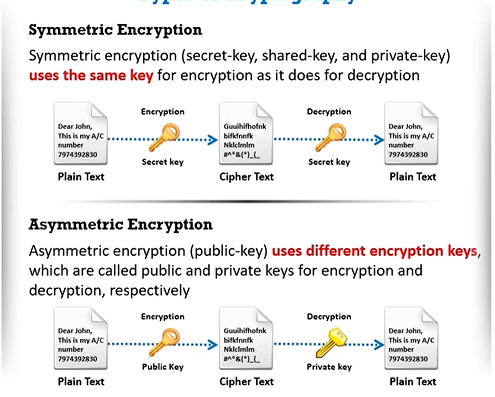
**Cryptography**

**What is Cryptography?**

Cryptography is the practice of securing communication and information through the use of codes and ciphers. It ensures confidentiality, integrity, authentication, and non-repudiation. Techniques include encryption, decryption, and key management, widely used in secure communication, online transactions, and data protection across digital platforms.

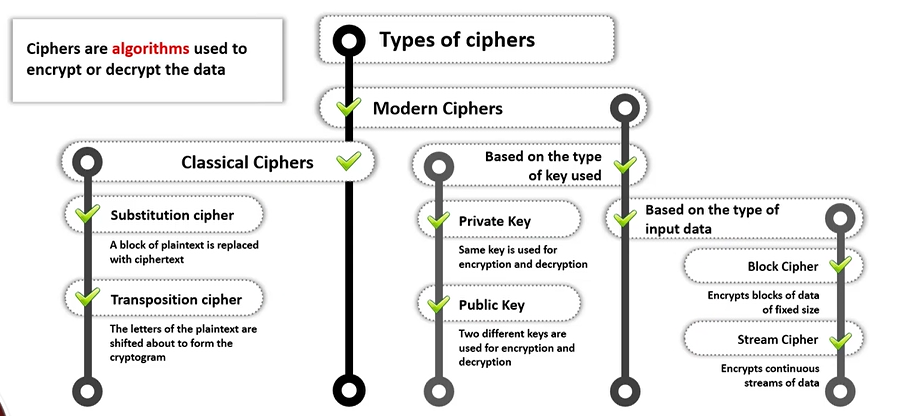
There are three main types of cryptography:

1. **Symmetric Key Cryptography**: Uses the same key for both encryption and decryption.
2. **Asymmetric Key Cryptography**: Uses a pair of keys (public and private).
3. **Hash Functions**: Converts data into a fixed-size hash value for integrity verification, without using keys.

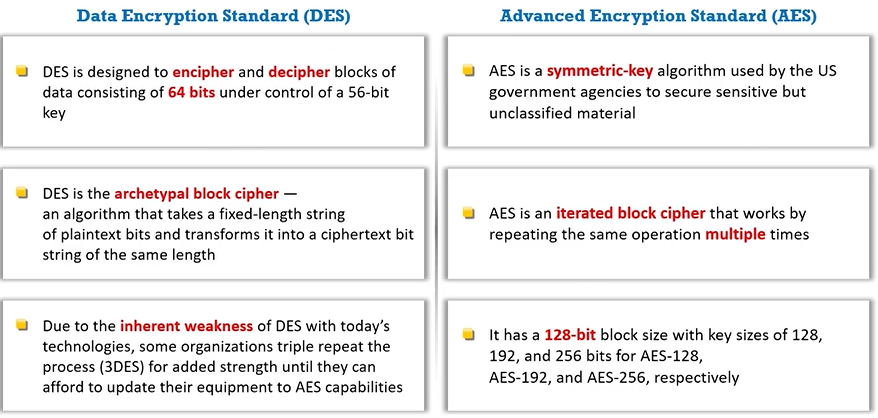


**Ciphers:**

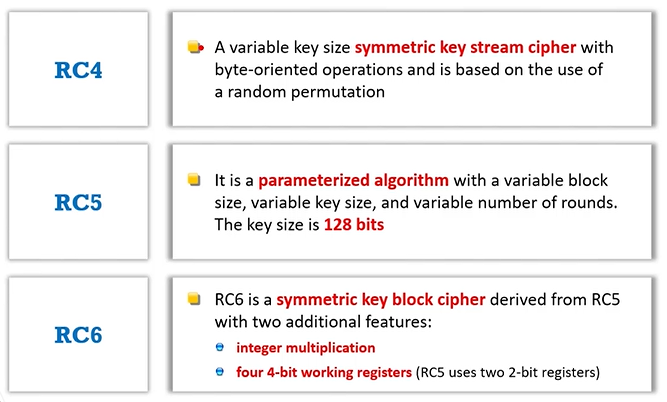
Ciphers are algorithms used to perform encryption and decryption of data. They transform plaintext into ciphertext (encoded text) to protect information. Ciphers can be symmetric (same key for encryption and decryption) or asymmetric (different keys), and they ensure confidentiality and secure communication in cryptography.



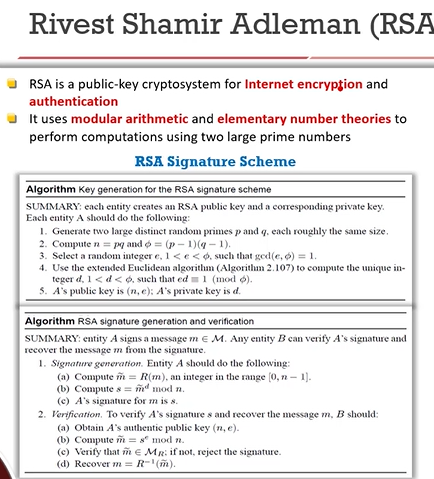
**Data Encryption Standard (DES) and Advanced Encryption Standard (AES)**



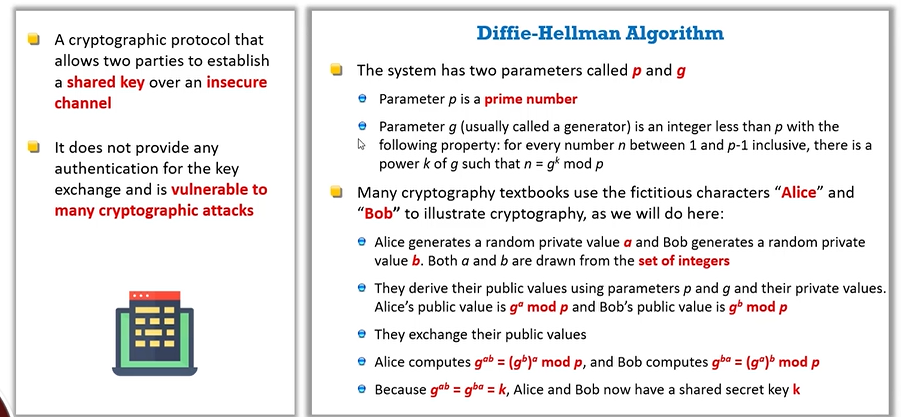
**RC4, RC5, and RC6 Algorithms:**

****

**Rivest Shamir Adleman (RSA):**

****

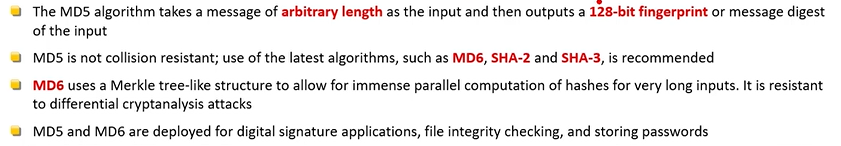
**Diffie-Hellman:**

****

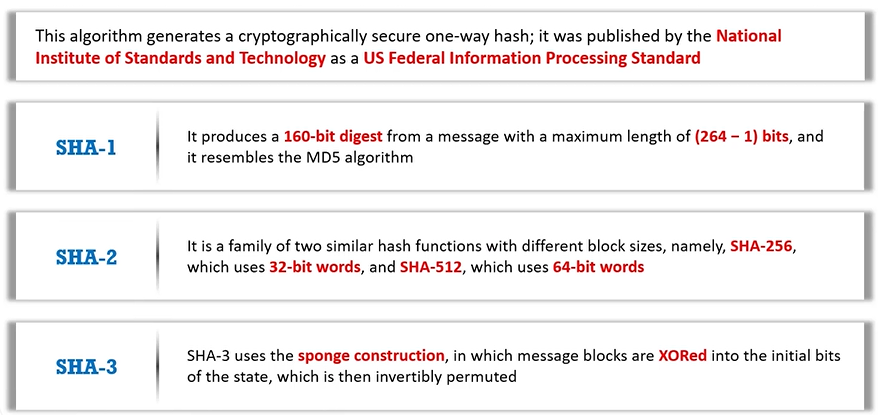
**Message Digest (One-Way-Hash) Functions:**

Message Digest (One-Way-Hash) functions are cryptographic algorithms that take input data and produce a fixed-size hash value, typically a string of characters. They are designed to be one-way, meaning the original data cannot be derived from the hash. Examples include MD5, SHA-1, and SHA-256.

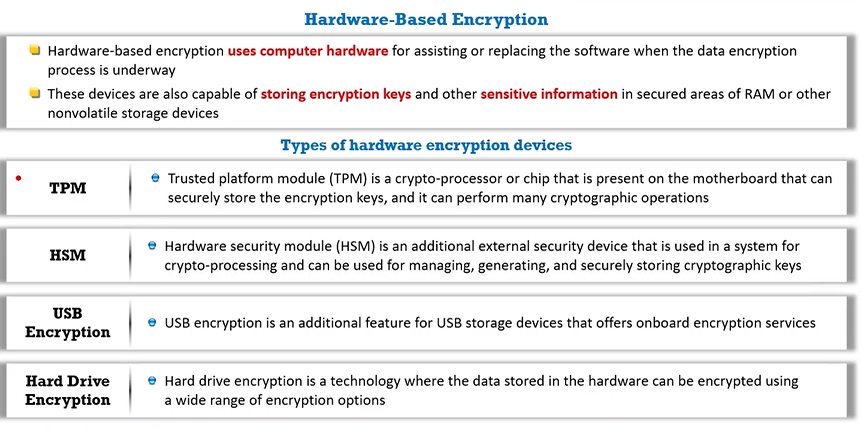
**MDF: MD5 and MD6:**



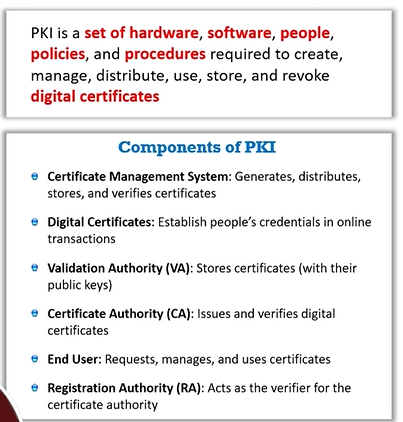
**MDF: Secure Hashing Algorithms:**



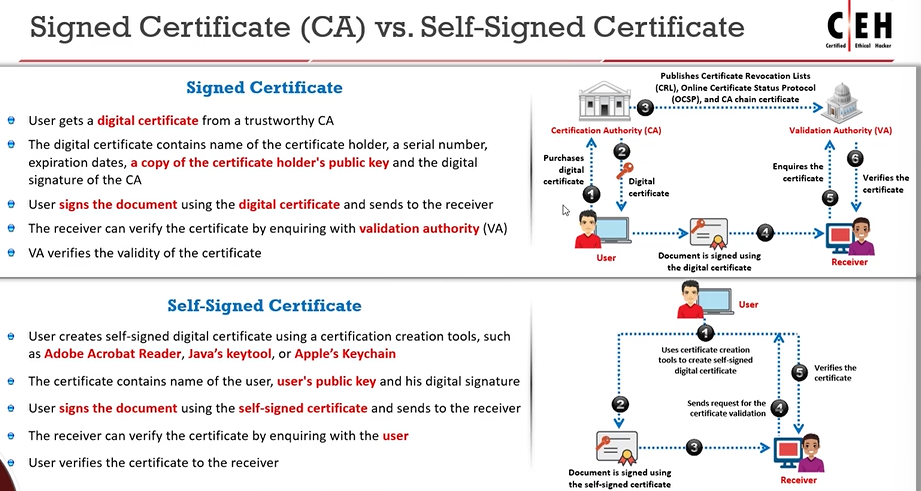
**Other encryption techniques:**



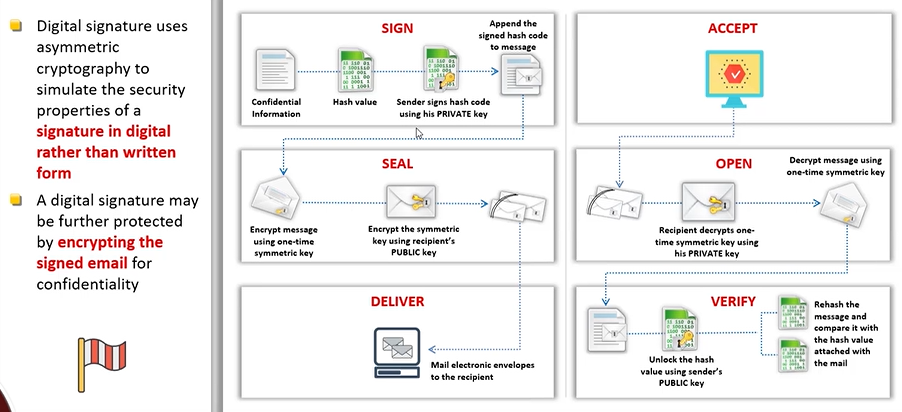
**Public Key Infrastructure (PKI):**

****

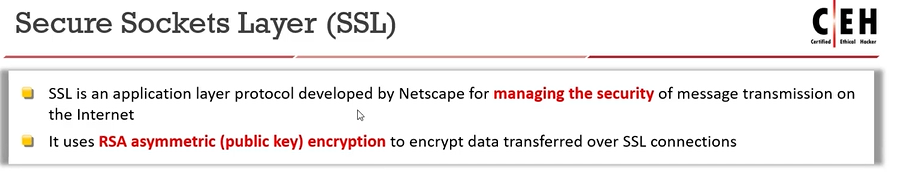
**Signed Certificate (CA) vs. Self-Signed Certificate:**

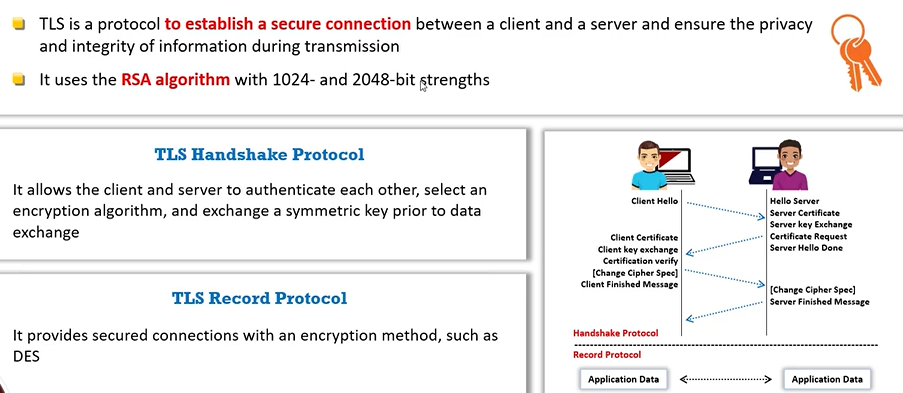
****

**Digital Signature:**

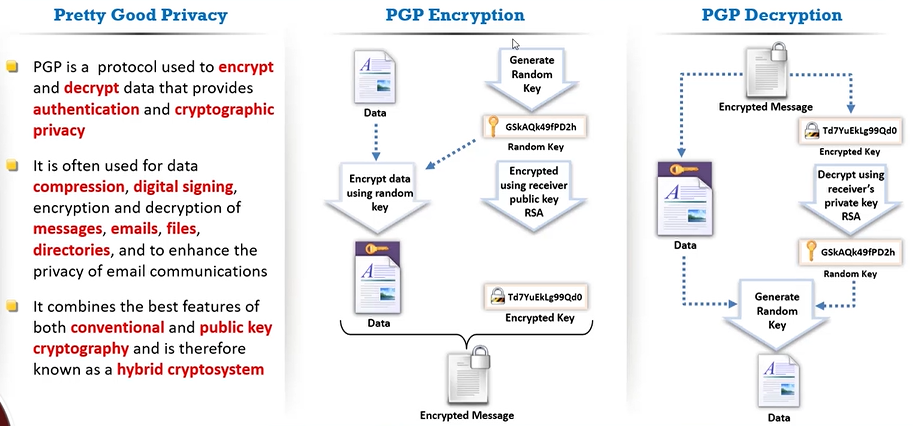
****

**Secure Socket Layer (SSL):**

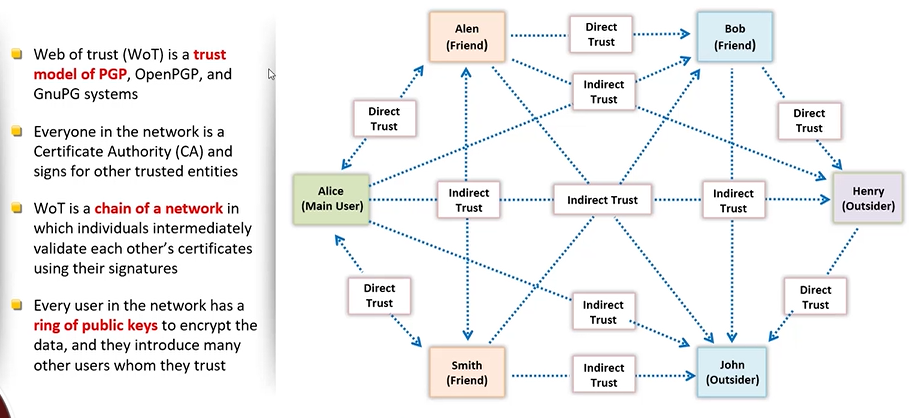
****

**Transport Layer Security (TLS):  
**

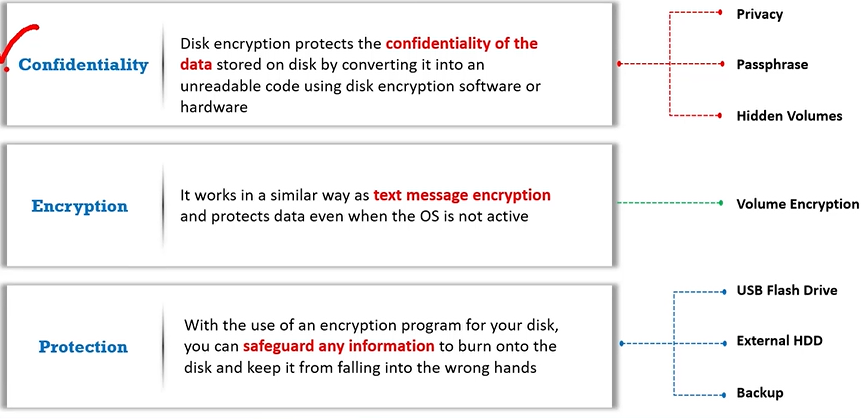
**Pretty Good Privacy (PGP):**

****

**Web of Trust (WOT):**

****

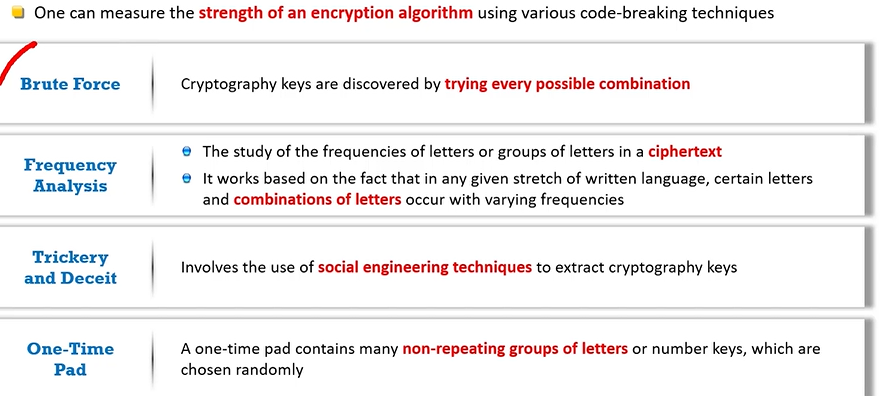
**Disk Encryption:**

****

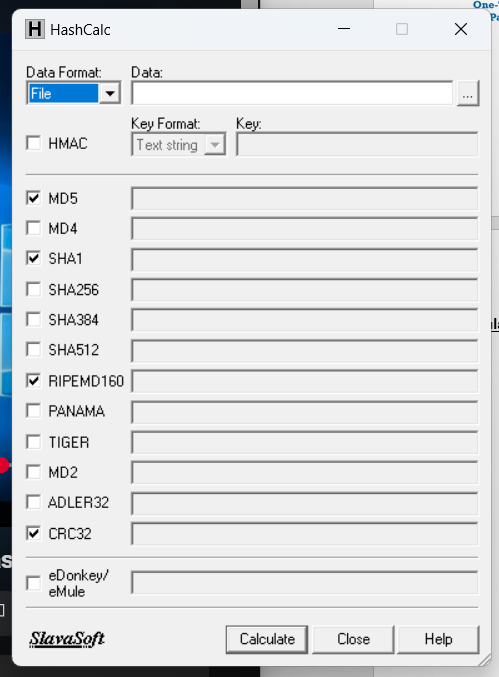
Tools:

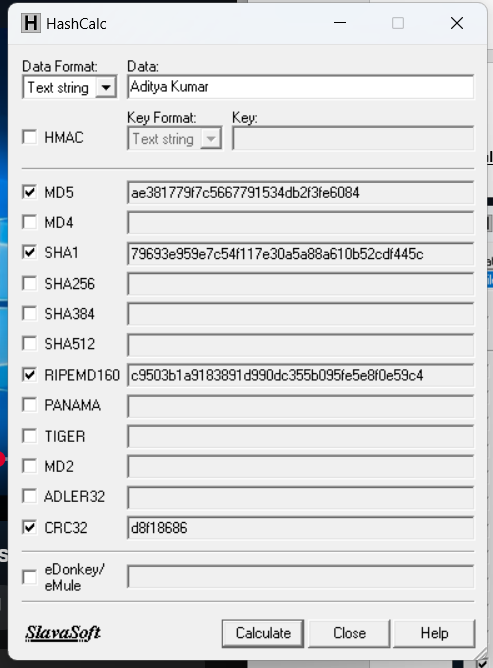
1. Veracrypt
2. Symantec Drive Encryption
3. BitLocker Drive Encryption

**Code Breaking methodologies:**

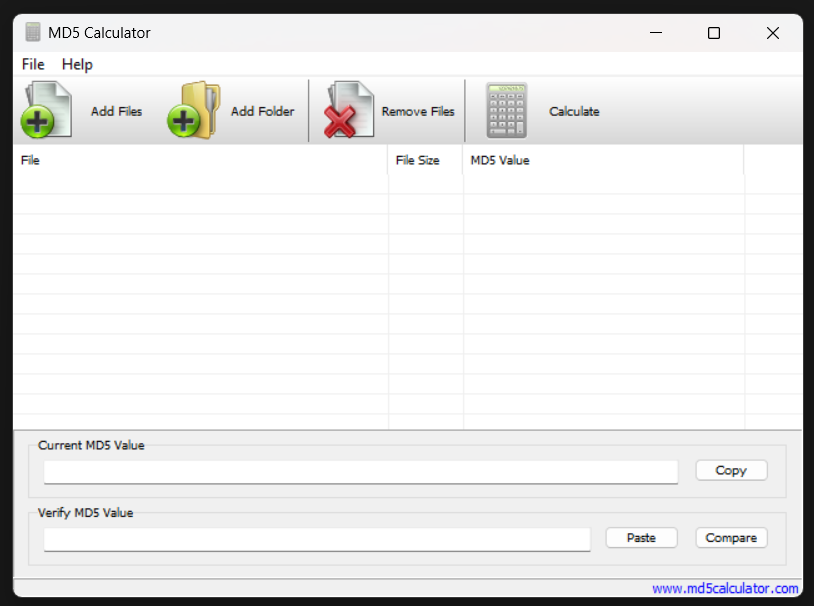


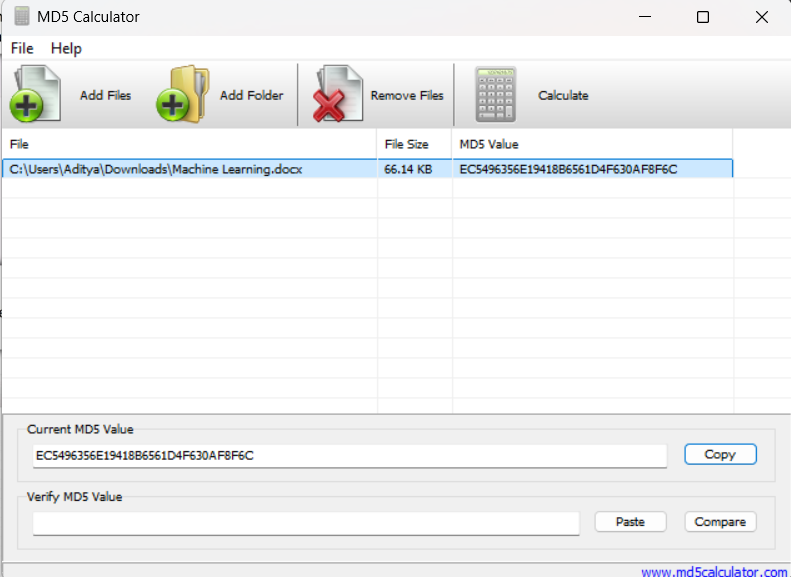
**Calculating One-way Hashes using HashCalc:**

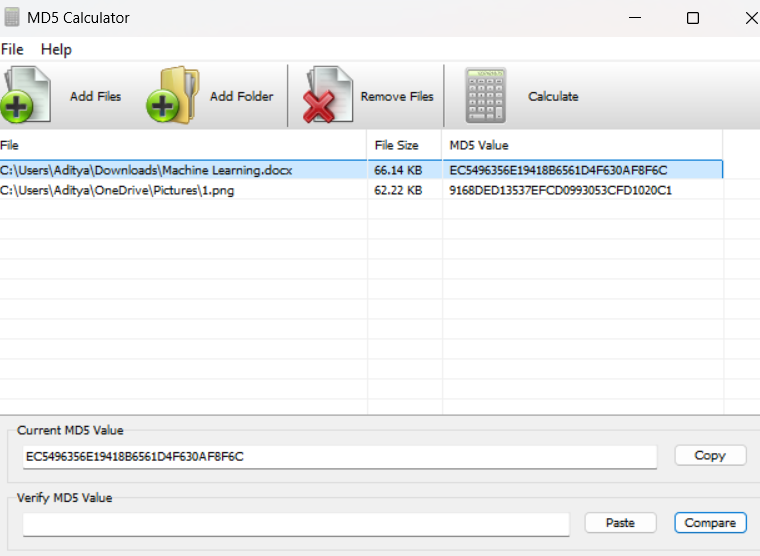
****

****

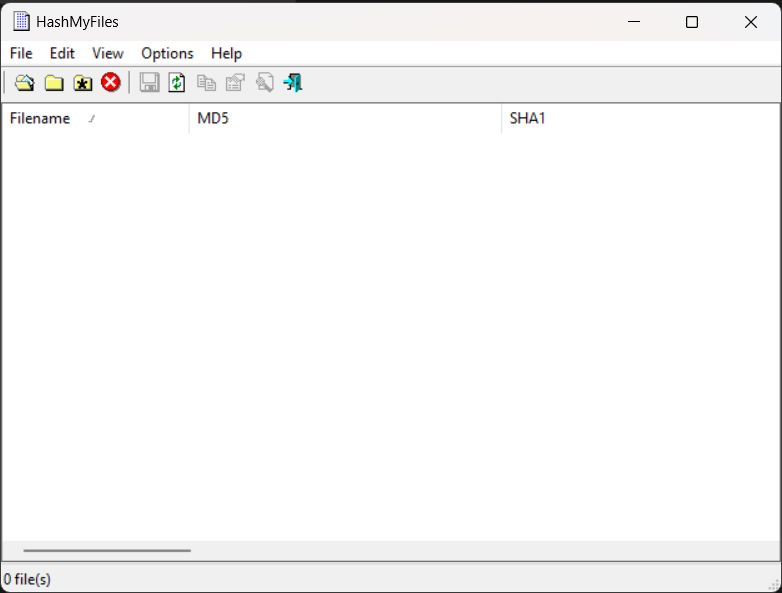
**Calculate MD5 Hashes using MD5 Calculator:**

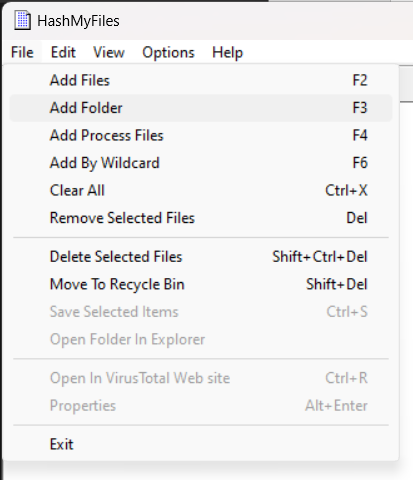
****

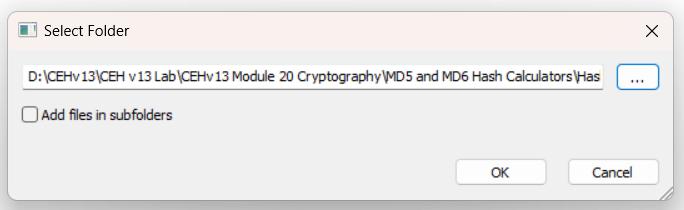
****

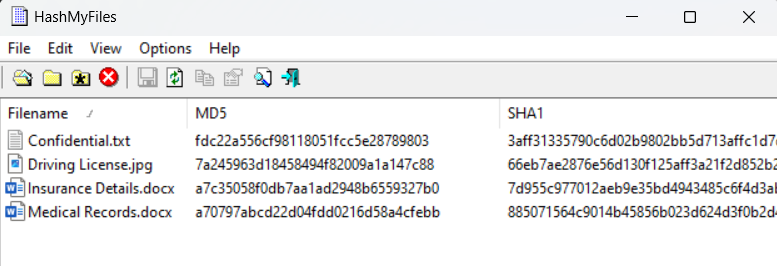
****

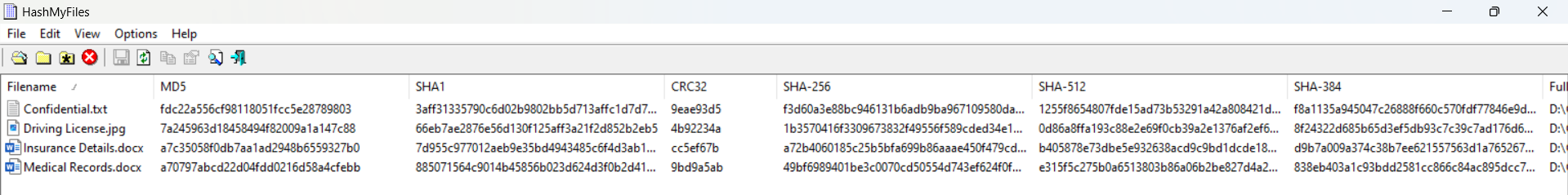
**Calculate MD5 hashes using HashMyFiles:**

****

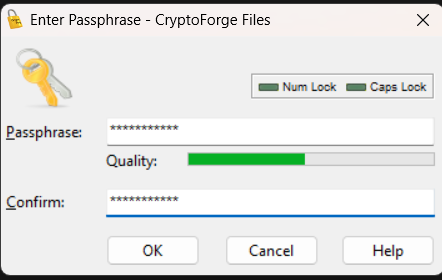
****

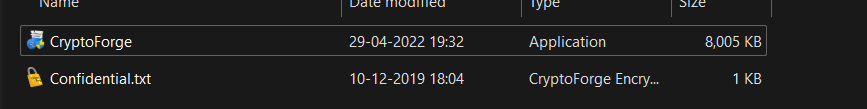
****

****

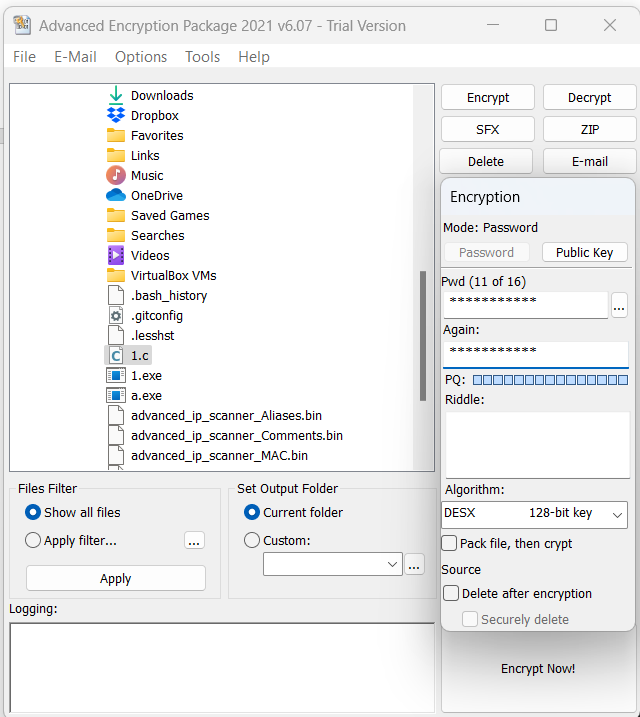
****

**Understanding File and Text Encryption using CryptoForge:**

****

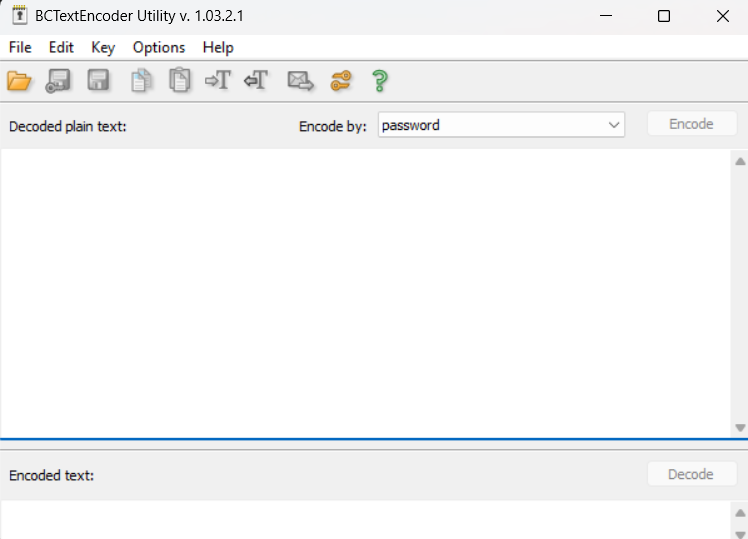
****

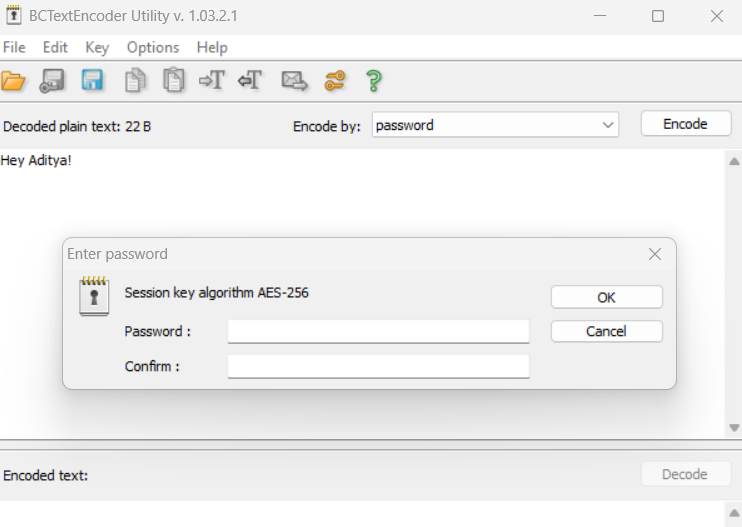
**Perform file encryption using advanced Encryption package:**

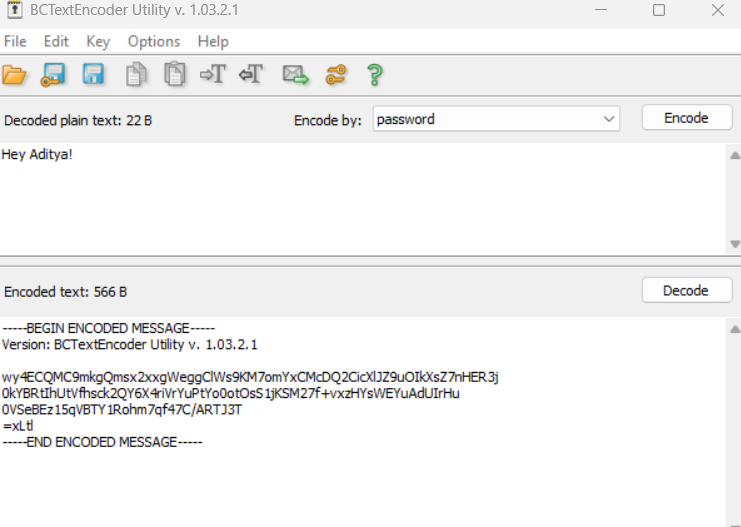
****

****

**Encrypt and Decrypt Data using BCTextEncoder:**

****

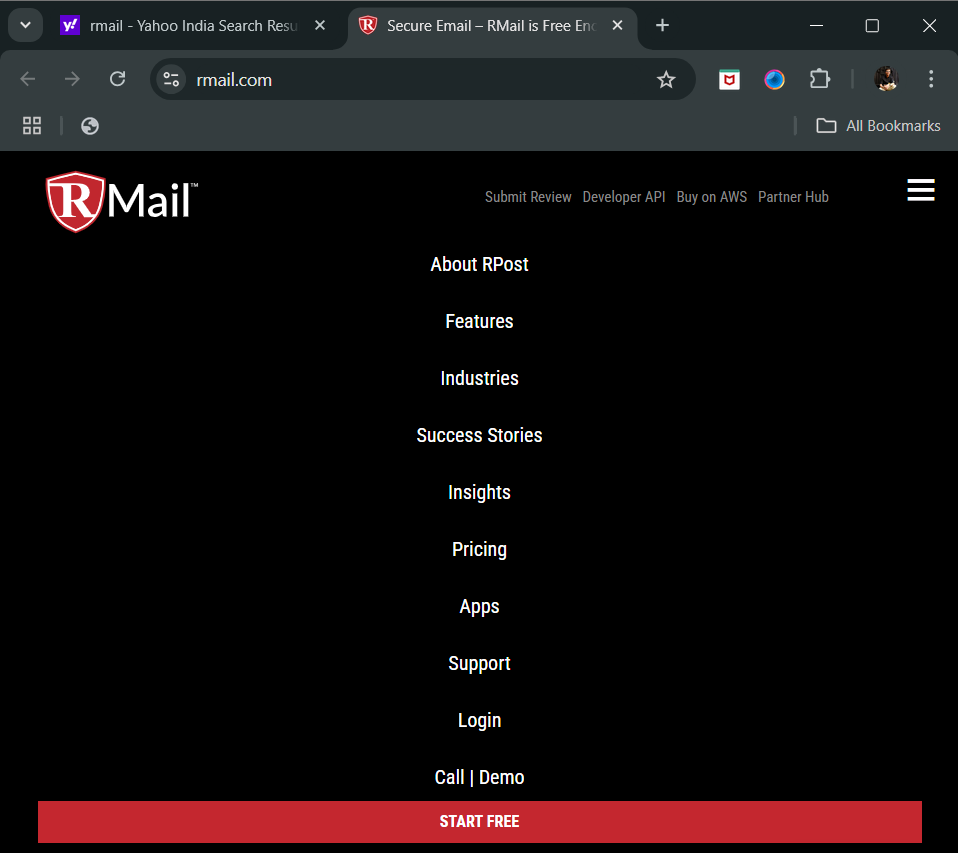
****

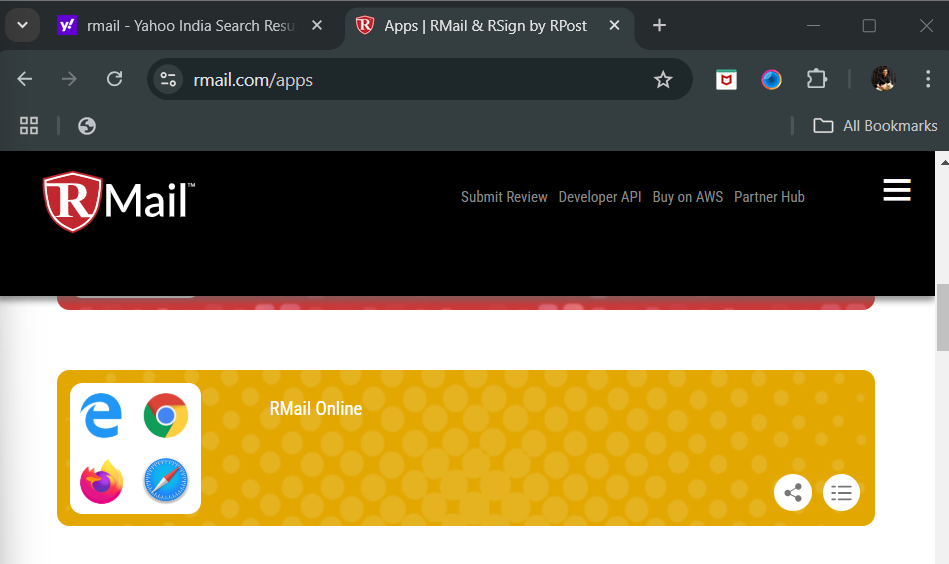
****

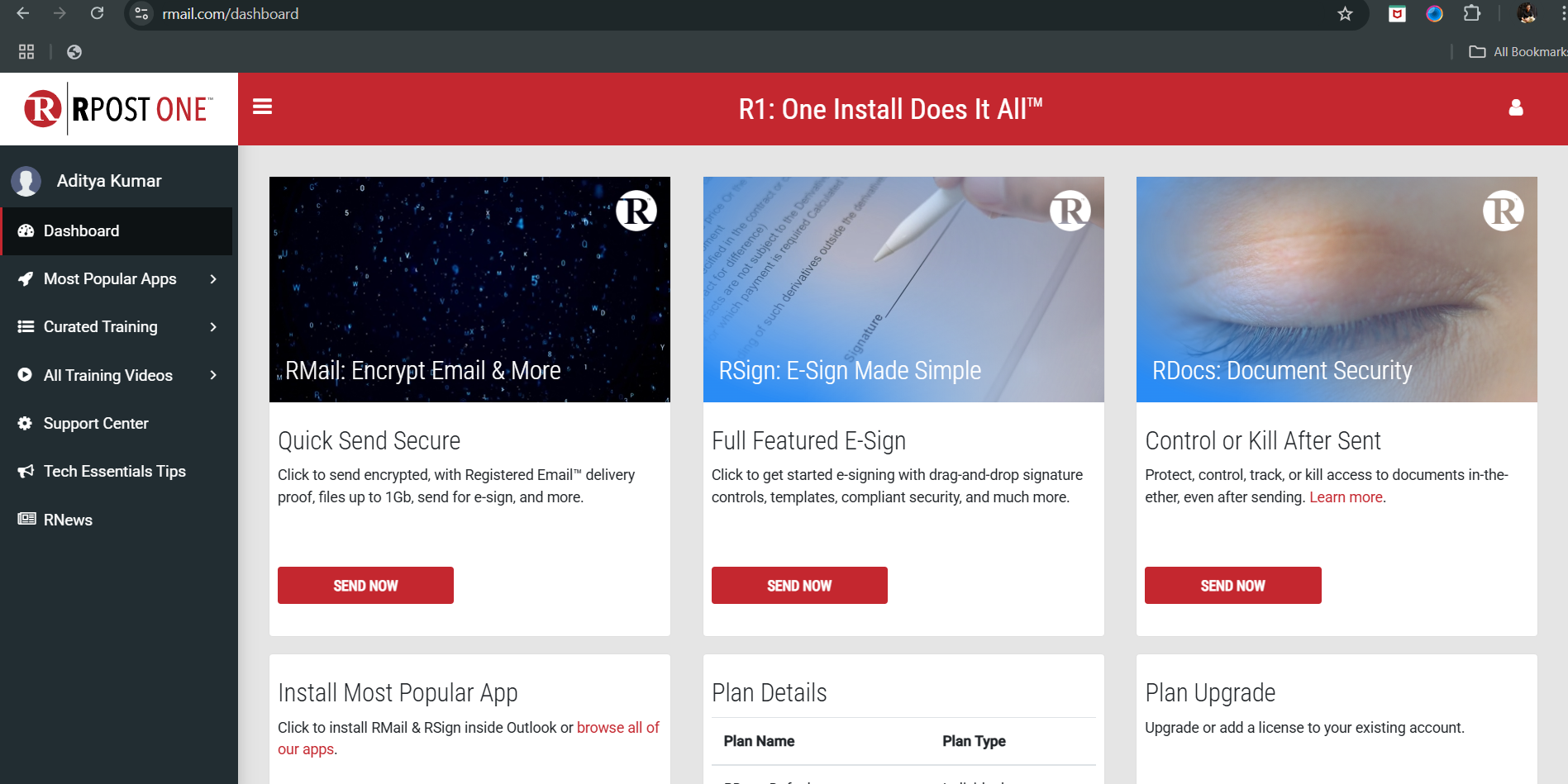
**How to Create Self Signed SSL Certificate for HTTPS**

**NA**

**Perform Email Encryption using RMail**

****

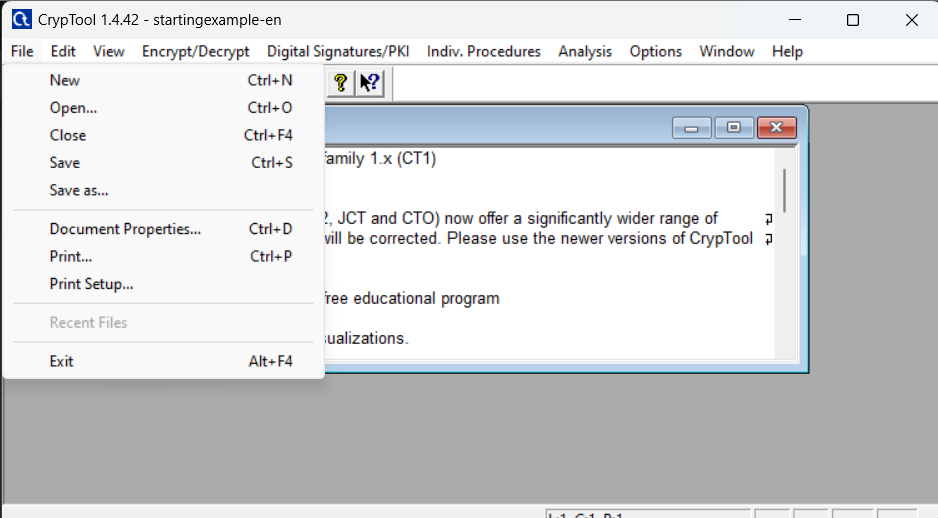
****

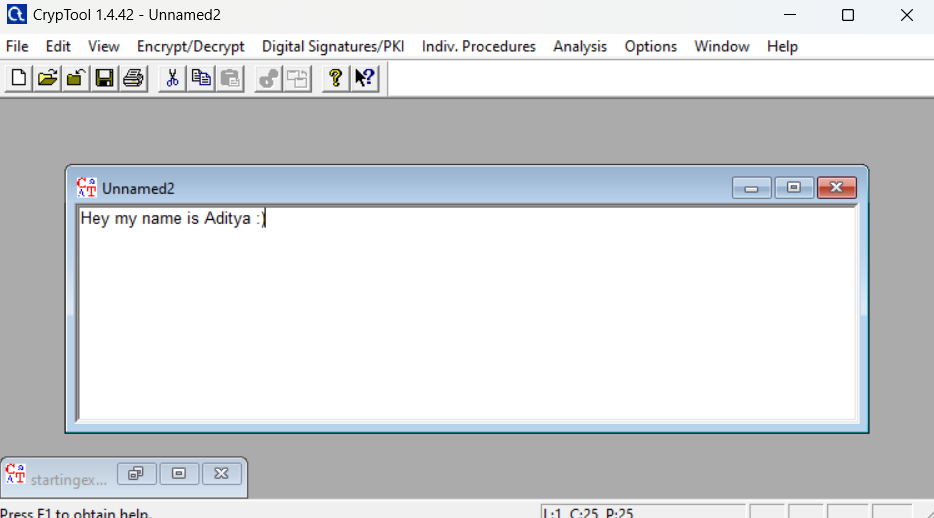
****

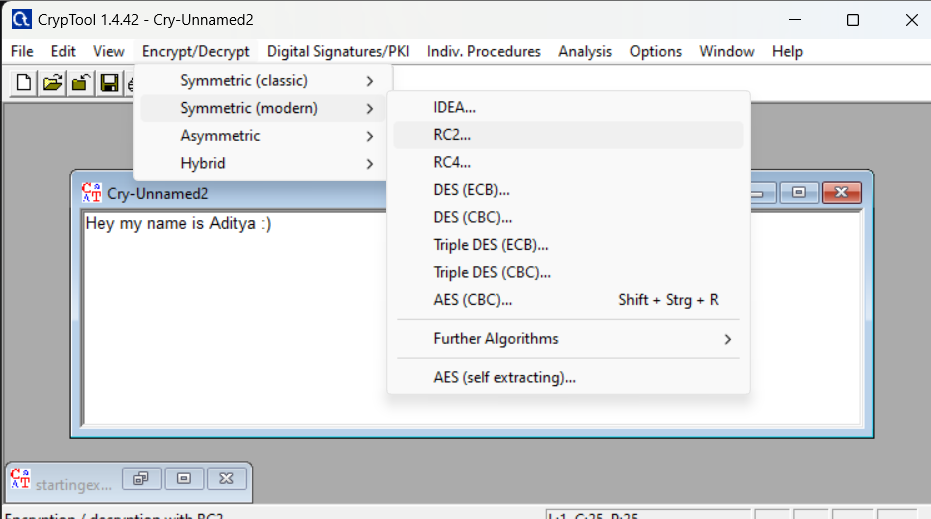
****

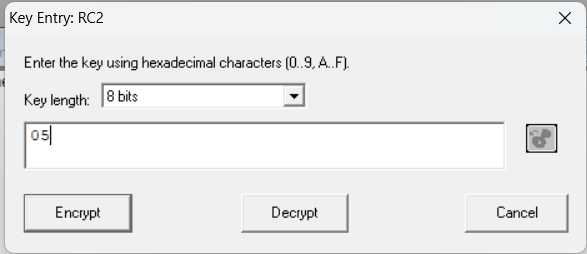
**Perform Cryptanalysis using CrypTool**

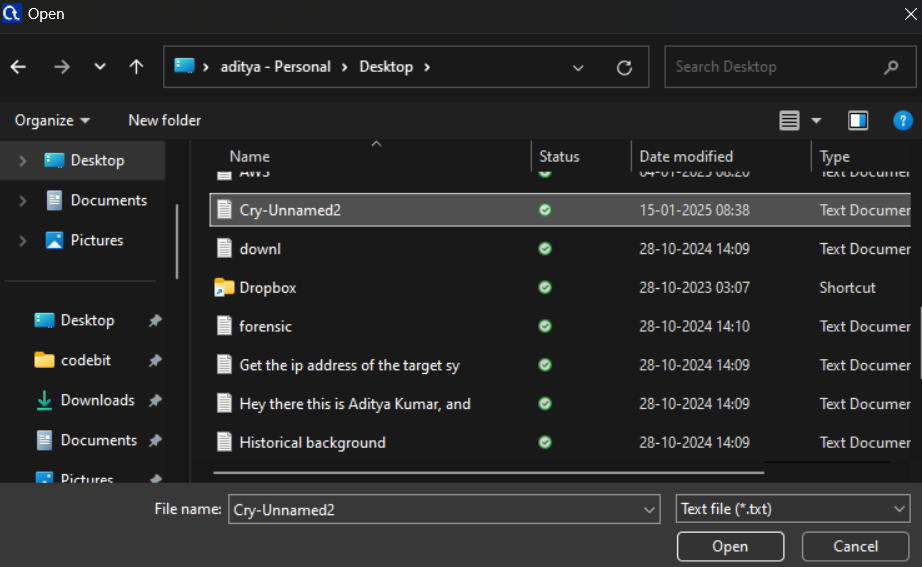
****

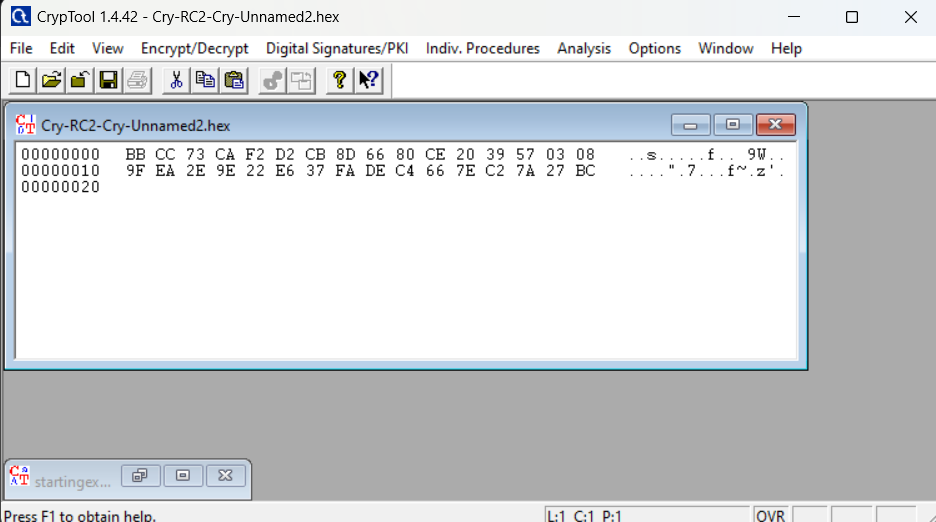
****

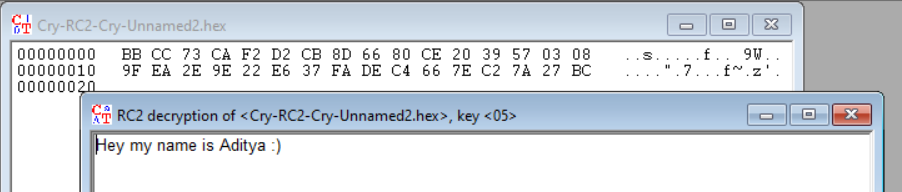
****

****

****

****

****

****