Cryptography and Network Security

Name: Jit Banerjee

Roll: 002310503011

Exam Roll: MCA00254011

Reg. No.: 1661867 of 2023 - 2025

Master of Computer Application,

Second Year Second Semester

Department of Computer Science,

Jadavpur University,

Kolkata – 700032, West Bengal

ABSTRACT

Cryptography is a crucial discipline within the fields of Computer Science and Mathematics, focused on securing communication and information in the presence of adversaries. It encompasses the study of techniques to encode and decode data, ensuring confidentiality, integrity, authentication, and non-repudiation in digital communications.

At its core, cryptography involves converting readable data (plaintext) into an unreadable format (ciphertext) using algorithms and secret keys. Only authorized parties possessing the appropriate keys can decrypt the ciphertext back into its original form. Traditional cryptographic systems are broadly categorized into symmetric key algorithms, where the same key is used for both encryption and decryption, and asymmetric key algorithms, where a public-private key pair is employed.

Modern cryptography incorporates mathematical rigor and computational hardness assumptions to design protocols that resist various attack vectors. Concepts such as block ciphers, stream ciphers, digital signatures, hash functions, and key exchange protocols like Diffie-Hellman or RSA are foundational to cryptographic systems in widespread use today.

Cryptography also plays a pivotal role in securing digital infrastructure, including online transactions, data storage, network communications, and user authentication systems. With the rise of technologies such as cloud computing, IoT, and blockchain, the demand for robust cryptographic solutions has never been more significant.
While current cryptographic techniques are considered secure under classical computational assumptions, the advent of quantum computing poses new challenges. Research is underway in the domain of post-quantum cryptography to develop algorithms that can withstand potential quantum attacks.

Thus, cryptography remains a dynamic and evolving field, at the heart of digital trust and security in an increasingly connected world.