AMITY UNIVERSITY
UTTAR PRADESH

Course Title: ADVANCED INFORMATION SECURITY **Credit Units:**

L	T	P/S	SW/FW	TOTAL CREDIT UNITS
3	1	-	-	4

Course Level: PG
Course Code: IT704

Course Objectives:

- Gain Expertise in different techniques used for information security.
- Learn different algorithms used for encryption.
- Identify different protocols used for network security
- To introduce the standards used in information security.

Prerequisites: Student should have learned all the concepts of Computer Networks. They should have the clear idea of layer Structure of Computer Network.

Course Contents/Syllabus:

	Weightage (%)
Module I Cryptography and cryptanalysis, Classical encryption techniques substitution ciphers and transposition ciphers, cryptographic algorithms and protocols, authentication and signature protocols, symmetric and public-key encryption, number theory and algebra, computational complexity, Pseudo random bit generators.	**20**
Module II Stream & Block Ciphers, Shannon's theory of confusion and diffusion, fiestal structure, Probabilistic encryption, Data Encryption Standard, International Data Encryption Algorithm, Advanced Encryption Standard, Hash and MAC algorithms, Blowfish, differential cryptanalysis, block cipher modes of operations, Cast-128, Triple DES, RC4; Fluhrer, Mantin and Shamir attack.	**25**
Module III Principals of public key crypto systems, RSA algorithm, security of RSA, Diffie-Hellman, Elliptic Curve cryptography, Digital signatures and authentication, DSS approach, algorithm, Public key distribution, X.509 Certificates, Public key Infrastructure.	**20**
Module IV Message authentication, Hash functions, SHA, MD5, MD6, Generator, Strong password protocols, HMAC, Rabin, ElGamal, Goldwasser-Micali, Blum-Goldwasser cryptosystems, birthday attacks, Zero knowledge interactive protocols.	**20**

Module V	15
Trusted intermediaries, Security handshake pitfalls, IPsec, SSL/TLS, PGP, PEM, S/MIME, Web security requirements, Kerberos, electronic payment protocols.	

Student Learning Outcomes:

- Student will able to recognize the basics of Security Constraints, Encryption and Decryption etc.
- Student will be able to distinguish between Computer Network and Computer Security issues.
- Student will be able to modify the encryption/decryption Algorithm in their Research work.

Pedagogy for Course Delivery:

The course would be covered under theory. In addition to assigning project–based learning, early exposure to hands-on design to enhance the motivation among the students. It incorporates designing of problems, analysis of solutions submitted by the students groups and how learning objectives were achieved. Continuous evaluation of the students would be covered under quiz, viva etc.

Assessment/ Examination Scheme:

Theory L/T (%)	Lab/Practical/Studio (%)	Total (%)
100%	NA	100%

Theory Assessment (L&T):

Continuous Assessment/Internal Assessment					End Term Examination
Components (Drop down)	Mid-Term Exam	Assignment	Viva	Attendance	
Weightage (%)	10%	8%	7%	5%	70%

Text Reading:

- William Stallings, "Cryptography and Network Security: Principles and Standards", Prentice Hall India, 3rd Edition, 2003.
- Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security: Private Communication in a public world", Prentice Hall India, 2nd Edition, 2002.
- Charles P. Pleeger, "Security in Computing", Pearson Education Asia, 5th Edition, 2001.
- William Stallings, "Network Security Essentials: Applications and standards", Person Education Asia, 2000.
- Jorg Roth, Complexity Theory and Cryptology – An introduction to cryptocomplexity, Springer, 2005.
- C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a public World, 2/e, Prentice Hall, 2002.
- Kurose J. F. & Ross K. W., Computer Networking: A Top-Down Approach Featuring the Internet, Pearson Education Asia, 3/e, 2005.