CYBER SECURITY INTERNSHIP

Ministry of MSME, Govt. of India

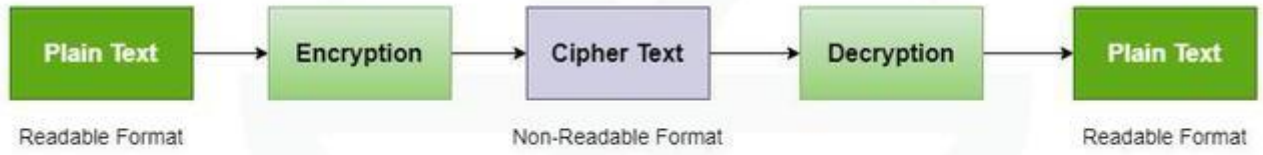
Task 6

INTRODUCTION TO CRYPTOGRAPHY

JASHMI KS

Cryptography is the science of protecting information using mathematical techniques to ensure confidentiality, integrity, and authentication. It transforms readable data into unreadable form, preventing unauthorized access and tampering.

- Converts plaintext into ciphertext using algorithms and keys
- Ensures confidentiality, integrity, authentication, and non-repudiation
- Used in secure communication, digital signatures, passwords, and online transactions

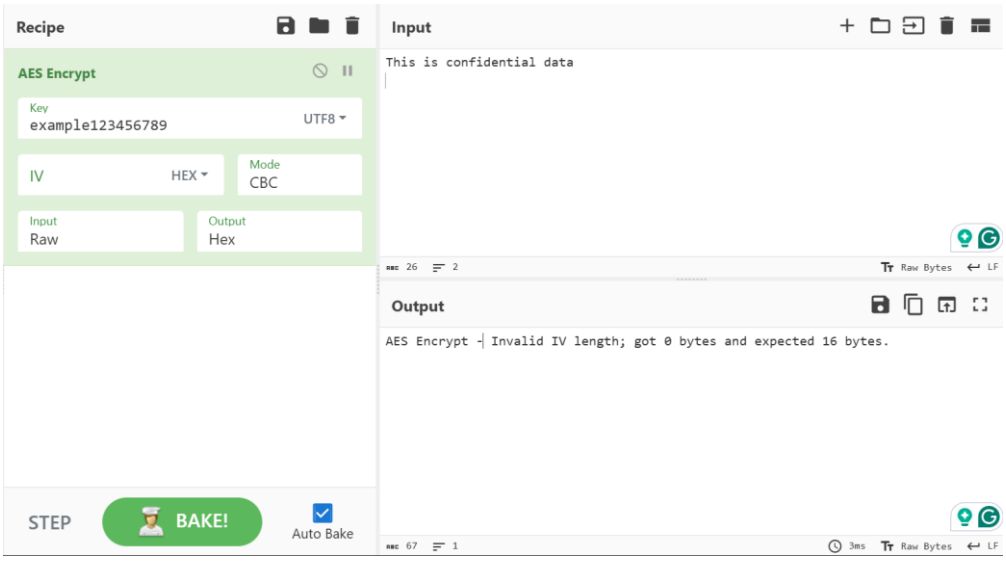


CyberChef is a web-based data analysis and cryptography tool developed by GCHQ. It allows users to perform encryption, decryption, hashing, encoding, decoding, and key generation without writing code. It is widely used in cybersecurity labs, malware analysis, digital forensics, and cryptography learning.

CyberChef works using recipes, where different cryptographic operations are dragged and executed step-by-step.

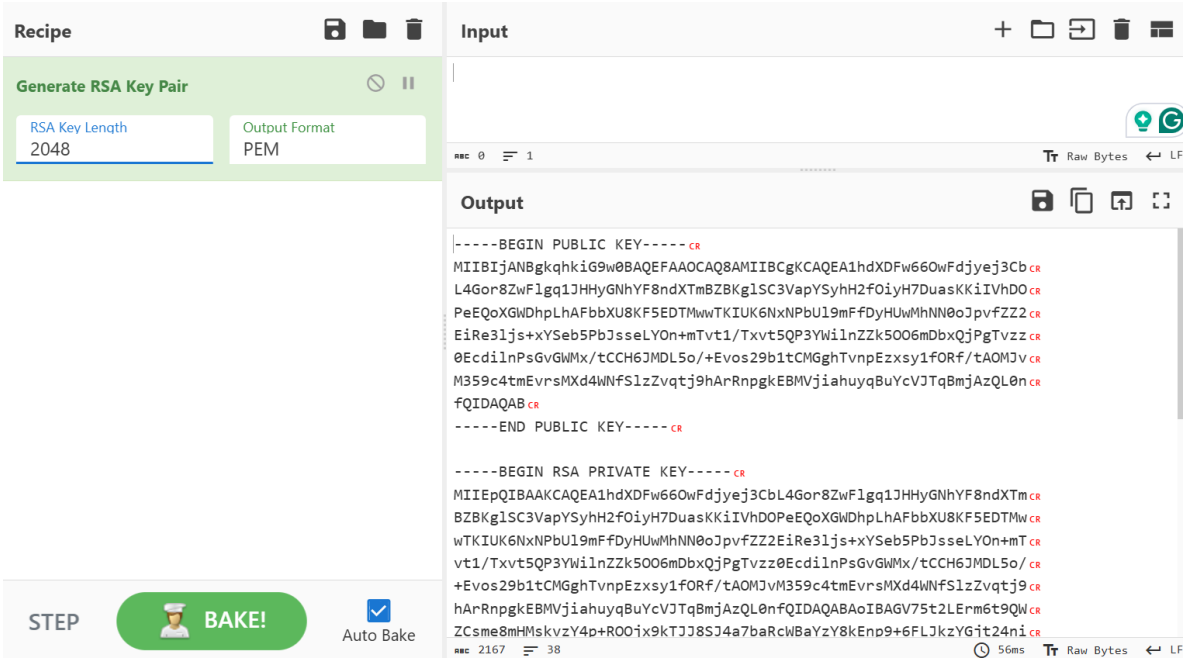
Symmetric Encryption

- Uses one single key for both encryption and decryption
- Faster and efficient
- Example: AES
- Real-world use: File encryption, disk encryption



Asymmetric Encryption

- Uses two keys
  - Public Key → Encryption
  - Private Key → Decryption
- More secure but slower
- Example: RSA
- Real-world use: HTTPS, secure email, digital signatures



Digital Signature

A digital signature is a cryptographic technique used to verify the authenticity, integrity, and non-repudiation of a digital message or document. It ensures that the message was created by a known sender and that it has not been altered during transmission.

The process of creating and verifying a digital signature involves the following steps:

1. The sender computes a message digest using a one-way hash function.
2. The message digest is encrypted using the sender's private key, forming the digital signature.

Digital Signature = Encryption (Sender's Private Key, Message Digest)

3. The sender transmits:
   - Original message
   - Digital signature
4. The receiver decrypts the digital signature using the sender's public key.
5. The receiver computes a fresh message digest from the received message.
6. If both message digests are identical, integrity and authenticity are verified.

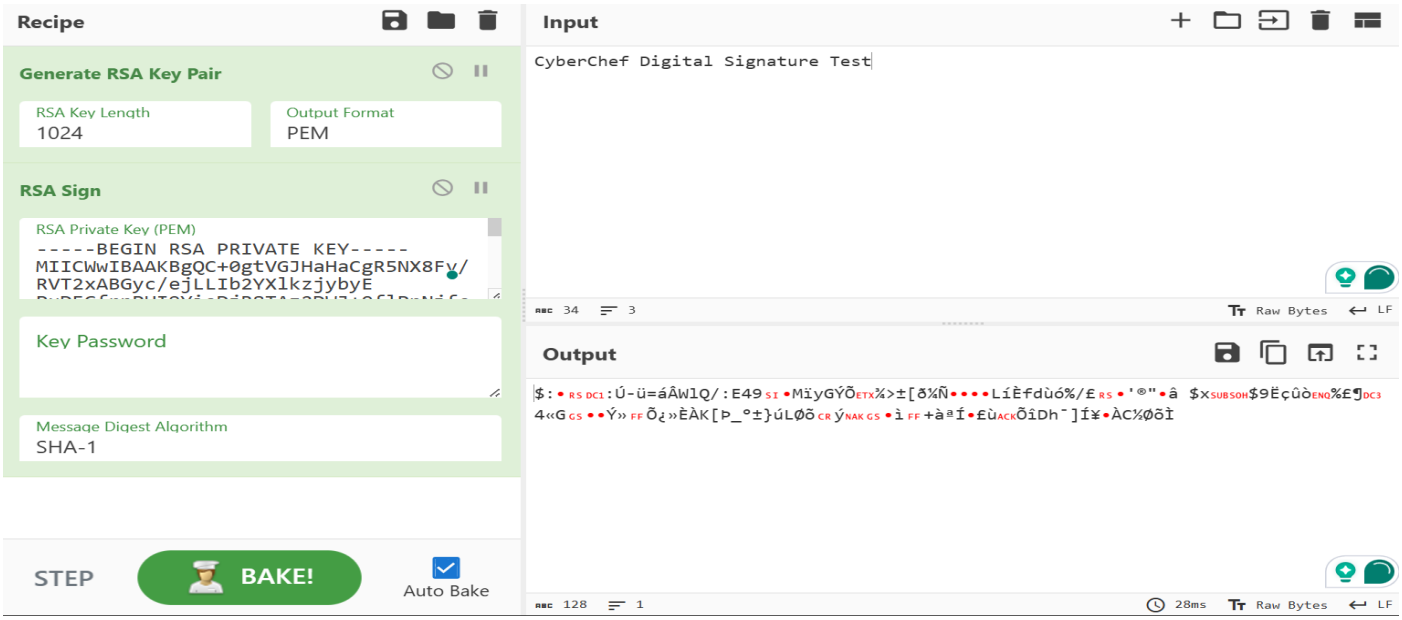
A one-way hash function ensures that:

- Hash computation is easy
- Retrieving the original message from the hash is computationally infeasible

Working of Digital Signature

Sender → Hash → Encrypt with Private Key → Digital Signature

Receiver → Decrypt with Public Key → Compare Hashes → Verify

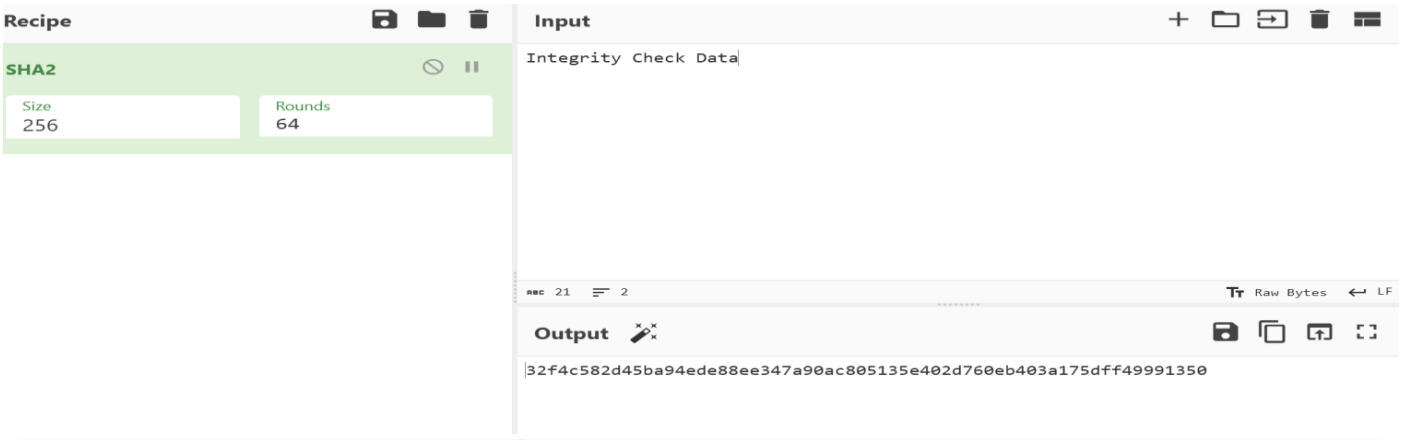


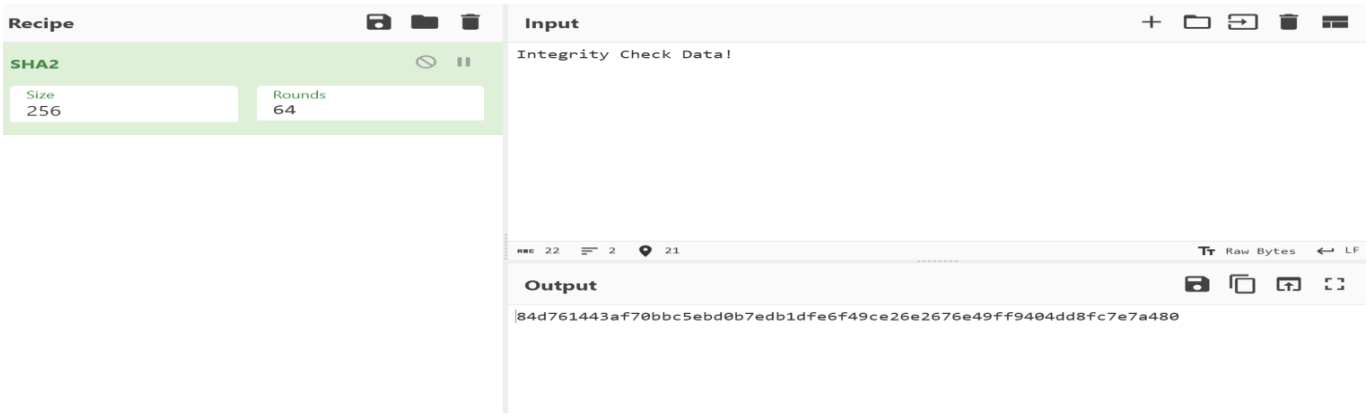
Hashing

Hashing converts data into a fixed-length hash value. Any change in input results in a completely different hash, making it useful for integrity verification.

Common hashing algorithms:

- SHA-256
- MD5





Cryptographic Algorithms

Algorithm	Type	Speed	Security	Usage
AES	Symmetric	Fast	Very High	File encryption
RSA	Asymmetric	Slow	High	Key exchange
SHA-256	Hash	Very Fast	Very High	Integrity
MD5	Hash	Fast	Weak	Legacy systems

Real-World Applications of Cryptography

HTTPS

- RSA → Key exchange
- AES → Data encryption
- SHA-256 → Integrity verification

VPN

- AES used for secure communication
- RSA for secure key exchange

Digital Certificates

- Use RSA digital signatures
- Ensure trust and authentication