

**BABU BANRASI DAS UNIVERSITY
LUCKNOW, UTTAR PRADESH**



IAM PROJECT ON ENCRYPTION & DECRYPTION

**SUBMITTE TO:-
MR ANAND KR GUPTA**

**SUBMITTED BY:-
ADITYA JAISWAL
U.ROLL NO:-12402640009**

TOPIC:- ENCRYPTION & DECRYPTION

Encryption:- is the process of converting readable data (plaintext) into unreadable code (ciphertext) using a mathematical algorithm and a key.

The purpose of encryption is to prevent unauthorized people from understanding or using the information.

Decryption :- is the reverse process of encryption.

It converts the ciphertext (unreadable code) back into plaintext (original readable message) using a decryption key.

TOOL:- DEVGLAN RSA ENCRYPTION & DECRYPTION



1. What is RSA?

RSA (Rivest–Shamir–Adleman) is one of the most widely used **asymmetric encryption algorithms** in cryptography.

It uses **two different keys**:

- **Public Key** → used for encryption
- **Private Key** → used for decryption

Because of this dual-key concept, RSA ensures **secure data transmission** even over insecure networks like the internet.

2. RSA Encryption Process

1. The sender obtains the **receiver's public key**.
2. The sender's system **encrypts the plaintext** message using this public key and a mathematical algorithm.
3. The result is **ciphertext**, which cannot be read without the private key.

Example:

Plaintext: HELLO

Encrypted (Ciphertext): b6Ej lmZ8DFe4+K8rHh0 . . .

3. RSA Decryption Process

1. The receiver uses their **private key** to **decrypt** the ciphertext.
2. The private key mathematically reverses the encryption process and restores the **original message**.

Example:

Ciphertext: b6Ej lmZ8DFe4+K8rHh0 . . .

Decrypted (Plaintext): HELLO

4. How RSA Works (In Simple Steps)

1. Key Generation:

- Two large prime numbers are chosen.
- Mathematical formulas generate the public and private keys.

2. Encryption:

- $\text{Ciphertext} = (\text{Plaintext}^e) \bmod n$
(using public key: e, n)

3. Decryption:

- $\text{Plaintext} = (\text{Ciphertext}^d) \bmod n$
(using private key: d, n)

5. Uses of RSA

- Securing online communications (HTTPS, SSL/TLS)
- Digital signatures and authentication
- Encrypting sensitive information such as passwords and tokens

6. Key Features

- **Asymmetric:** Uses two separate keys.
- **Highly Secure:** Based on complex prime factorization.
- **Widely Used:** In banking, emails, and digital certificates.
- **Slower than symmetric encryption**, so often combined with AES for performance.

ENCRYPTION USING RSA

Key Generation:

Two large prime numbers are generated to produce:

- A public key (modulus + exponent) for encryption.
- A private key for decryption.
- Encryption:
The sender encrypts data using the public key.
- Decryption:
The receiver decrypts the ciphertext using the private key.
- Security:
The keys are mathematically related but computationally infeasible to derive one from the other.

RSA Encryption

Enter Plain Text to Encrypt ?

HII THIS IS ADITYA,

Enter Public/Private key ?

```
bvxLjcwRldJ5KUWwXL6LIqaDaBpy1gSuKXY96Z6J8TYgU5eAadjAJWnCq2Cc7NWEclH9g
hdFTVDmcWEXqqPid/XI8uPQSkk83m88UpK2td9Dwas69GgiC/DQZ6JRY26P0ItFTIWJDnf
I+pZC2OGMbeJ4/DL862+EmXtzBJFt/270xbqvgHkJthAJnNc/I57epymPj+PgfgDvLinjezw
H+HV8pnZ+fw8xeemgMOnQv6nzZ60t2Q2rdWnwvRGLGOhf5+vytCBVpJPxSFUAE9boOIVy
frAbK5Pji10ffZ4hiHtX6E++BfTwEOZJGwIDAQAB
-----END PUBLIC KEY-----
```

RSA Key Type: ? ☒ Public key ☐ Private Key

Select Encryption Algorithm ?

RSA/ECB/OAEPWithSHA-1AndMGF1Padding

Encrypt

Encrypted Output (Base64):

```
UVB3IfBAY3HySEnEDE9VRroTopVEF+rr+u2OYxY0UvCHZH+d3MEaks5dvjGf8LUZREtCvXHC
zFlobJ4FEVtcEVyBdzZp9qmMk5xiuLI2oJPefJuWvx9CbmW+jqkzdl+hDcnIU3Y6Vi4BDI/LYUa
SFLtuEyuSKmjCjplqK3JtR1M+WyyMKW06eZXrtuvd5l0JsaYDywC+E+NlsVLp58NyBkjPey1S
o/B+rIDsorS4l5P7fj5CH64zLDzgV2g3T4V5MLWu8vK1AEGvrOM6qQJ5QKpweK//WnYw8pU
sdGU63wyy5k0LeXZE/7+vzozaCLjhtj6VgMWA6OAu1d7uDLdC2Q==
```

DECRYPTION USING RSA

When a sender encrypts data using the **receiver's public key**, only the receiver — who holds the **private key** — can decrypt and read the message.

This ensures **data confidentiality** and **secure communication**.

Step-by-step Process:

1. The sender encrypts the message using the **public key**.
2. The receiver receives the ciphertext.
3. The receiver uses their **private key** to decrypt it back to the **original plaintext**.

RSA Decryption

Enter Encrypted Text to Decrypt (Base64) ?

```
CzFlobJ4FEVtcEVyBdzZp9qmMk5xiuLI2oJPefJuWvx9CbmW+jqkzdl+hDcnIU3Y6Vi4BDI/L
YUaSFLtuEyuSKmjCjplqK3JtR1M+WyyMKW06eZXrtuvd5l0JsaYDywC+E+NlsVLp58NyBkjP
ey1So/B+rIDsorS4l5P7fj5CH64zLDzgV2g3T4V5MLWu8vK1AEGvrOM6qQJ5QKpweK//Wn
Yw8pUsdGU63wyy5k0LeXZE/7+vzozaCLjhtj6VgMWA60Au1d7uDLdC2Q==
```

Enter Public/Private key ?

```
-----BEGIN RSA PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQCtGBKFuJaRRmmXEggP
k9C2VuS2Folu/EuNzBEh0nkpRbBcvouWpoNoGnLWBK4pdj3pnonxNiBTI4Bp2MAIacKrYJz
s1YRyUf2CF0VNUOZxYRego+J39cjy49BKSTzebxSkra130PBqzr0aCIL8NBnolFjbo84i0VM
hYkOd8j6lkLY4Yxt4nj8Mvzrb4SZe3MEkW3/bvTFuq+AeQm2EAmc1z+Xnt6nKY+P4+B8YO8
uKeN7PAf4dXymdn5/DzF56aAw6dC/qfNnrS3ZDat1afC9EYsY6F/n6/K0IFWkk/FIVQAT1ug
```

RSA Key Type: ? ☐ Public key ☒ Private Key

Select Decryption Algorithm ?

RSA/ECB/OAEPWithSHA-1AndMGF1Padding

Decrypt

Decrypted Output:

HII THIS IS ADITYA,