1	**Name of Course/Module : CRYPTOGRAPHY**						
2	**Course Code: CRPT-351**						
3	**Name(s) of academic staff:**						
4	**Rationale for the inclusion of the course /module in the programme:** This course provides an introduction to modern cryptography and communication security. It focuses on how cryptographic algorithms and protocols work and how to use them.						
5	**Semester and Year offered:** year 3 semester 5						
6	**Course Hours**	Face to Face				ILT	TSLT
		L	T	P	O		
	L=Lecture T=Tutorial P=Practical O=Others TSLT=Total student learning time	51	13	17	6	81	168
7	**Credit Value:3**						
8	**Prerequisite:** Nil						
9	**Course Learning Outcomes:** On completion of this course students will be able to: • Understand basic principles of cryptography and general cryptanalysis. • Compose, build and analyze simple cryptographic solutions in a professional manner. • Acquaint with the concepts of symmetric encryption and authentication.						
10	**Transferable Skills:** • Critical Thinking & Problem Solving Skills • Information Management & Life Long Learning • Ethics, moral and professionalism						
11	**Teaching –learning and assessment strategy** • Lectures • Tutorials At the end of the programme, students are given an opportunity to evaluate the course and the lecturer.						
12	**Synopsis:** The course objective is to familiarize basic concepts of cryptography so as the students can use their understanding for information security purpose.The course covers the concepts of block ciphers and message authentication codes, public key encryption, digital signatures and key establishment.						
13	**Mode of Delivery:** Lectures, Tutorials, Practical.						
14	**Assessments Methods and Types:** Assignments 20% Mid Exam 20% Final Exam 50% Quiz 10% **Total 100%**						
15	**Content Outline of the course/module and the SLT per topic**						
	No	**Subject description**	**Face to face**			**ILT**	**Total**

			Lecture	Tutorial	Practical	Others		
1.	**Introduction to Cryptography:** • Computer Security, Information Security, Cybersecurity, Network Security • CIA Traid • Introduction to Cryptography, Cryptosystem, Cryptanalysis • Security Services and Mechanisms	5	2	-	-	7	14
2.	**Classical Encryption Techniques:** • Classical Cryptosystems, Introduction to Substitution and Transposition techniques • Caesar Cipher, Monoalphabetic ciphers • Polyalphabetic Ciphers, Playfair Cipher, Hill Cipher, Vigenere Cipher, Verman Cipher, One-time pad, Rail Fence cipher	4	-	4	-	8	16
3.	**Block Ciphers and the Data Encryption Standard:** • Modern Ciphers, Stream Cipher, Block Cipher • Data Encryption Standard (DES), Double DES, Triple DES	3	1	-	-	4	8
4.	**Advanced Encryption Standard:** • Introduction, Structure of AES • Encryption Process, Round Functions, Decryption Process	3	1	-	-	4	8
5.	**More on Symmetric Ciphers:** • International Data Encryption Standard (IDEA) • Blowfish Algorithm	3	1	-	-	4	8

	6.	**Confidentiality Using Symmetric Encryption:** • Potential Locations for Confidentiality attack, Approaches for encryption: Link encryption & End-to-end encryption, Traffic analysis • Placement of Encryption based approach, Key Distribution scenario and issues • Random numbers and Pseudorandom number generators	3	2	-	-	5	10
	7.	**Public Key Cryptography and RSA:** • Introduction to public key cryptosystems, • Encryption and Decryption process, Applications • Distribution of Public key, Man-in themiddle attack • RSA algorithm with example	5	-	3	-	8	14
	8.	**Key Management, other Public Key Cryptosystems:** • Key generation scheme • Key distribution scheme, Diffie-Helman Key Exchange Elgamal Cryptographic system	3	-	2	-	5	10
	9.	**Message Authentication and Hash Functions:** • Message Authentication, Message Authentication Functions, Message Authentication Codes • Hash Functions, Properties and Applications	4	-	3	-	7	14
	10.	**Hash and MAC Algorithms:** • Message Digests: MD4 and MD5 • Secure Hash Algorithms: SHA-1, SHA-2	2	-	2	-	4	8

	11.	**Digital Signatures and Authentication Protocol:** • Digital Signatures: Direct and Arbitrated digital signature • Digital Signature Standard: The DSS approach, The RSA approach • Authentication System, Password Based Authentication, Challenge Handshake authentication protocol, Extensible Authentication protocol, Kerberos	5	2	-	-	7	14
	12.	**Authentication Applications:** • Authentication Factors • Authentication Types • Authorization, Access Control	3	2	-	-	5	10
	13.	**Electronic Mail Security, IP Security, Web Security:** • Web Security, Threats, Overview of SSL and TLS, Overview of HTTPS • Secure Electronic Transaction Overview, Dual Signature, Payment Processing • E-Mail, SMTP, PEM, PGP, Concept of Secure Email	4	-	3	-	7	14
	14.	**Intruders, Malicious Software, Firewalls:** • Malicious Logic: Virus, Worm, Trojan Horse, Denial of Service attacks • Intrusion, Intruders and their types, Intrusion detection system • Firewall and its types	4	2	-	-	6	10
		Total	51	13	17	-	81	162
16.	**Main references supporting the course:** • Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition by Bruce Schneier							