SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : Fundamentals Of Cryptography

II YEAR / III SEMESTER

Unit II-

Topic : DIMENSIONS IN CRYPTOGRAPHY

DIMENSIONS OF CRYPTOGRAPY:

Cryptography involves various dimensions and aspects that collectively contribute to its effectiveness in securing communication and data. Here are some key dimensions of cryptography:

Confidentiality:

Cryptography helps ensure the confidentiality of data by encoding it in such a way that only authorized parties can access and understand it. This prevents unauthorized interception and reading of sensitive information.

Integrity:

Cryptographic techniques can verify the integrity of data, ensuring that it has not been tampered with during transmission or storage. If any modifications are made, the integrity check will fail, indicating potential unauthorized changes.

Authentication:

Cryptography enables the authentication of entities involved in communication, such as verifying the identity of users or devices. This helps prevent impersonation and ensures that data is exchanged with trusted parties.

Non-Repudiation:

Non-repudiation ensures that a sender cannot deny having sent a message or performed a transaction. This is achieved through digital signatures, which provide evidence of the sender's identity and intent.

Access Control:

Cryptography can control access to resources by encrypting or securing sensitive information. This helps enforce authorization and restricts access to authorized personnel only.

Key Management:

Cryptographic systems rely on keys for encryption and decryption. Effective key management involves generating, distributing, storing, and updating keys securely to prevent unauthorized access or compromise.

Algorithm Strength:

The security of cryptographic systems depends on the strength of the algorithms used. Strong algorithms withstand various attacks and attempts to reverse-engineer the encrypted data.

Key Length and Complexity:

The length and complexity of cryptographic keys significantly impact the security of the system. Longer keys are generally more secure against brute-force attacks.

Symmetric Cryptography:

In symmetric cryptography, the same key is used for both encryption and decryption. This requires secure key distribution but is efficient for large amounts of data.

Asymmetric Cryptography:

Asymmetric cryptography uses a pair of keys: a public key for encryption and a private key for decryption. It provides secure key exchange but is slower than symmetric cryptography.