Academic Year	: 2021-2022
Semester	: I
Category of the Course	: Program Elective-II
Course Name & Code	: Cyber Security and Cryptography: Principles and Practices (4715907)

Prerequisite:

- Mathematical concepts: Random numbers, Number theory, finite fields

Rationale:

- The subject covers various important topics concerning Cryptography and Cyber Security which are important for secure digital communication and protection of the content from criminals.
- The subject also covers the applications and attacks which use the concepts of cryptography and cyber security.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr No	Course Content	No of Hours	%
1	Unit I: Introduction to cryptography Symmetric Cipher Model, Cryptography, Cryptanalysis; Substitution and Transposition techniques. Stream ciphers and block ciphers, Block Cipher structure, Data Encryption Standard (DES) with an example, the strength of DES, Design principles of block cipher, AES with structure, its transformation Functions, key expansion, example and implementation.	7	17
2	Unit II: Cryptosystems MD5, Secure Hash Algorithm (SHA), HMAC, Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers, Cryptographic Protocols like SSL and PGP, Digital Signature and Digital Certificate, X.509 certificates, Public key infrastructure.	7	17
3	Unit III: Introduction to Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET), Intruders, Viruses and related threats. Firewall Design principles, Trusted Systems, MIME	7	17
4	Unit IV: Cryptographic Attacks Brute Force Attack, Dictionary Attack, Rainbow Table Attack, Man-in-Middle attack, Collision Attack, and Pre-image Attack	7	17

5	Unit V: Advanced Tools from Modern Cryptography Secure Multi-Party Computation, Functional Encryption, (Full) Homomorphic, Private Information Retrieval, Oblivious RAM, Symmetric Searchable Encryption, Oblivious RAM.	10	20
6	Unit VII: Current Trends The latest development in the field of Cryptography is majorly new tools for modern cryptography.	4	12

Reference Book:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Ronald Cramer, Ivan Bjerre, Jesper Buus "Secure Multiparty Computation and Secret Sharing", Cambridge University Press, 2015
3. Information Security Principles and Practice By Mark Stamp, Willy India Edition
4. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGraw-Hill
5. Cryptography and Network Security Atul Kahate, TMH
6. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
7. Information Systems Security, Godbole, Wiley-India

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Understand Cryptography and Cybersecurity concepts and types of attacks on the network.	UN
02	Differentiate the different types of symmetric and asymmetric key cryptography techniques to encrypt and decrypt text.	AP
03	Apply a different hashing function to generate secure communication.	AP
04	Evaluate the Digital Signature and latest authentication techniques for logging systems of different services.	AN
05	Critiquing the network security and web security using cryptographic algorithms.	EL

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM platform
- https://www.cse.iitb.ac.in/~mp/teach/advcrypto/s20/
- Recently Published papers/articles in reputed journals
- Software and Hardware: Bitlocker, DiskCryptor, LUKS, Calculator, FTK, SIFT, Eraser, AVG Shredder, CCleaner, Steg, Our Secret, OpenPuff