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 ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit I- NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

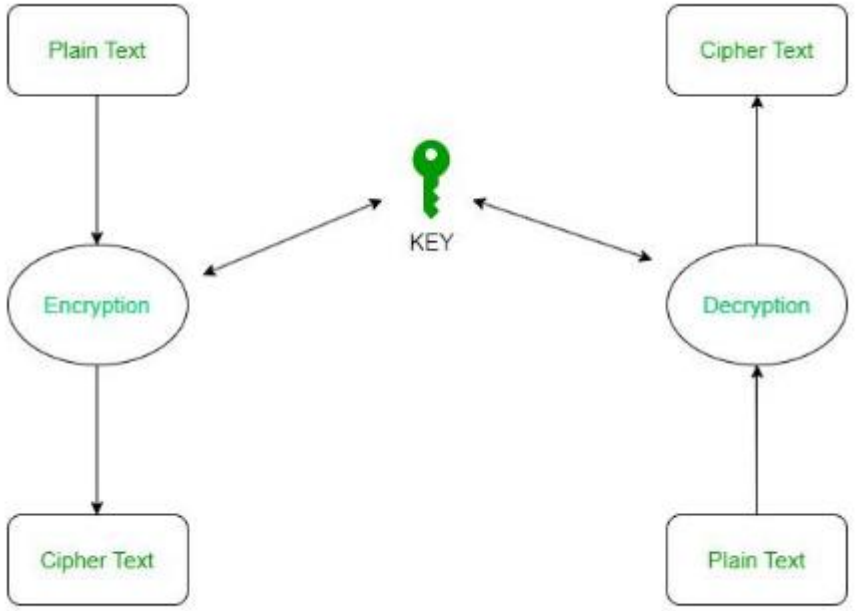
Topic : CRYPTOGRAPHIC COMPUTATIONS

What is Cryptographic Computations

- Cryptographic computations involve mathematical algorithms and techniques used to secure data through encryption, decryption, hashing, and digital signatures. These computations ensure confidentiality, integrity, authentication, and non-repudiation in secure communications and data.

What are Cryptographic Algorithms

A cryptographic algorithm is a set of steps that can be used to convert plain text into cipher text. A cryptographic algorithm is also known as an **encryption algorithm.**
A cryptographic algorithm uses an **encryption key** to hide the information and convert it into an unreadable format. Similarly, a **decryption key** can be used to convert it back into plain-readable text.



Process of Cryptography

CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms are mathematical procedures used to secure data by encrypting and decrypting information. These algorithms ensure **confidentiality, integrity, authentication, and non-repudiation** in secure communications.

Types of Algorithms :

1. Symmetric Key Algorithms (Private Key Cryptography)

- Uses a single key for both encryption and decryption.
- **Examples:**
  - **AES (Advanced Encryption Standard)** – Highly secure and widely used.
  - **DES (Data Encryption Standard)** – Older standard, now considered weak.
  - **3DES (Triple DES)** – An improvement over DES, but slower than AES.
  - **Blowfish, Twofish** – Lightweight encryption algorithms.

2. Asymmetric Key Algorithms (Public Key Cryptography)

Uses a pair of keys: a **public key** (for encryption) and a **private key** (for decryption).

Examples:

RSA (Rivest-Shamir-Adleman) – Commonly used for secure key exchange.

ECC (Elliptic Curve Cryptography) – Provides strong security with smaller key sizes.

Diffie-Hellman Key Exchange – Securely exchanges cryptographic keys over public channels

CRYPTOGRAPHIC ALGORITHMS

3. Hashing Algorithms (Message Digests)

- Converts data into a fixed-length hash value that cannot be reversed.
- Used for data integrity verification and digital signatures.
- **Examples:**
  - **SHA (Secure Hash Algorithm)** – SHA-256, SHA-512 (commonly used for security).
  - **MD5 (Message Digest 5)** – Weak due to vulnerabilities but still used for checksums.
  - **BLAKE2, Whirlpool** – Alternatives to SHA for cryptographic hashing.

4. Digital Signature Algorithms

- Ensures authenticity and integrity of digital messages and documents.
- **Examples:**
  - **DSA (Digital Signature Algorithm)** – Standard for secure digital signatures.
  - **ECDSA (Elliptic Curve Digital Signature Algorithm)** – An optimized form of DSA.
  - **RSA Digital Signatures** – Uses RSA encryption for signing messages.

Advanced Encryption Standard (AES)

1. Advanced Encryption Standard (AES)

AES (Advanced Encryption Standard) is a popular encryption algorithm which uses the same key for encryption and decryption It is a symmetric block cipher algorithm with block size of 128 bits, 192 bits or 256 bits. AES algorithm is widely regarded as the replacement of DES (Data encryption standard) algorithm, which we will learn more about later in this article.

There are many types of AES depending on the rounds:

- AES-128 uses 10 rounds
- AES-192 uses 12 rounds
- AES-256 uses 14 rounds

The more rounds there are, the safer the encryption. This is why AES-256 is considered the safest encryption.

Characteristics of AES Algorithm

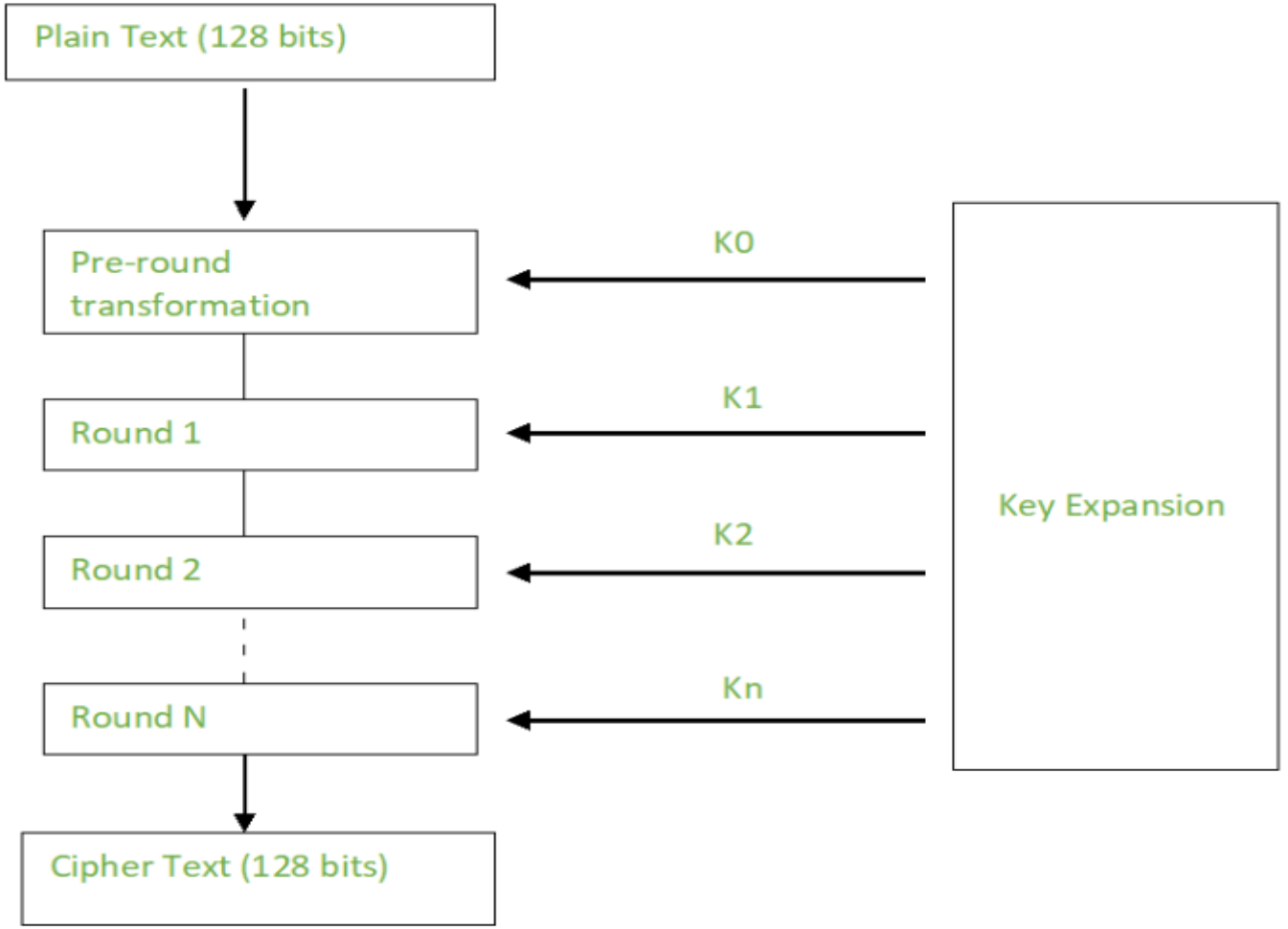
Many key sizes: Three key sizes available: 128, 192, and 256 bits

Security: Strong security measures to protect against threats

Versatile: It is versatile because it can be used for both hardware and software

Wide applications: Widely adopted in various applications, including:Google Cloud, Facebook and Password managers.

Advanced Encryption Standard (AES)



Data Encryption Standard (DES)

2. Data Encryption Standard (DES)

DES is an older encryption algorithm that is used to convert 64-bit plaintext data into 48-bit encrypted ciphertext. It uses symmetric keys (which means same key for encryption and decryption). It is kind of old by today's standard but can be used as a basic building block for learning newer encryption algorithms.

Characteristics of DES

Same symmetric key: DES uses symmetric-key algorithm and therefore, encryption and decryption can be done by single key using same algorithm.

Easier Implementation: DES was designed for hardwares rather than software and shows efficiency and fast implementation in hardwares.

Cipher technique: Transposition and substitution cipher is used: This algorithm uses both transposition cipher and substitution cipher technique.

Building block: DES technique acts as a building block for other cryptographic algorithms.

RSA Algorithm (Rivest, Shamir, Adleman Algorithm)

3. RSA Algorithm (Rivest, Shamir, Adleman Algorithm)

So, RSA is an basic asymmetric cryptographic algorithm which uses two different keys for encryption. The RSA algorithm works on a block cipher concept that converts plain text into cipher text and vice versa.

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.

Characteristics of RSA Algorithm

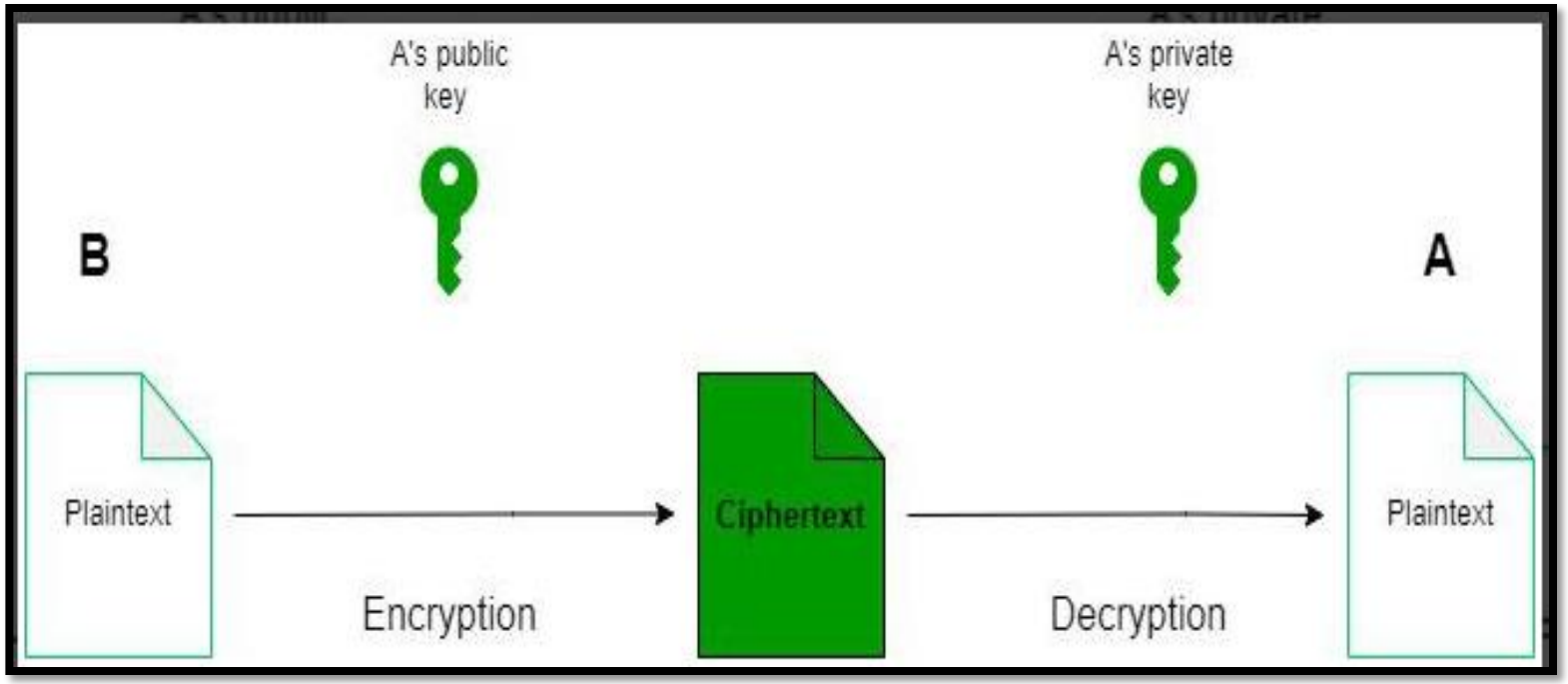
•**Security:** Many consider the RSA method to be highly secure and widely used for transmitting data

•**Fast Speed**: The RSA approach is known for its speed. Can be implemented swiftly when cryptography needs arise.

•**Different keys:** In the RSA technique two separate keys are utilized for encrypting and decrypting data. The public key is used to encrypt the information while the private key is employed for decryption.

•**Key exchange:** With the RSA method secure exchange can be achieved, enabling two parties to swap a key without transmitting it over the network.

RSA ALGORITHM



Secure Hash Algorithm (SHA)

4. Secure Hash Algorithm (SHA)

SHA is used to generate unique fixed-length digital fingerprints of input data known as hashes. SHA variations such as **SHA-2** and **SHA-3** are commonly used to ensure data integrity and authenticity. The tiniest change in input data drastically modifies the hash output, indicating a loss of integrity. Hashing is the process of storing key value pairs with the help of a hash function into a hash table.

Characteristics of Secure Hash Algorithm (SHA)

•**Security:** The SHA 256 is highly recognized for its robust security features, among hashing algorithms. It effectively prevents collision attacks ensuring that different inputs do not produce the hash value. Websites prioritize user privacy by storing passwords in a format.

•**One-way hashing:** Using SHA algorithms for one way hashing enables the storage of information like passwords. Data hashing into a fixed length output simplifies indexing and comparisons. Even a minor change in the message results, in a hash when using SHA algorithms facilitating the identification of corrupted data.

•**Avalanche effect:** A small change in the input value, even a single bit, completely changes the resultant hash value. This is called the

•**Variable input length and fixed output length:** SHA algorithm consits of a variable input length (meaning the length of input is dynamic) and a fixed output length.

COMPARISION OF ALGORITHMS
(AES, DES, RSA & SHA)

Feature	AES (Advanced Encryption Standard)	DES (Data Encryption Standard)	RSA (Rivest-Shamir-Adleman)	SHA (Secure Hash Algorithm)
Type	Symmetric Key Encryption	Symmetric Key Encryption	Asymmetric Key Encryption	Hashing Algorithm
Key Size	128, 192, or 256 bits	56 bits	1024, 2048, 4096 bits	160 (SHA-1), 256/512 bits (SHA-2)
Security Level	Very High	Low (obsolete)	Very High	High (SHA-2 recommended)
Encryption/Decryption Speed	Fast (optimized for hardware & software)	Fast (but weak security)	Slow (due to large key size)	Very Fast (one-way function)
Algorithm Type	Block Cipher (Substitution-Permutation)	Block Cipher (Feistel Structure)	Public Key Cryptography (Factorization-based)	Cryptographic Hash Function
Block Size	128 bits	64 bits	Variable (depends on key size)	160 (SHA-1), 256/512 bits (SHA-2)
Vulnerability	Resistant to brute force & cryptanalysis	Susceptible to brute force & differential cryptanalysis	Susceptible to quantum computing attacks	SHA-1 is weak; SHA-2 is secure
Usage	Wi-Fi Security, VPNs, Data Encryption	Legacy Systems (replaced by AES)	Digital Signatures, Secure Key Exchange	Digital Signatures, Password Hashing
Common Applications	TLS/SSL, Secure Storage, IoT Security	Older Banking & Telecom Systems	PKI, SSL/TLS, Email Encryption	Blockchain, Password Hashing, Digital Signatures

Any Query????

Thank you……