Course Type	Course Code	Name of Course	L	T	P	Credit
DE	OCSD602	Cryptography and Network Security	3	0	0	3

Course Objective

This course is to introduce the student to the areas of cryptography and cryptanalysis. This course develops a basic understanding of the algorithms used to protect users online and to understand some of the design choices behind these algorithms. Our aim is to develop a workable knowledge of the mathematics used in cryptology in this course. The course emphasizes to give a basic understanding of previous attacks on cryptosystems with the aim of preventing future attacks.

Learning Outcomes

A wide variety of basic cryptographic primitives will be discussed along with recent developments in some advanced topics like identity-based encryption, attribute-based encryption, functional encryption, two-party/multi-party computation, bitcoin and crypto-currency and postquantum cryptography. The cryptanalysis part will help us understanding challenges for cybersecurity that includes network security, data security, mobile security, cloud security and endpoint security.

Unit No.	Topics To be covered	No of Lecture Video	Video Time (Minutes)	Learning Outcome
1	Introduction to cryptography, Classical Cryptosystem, Block Cipher. Fundamental objective of Cryptography, Conventional Cryptography, Cryptanalysis, Cryptosystem. Classical Cryptosystem, Shift Cipher, Ceaser Cipher, Cryptanalysis of Shift Cipher, Shift Cipher is not secure, Substitution Cipher. Frequency analysis on Substitution Cipher, Monoalphabetic Cipher, Polyalphabetic Cipher, Transportation, Rail fence, Permutation Cipher. Polyalphabetic Cipher, Playfair Cipher. Introduction to Block Cipher, Substitution and Permutation network.	5	150	Understand the core principles, objectives, and taxonomy of conventional cryptographic systems and cryptanalysis. Analyze classical ciphers—including Shift, Caesar, Substitution, Playfair, and Transposition schemes—and assess their structural vulnerabilities. Apply frequency analysis and cryptanalytic methods to demonstrate the insecurity of historical monoalphabetic and polyalphabetic ciphers. Explain the foundational concepts of modern block ciphers and the architectural design of Substitution-Permutation Networks (SPN).
2	Data Encryption Standard (DES), Triple DES, Modes of Operation, Stream Cipher. DES encryption, Feistel Cipher, DES Key Scheduling. Attacks on DES, Generic attack, Exhaustive search, DES is not secure, Attack models Ciphertext only, Known plaintext, etc. Triple DES, Problem with Triple DES, Modes of Operation, ECB, Problem with ECB, CBC, CFB, OFB, CTR. Key Stream Generation, Shannon Perfect Secrecy, One Time Pad, Pseudorandom sequence generation, LFSR. Key stream generation, Pseudo-randomness, Golomb\\\'s randomness test.	5	150	Analyze the Feistel structure, key scheduling, and operational mechanics of DES/3DES alongside their cryptanalytic vulnerabilities and attack models. Evaluate block cipher modes of operation (ECB, CBC, CFB, OFB, CTR) to identify structural weaknesses and misuse vulnerabilities like pattern leakages in ECB. Understand stream cipher mechanics, key stream generation, Shannon's Perfect Secrecy, and the theoretical guarantees of the One-Time Pad. Assess pseudorandom sequence generation techniques using Linear Feedback Shift Registers (LFSRs) and validate statistical randomness using Golomb's randomness tests.
3	LFSR based Stream Cipher, Mathematical background, Abstract algebra, Number Theory. LFSR based Stream Cipher, Mathematical background. Abstract algebra, Number Theory, Modular Inverse.	5	150	Analyze the operation, keystream generation, and feedback polynomial mechanics of Linear Feedback Shift Register (LFSR) based stream ciphers. Master fundamental algebraic structures and number theory concepts, including modular arithmetic, prime fields, and congruences. Calculate modular multiplicative inverses (e.g., using the Extended Euclidean Algorithm) and apply abstract algebra principles to cryptographic algorithms.
4	Modular Inverse, Extended Euclid Algorithm, Fermat's Little Theorem, Euler Phi-Function, Euler's theorem. Modular Inverse, Extended, Euclidean Algorithm, Fermat's Little Theorem, Euler Phi – Function, Euler's theorem, Quadratic Residue, Polynomial Arithmetic.	5	150	Apply the Extended Euclidean Algorithm to compute modular multiplicative inverses and solve linear congruences in cryptographic algorithms. Master core number-theoretic concepts, including Fermat's Little Theorem, Euler's Phi-function, and Euler's Theorem, to simplify modular exponentiations and verify primality. Analyze advanced algebraic constructs, including quadratic residues and polynomial arithmetic over finite fields, underpinning public-key cryptosystems.
5	Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Diffie-Hellman Key Exchange, Knapsack	5	150	Analyze the non-Feistel architecture, state transformations, and finite field arithmetic of the Advanced Encryption Standard (AES).

	Cryptosystem, RSA Cryptosystem. Deepen the understanding regarding Advanced Encryption Standard (AES), it will be introducing Public Key Cryptosystem, Diffie-Hellman Key Exchange and RSA Cryptosystem.			Understand the core principles of asymmetric cryptography and the discrete logarithm problem underpinning Diffie-Hellman key exchange. Construct and evaluate foundational public-key algorithms, including RSA and the Merkle-Hellman Knapsack cryptosystem, analyzing their underlying mathematical hardness assumptions.
6	Primarily Testing, ElGamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime.	5	150	Analyze primality testing algorithms alongside the Discrete Logarithm Problem underpinning the ElGamal cryptosystem. Examine the geometric group law, point addition, and algebraic properties of Elliptic Curves defined over real numbers ($\mathbb{R}$). Apply Elliptic Curve arithmetic modulo a prime ($\mathbb{F}_p$) to construct and evaluate modern Elliptic Curve Cryptography (ECC) schemes.
7	Generalized ElGamal Public Key Cryptosystem, Rabin Cryptosystem. Generalized ElGamal Public Key Cryptosystem, Chinese Remainder Theorem, Rabin Cryptosystem, Legendre and Jacobi Symbol, Jacobi Symbol.	5	150	Analyze the mathematical formulations of the Generalized ElGamal and Rabin cryptosystems, evaluating their security reductions to discrete logarithms and integer factorization. Master number-theoretic tools, including the Legendre and Jacobi symbols, for quadratic residue determination and efficiency in public-key algorithms. Apply the Chinese Remainder Theorem (CRT) to solve systems of modular congruences and compute square roots modulo a composite integer during Rabin decryption.
8	Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function.	5	150	Analyze cryptographic hash functions and Message Authentication Codes (MACs) to guarantee data integrity and source authentication. Evaluate digital signature schemes to establish non-repudiation and identity verification across untrusted networks. Construct secure key exchange mechanisms and Key Management architectures (including PKI and key distribution centers) for cryptographic lifecycle management.
9	Cryptographic Hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS). Universal Hashing, Cryptographic Hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS), More on Key Exchange Protocol	5	150	Analyze Universal Hashing principles and the internal construction of Cryptographic Hash Functions (e.g., the SHA family), evaluating collision resistance and preimage resistance. Evaluate the Digital Signature Standard (DSS/DSA) framework for generating and verifying signatures to ensure message integrity and non-repudiation. Construct authenticated key exchange protocols to achieve mutual entity authentication and prevent man-in-the-middle and replay attacks.
10	Cryptanalysis, Time-Memory Trade-off Attack, Differential and Linear Cryptanalysis.	5	150	Analyze advanced cryptanalytic frameworks and attack paradigms used to evaluate symmetric cipher security and establish key recovery complexity bounds. Evaluate Time-Memory Trade-off (TMTO) attacks—such as Hellman's construction and Rainbow tables—balancing precomputation storage against online search time. Apply Differential and Linear Cryptanalysis techniques to identify statistical biases, differences, and linear approximations across iterative block cipher rounds.
11	Cryptanalysis on Stream Cipher, Modern Stream Ciphers, Shamir's secret sharing and BE, Identity-based Encryption (IBE), Attribute-based Encryption (ABE). Cryptoanalysis and Stream Cipher, Modern Stream Cipher. Shamir Secret Sharing, Identity Based Encryption (IBE), Attribute Based Encryption.	5	150	Analyze modern stream cipher designs and cryptanalytic techniques (e.g., correlation and algebraic attacks) to evaluate keystream randomness and structural vulnerabilities. Apply secret sharing paradigms—such as Shamir's threshold scheme using Lagrange interpolation—and analyze Broadcast Encryption (BE) protocols for multi-recipient data distribution.

				Evaluate advanced public-key primitives including Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE) for identity-centric key management and fine-grained access control policies.
12	Side-channel attack, The Secure Sockets Layer (SSL), Pretty Good Privacy (PGP), Introduction to Quantum Cryptography, Blockchain, Bitcoin and Cryptocurrency.	5	150	Analyze hardware-level side-channel attacks on cryptographic implementations alongside applied security protocols including SSL/TLS and Pretty Good Privacy (PGP). Evaluate the fundamentals of Quantum Cryptography and quantum key distribution to address cryptographic vulnerabilities in post-quantum security environments. Examine the architectural foundations of Blockchain technology, distributed ledger consensus mechanisms, and cryptocurrency frameworks like Bitcoin.
Total No of video lectures & Video time		**60**	**1800**	

Text books

No Textbook available on the course topic as yet. All material will be made available via the NPTEL course website

Reference books:

No Reference book available on the course topic as yet. All material will be made available via the NPTEL course website

Link of NPTEL Course:

https://nptel.ac.in/courses/106105162