National Institute of Technology Meghalaya

An Institute of National Importance

CURRICULUM

Programme	**Master of Computer Applications**	Year of Regulation	**2024-25**
Department	**Computer Science and Engineering**	Semester	**V**

Course Code	Course Name	Pre-Requisite	Credit Structure				Marks Distribution			
			L	T	P	C	INT	MID	END	Total
CA677	**Cryptography and Network security**		**3**	**0**	**0**	**3**	**50**	**50**	**100**	**200**

			CO's	**Statement**	**Bloom's Taxonomy**
Course Objectives	**To develop the student's ability to understand the concept of security goals in various applications.**	Course Outcomes	CA677.1	**Able to understand about security goals, background of cryptographic mathematics and identification of its application**	**Understand**
	To provide the students with some fundamental cryptographic mathematics used in various symmetric and asymmetric key cryptography.		CA677.2	**Able to acquire knowledge about the background mathematics of symmetric key cryptography and understand, analyse and implement – the symmetric key algorithm.**	**Analyse**
	To develop the student's ability to analyse the cryptographic algorithms.		CA677.3	**Able to acquire knowledge about the background mathematics of asymmetric key cryptography and understand and analyse – asymmetric key encryption algorithms, digital signatures**	**Analyse**
	To familiarize the student the need of security in computer networks.		CA677.4	**Able to understand and analyse the concept of message integrity and the algorithms for checking the integrity of data.**	**Analyse**
			CA677.5	**Able to understand and analyse the existing cryptosystem used in networking**	**Analyse**

COs	Mapping with Program Outcomes (POs)												Mapping with PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CA677.1	**3**	**3**											**2**		**3**
CA677.2	**3**	**3**				**1**			**2**				**3**	**3**	**2**
CA677.3	**3**	**3**	**3**	**1**	**2**	**1**			**2**				**3**	**3**	**2**
CA677.4	**2**	**3**	**3**	**1**	**2**	**2**	**3**		**2**			**1**	**3**	**2**	**2**
CA677.5	**2**	**3**	**3**	**1**	**2**	**2**	**3**		**2**			**1**	**3**	**3**	**3**
CA677	**2.6**	**3**	**1.8**	**0.6**	**1.2**	**1.2**	**1.2**		**1.6**			**0.4**	**2.8**	**2.2**	**2.4**

SYLLABUS

No.	Content	Hours	COs
I	Introduction Security goals, cryptographic attacks. Mathematics of cryptography: modular arithmetic, Euclidean and extended Euclidean algorithm. Traditional symmetric key ciphers; Monolithic ciphers: addition and multiplication ciphers, Polyalphabetic ciphers: Vigenere's ciphers, Hill ciphers, playfair ciphers.	**08**	**CA677.1**
II	Symmetric key cryptography Mathematics of symmetric key cryptography: Groups, Rings, Fields, GF, Inverse of a number and polynomial using extended Euclidean algorithm. Modern Block ciphers and its components, DES, AES	**08**	**CA677.2**
III	Asymmetric key cryptography Mathematics of asymmetric key cryptography: Euler's Phi-Function, Fermat's Little Theorem, Euler's theorem, Chinese remainder theorem. Diffie-Hellman, Digital signature: RSA, Elgamal, Entity authentication	**08**	**CA677.3**
IV	Message Integrity and authentication: MAC, HMAC. Cryptographic Hash Function: Merkle-Damgard, MD5, SHA512.	**08**	**CA677.4**
V	Network Security Key Management, PGP, IPSec, SSL, Firewalls, Intrusion Detection, Password management, Virus. Virtual Private Network.	**10**	**CA677.5**
	Total Hours	**42**	

Essential Readings

1. Behrouz A. Forouzan, "Cryptography and Network Security", McGraw-Hill publication, 2nd Edition, 2010.
2. William Stallings ,"Cryptography and Network Security: Principles and Standards", Prentice Hall India, 7th Edition, 2017.
3. John R. Vacca, "Computer and Information Security Handbook", Morgan Kaufmann Publishers, 3rd Edition, 2017.

Supplementary Readings

1. Richard H. Baker, Network Security, McGraw Hill International 3rd Edition,1996.
2. B. Schneier, Applied Cryptography, John Wiley New York, 2nd Edition, 1996.
3. C. Kaufman et. al, Network Security, Prentice Hall International, 2nd Edition, 2002.