied Cryptography	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**0**	**3**	**1**	**0**	**4**

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

COURSE CONTENT

Unit I : Modular Arithmetic and Multiplicative Group
Modular Arithmetic for advanced cryptography, Multiplicative group of integers ,, order of an element in , generator of , extended Euclidean algorithm, Pohlig-Hellman and Pollard-Rho algorithm for computing DLP, Integer factorization problems, Pollard-Rho factoring algorithm.

Unit II : Tools for Symmetric key & Public key Cryptography
Shannon ciphers and perfect security, computational ciphers and semantic security, efficient adversaries and attack games, trapdoor function schemes, trapdoor function pair schemes, ElGamal cryptographic system, ElGamal digital signatures, fun applications.

.

Unit III : Block Ciphers and Their Attacks
Polynomial arithmetic, finite field GF(2^n), constructing block cipher in practice, sophisticated attacks on block ciphers, case study block cipher AES: AES structure, AES transformation functions, AES key expansions, AES Implementation, fun applications.

Unit IV : Cryptanalysis, IDS and Attacks
Intrusion detection system (IDS), cross site scripting attacks, SQL injection attacks, fault injection attacks, side channel attacks, algorithmic attacks.

Unit V : Asymmetric Key Cryptosystems
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.