

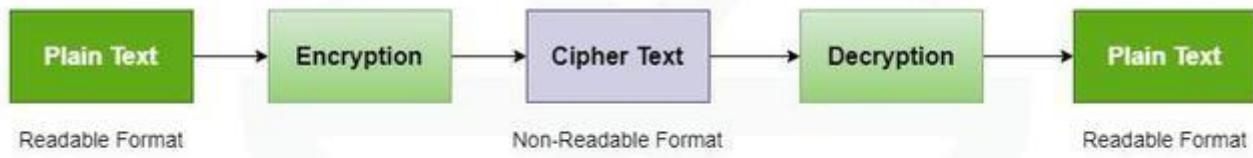
## Task 6

### 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

The screenshot shows the CyberChef interface with the following details:

- Recipe:** AES Encrypt
- Input:** "This is confidential data"
- Key:** example123456789
- IV:** (empty)
- Mode:** CBC
- Input:** Raw
- Output:** Hex
- Output Panel:** Shows an error message: "AES Encrypt - Invalid IV length; got 0 bytes and expected 16 bytes."
- Buttons:** STEP, BAKE!, Auto Bake

## 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

The screenshot shows a software interface for generating an RSA key pair. The left panel, titled 'Recipe', has a green header 'Generate RSA Key Pair' with fields for 'RSA Key Length' (set to 2048) and 'Output Format' (set to PEM). The right panel, titled 'Input', shows a text area with the generated RSA key pair. The output is displayed in two sections: 'Output' and 'Raw Bytes'. The 'Output' section shows the PEM-encoded RSA key pair, starting with '-----BEGIN PUBLIC KEY-----' and ending with '-----END PUBLIC KEY-----'. The 'Raw Bytes' section shows the raw binary data of the keys. At the bottom, there are buttons for 'STEP', 'BAKE!', and 'Auto Bake'.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEa1hdXDFw660wFdjyej3Cb
L4Gor8ZwFlgq1JHhYGNhYF8ndXTmBZBkg1SC3VapYsyhH2fOiyH7DuasKKiIVhDO
PeEqoXGWDhpLhAFbbXU8KF5EDTMwvTKIUK6NxNPbU19mFFdyHuWmNN0oJpvfZZ2
E1Re3ljs+xYSeb5PbJsselyOn+mTv1/Txvt5QP3YwilnZzk5006mDbxQjPgTvzz
0EcdilnPsvGWMx/tCCH6JMDL5o/+Evos29b1tCMGghTvpnEZxsy1fORF/tAOMJv
M359c4tmEvrsMxd4WNfs1zZvqtj9hArRnpkEBMVjiahuyqBuYcVJTqBmjAzQL0n
fQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEa1hdXDFw660wFdjyej3CbL4Gor8ZwFlgq1JHhYGNhYF8ndXTm
BZBkg1SC3VapYsyhH2fOiyH7duasKKiIVhDOPeEqoXGWDhpLhAFbbXU8KF5EDTMw
wTKIUK6NxNPbU19mFFdyHuWmNN0oJpvfZZ2EiRe3ljs+xYSeb5PbJsselyOn+mT
v1/Txvt5QP3YwilnZzk5006mDbxQjPgTvzz0EcdilnPsvGWMx/tCCH6JMDL5o/
+Evos29b1tCMGghTvpnEZxsy1fORF/tAOMJvM359c4tmEvrsMxd4WNfs1zZvqtj9
hArRnpkEBMVjiahuyqBuYcVJTqBmjAzQL0n fQIDAQABaoIBAGV75t2LERm6t9QW
ZCsme8mhMskvzY4p+ROoix9KTJ3SJA7baRclwBaYzY8kEnp9+6FLJkzYGjt24ni
acc 2167 56ms Tr Raw Bytes LF
```

## 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.
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

The screenshot shows the CyberChef interface with two main sections: 'Recipe' and 'Input'.

**Recipe:**

- Generate RSA Key Pair:** RSA Key Length: 1024, Output Format: PEM.
- RSA Sign:** RSA Private Key (PEM) is displayed, starting with "-----BEGIN RSA PRIVATE KEY-----".  
Key Password: [REDACTED]
- Message Digest Algorithm:** SHA-1

**Input:** CyberChef Digital Signature Test

**Output:** The output is a long string of raw bytes: \$ : • RS DC1 : Ú-ü=áW1Q/ : E49 SI • MiyGÝÖETX%>±[ð%Ñ••••LiÈfdùó%/E RS • '®"•â \$XSUBSON\$9ÈçùòENO%EJDC3 4«G CS ••Ý» FF Öç»»ÈÀK[P\_°±}úLØð CR ýNAK GS •ì FF +àºÍ•ÈùACKÖidh-]í¥•Ac%Øðì

**STEP:** BAKE! (with a chef icon), Auto Bake checked.

## 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

The screenshot shows the CyberChef interface with two separate hashing operations.

**Top Operation:**

**Recipe:** SHA2, Size: 256, Rounds: 64.

**Input:** Integrity Check Data!

**Output:** 32f4c582d45ba94ede88ee347a90ac805135e402d760eb403a175dff49991350

**Bottom Operation:**

**Recipe:** SHA2, Size: 256, Rounds: 64.

**Input:** Integrity Check Data!

**Output:** 84d761443af70bbc5ebd0b7edb1dfef49ce26e2676e49ff9404dd8fc7e7a480

## 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