CRYPTOGRAPHY

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

Cryptography change Plain Text to Cipher Text i.e., a plain text is a readable format( non- encrypted data) and cipher text is non-readable format( encrypted data).

It is a method of encryption to decryption.

* Encryption is a method which information is covered into secret code.
* Decryption is a conversion of encrypted data into its original form.

**PLAIN TEXT🡪 ENCRYPTION 🡪 CIPHER TEXT 🡪 DECRYPTION 🡪 PLAIN TEXT**

**Plain text (readable format, non-encrypted data)**

**Cipher text (non-readable format, encrypted data)**



**FOR EXAMPLE:-**



HOLD ----------> QANP#\*! ------------> HOLD



Encryption key decryption key

Plain text

Encrypted data

Cipher Text

Unencrypted plain text

Decryption Key-



Algorithm like

1. AES (Advanced Encryption Standard),
2. DES (Data Encryption Standard) ,
3. ABE (Attribute-based encryption ) algorithm.

AES Algorithm takes the plain text in blocks of 128 bits and converts them into cipher text using keys of 128, 192, and 256 bits.

🡪The AES algorithm is considered secure.

DES Algorithm uses a key of 56-bit size.

🡪Using this key, the DES takes a block of 64-bit plain text as input and generates a block of 64-bit cipher text.🡪The same algorithm and key are used for encryption and decryption.

ABE Algorithm (ABE) is a vision of public key encryption that allows users to encrypt and decrypt messages based on user attributes.

🡪It allows users to encrypt & decrypt messages based on user attribute i.e., set of attribute of user key matches the attribute of cipher text.