

# BABU BANARASI DAS UNIVERSITY



## SCHOOL OF COMPUTER APPLICATION

Department of Computer Application

**BCACSN11**

Session 2025-26

## PRACTICAL LAB FILE

**SUBMITTED BY :-**

NAME –Asmit Kumar

SECTION – BCACS11

ROLL NO - 1250264029

**SUBMITTED TO:-**

Mr Anand Kumar

## INDEX

| S.No. | Name of Experiments | Page No. | Sign/ |
|-------|---------------------|----------|-------|
|-------|---------------------|----------|-------|

|    |   |  |               |
|----|---|--|---------------|
|    |   |  | <b>Remark</b> |
| 1. | RSA encryption decryption using public and private key. |  |               |
|    |   |  |               |

# Practical

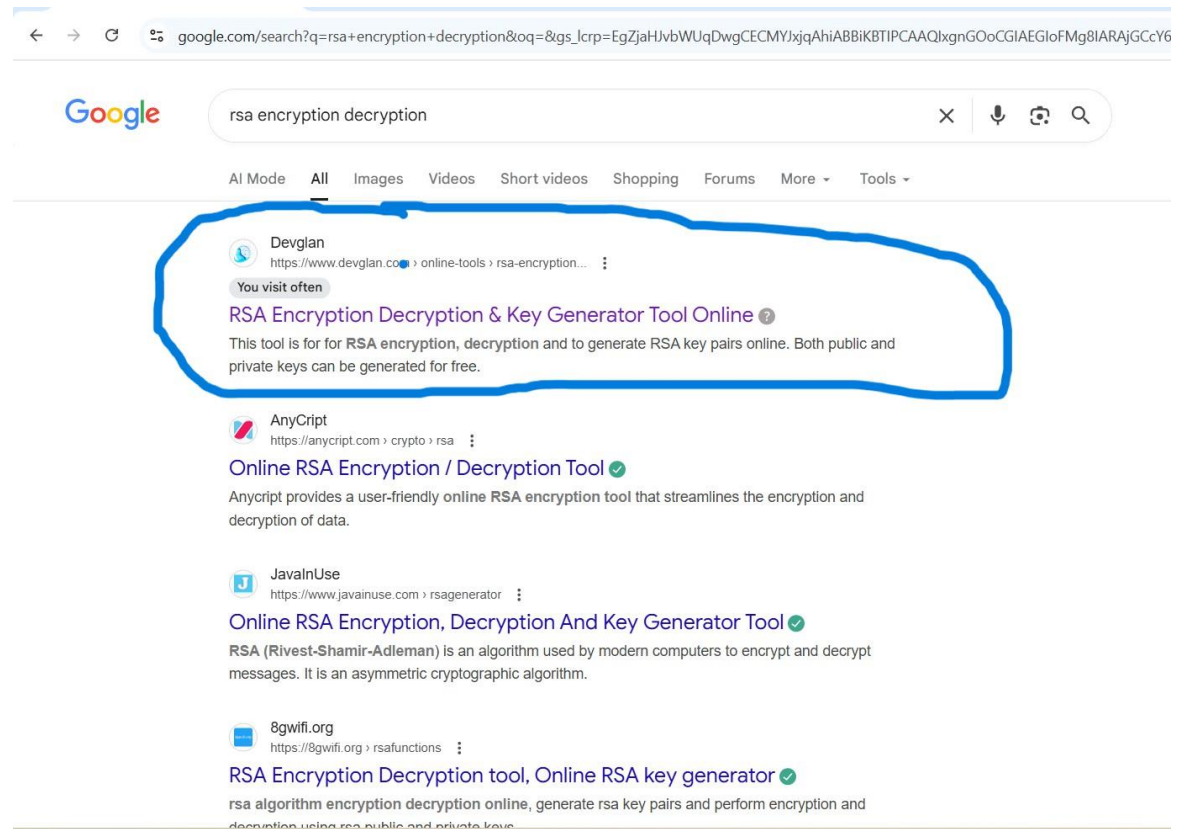
## RSA Incryption decryption

**Definition :** Rsa is a public-key cryptographic algorithm used to secure data transmission. It uses two keys- a public key for encryption and a private key for decryption.

### tools:

- \* Google chrome
- \* Incryption & decryption website

Step 1: Open google and search RSA Encryption and decryption.



Step 2: Click first link.

2048 bit

**Generate RSA Key Pair**

**Public Key(X.509 Format)**

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAstL98Yx5v/a
9GHCv8l2J9zdfGcTKPk00yM6zYlm3C9oHrMz/i9ZHBSHrsV5DThs3C
Gf01aqq1fqtWEl4p6N+wL2hna+3brrMizYneJRQK1vvukn+mByAIN2O9
2Xb18bQb7M+b0ciG+iXSI/vYLlaDnev1mFf5MeYpvjIQgRMD/NRPQilQ
fidZOcfW4PUH63flxC9zP93AjLu0j213xNPF71Ame/w7LCrgl8CvTVFG
-----
```

**Download Public Key**

Discover more [Encryption](#) [OpenSSL consulting services](#)

[cryptographic](#) [Secure email providers](#)

[Data encryption software](#) [Blockchain technology courses](#)

[Encryption algorithm selection](#) [SSL TLS certificates](#)

[Asymmetric encryption guide](#) [Penetration testing services](#)

**Private Key(PKCS8 Format)**

```
-----BEGIN RSA PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBCgwwgSkAgEAAoIBAQCys
v3xjHm/9r0YcK/yXYn3N18ZxMo+TTTlZrNiWbcl2geszP+L1kcFKGux
XkNOGzclZ/TVqqTV+q3AQjino37AvaGdr7duusyLNid4lFARW++6Sf6Y
HlAg3Y73ZdvXxtBvsz5vRylb6Jdlj+9gshoOd6/WYV/kx5im+OVCEwP
81E9CIhB+J1k5x9bg9Qfrd8JEL3M/3cCMu7SPbXfE08XvUCZ7/DssKu
-----
```

**Download Private Key**

Step 3: Generate RSA key pair.

Step 4: Enter plain text to Encrypt in RSA Encryption.

Discover more [Secure key generation](#) [cryptography](#) [Password managers](#) [Blockchain technology courses](#) [VPN services](#) [Cryptography](#) [Data encryption service](#) [Optimal key length](#) [cryptographic](#) [Generate public key](#)

### RSA Encryption

Enter Plain Text to Encrypt ?

ASHMITH

Enter Public/Private key ?

2Xb18bQb7M+b0ciG+iXSI/vYLlaDnev1mFf5MeYpvjlQgRMD/NRPQilQ  
fidZ0cfW4PUH63flxC9zP93AjLu0j213xNPF71Ame/w7LCrgI8CvTVFG  
ZYuBrKzIHrmEuQBczTKgxBZmTS7BqJhRqxDM75VMKP73nNNI639x  
M9H9SBW428G59QnEv9ANnaYuiMMGcy2kuTAYQRYq3OQlQcQBrqy  
wJ0hKwIDAQAB  
-----END PUBLIC KEY-----

Enter Encrypted Text to Decrypt (Base64) ?

Enter Encrypted Text to Decrypt

Enter Public/Private key ?

-----BEGIN RSA PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQCys  
v3xjHm/9r0YcK/yXyn3N18ZxMo+TTTlZrNiWbcL2geszP+L1kcFKGux  
XkNOGzclZ/TVqqTV+q3AQjino37AvaGdr7duusyLNid4lFarW++6Sf6Y  
HIAg3Y73ZdvXxtBvsz5vRylb6Jdlj+9gshoOd6/WYV/kx5im+OVCBEwP  
81E9CihB+J1k5x9bg9Qfrd8jEL3M/3cCMu7SPbXfE08XvUCZ7/DssKu

RSA Key Type: ☐ Public key ☒ Private Key

Select Decryption Algorithm ?

RSA/ECB/PKCS1Padding

Step 5: The data has been encrypted .

Step 6: The encrypted data was copied and pasted into RSA decryption.

### RSA Encryption

Enter Plain Text to Encrypt ?

ASHMITH

Enter Public/Private key ?

TgT79p/Dok0Tq6CiZgT/GJtlgoUmSYt24o5/GOVbOrhqBOUM/ZknPGt  
mOczY/XGFfc6ssZTEl0FI4N1HpvdxdRrpQIKl3yud4fxFj8D3k5SWV6Pg  
5cEjMw7HkymJ8WOWrlyT/yg6oAs5P/0ur/2hz8VO1oUOtfc6Tzmp+  
AzEEmkTci75RFfp19grucPA3ehJ4GwWoznQ22jRYi6PrKEmkqle2+NR  
ap2wbVh0AQuiEm51H2Wu1JGYgid48Qef0K21UlaCMIJUGjAos63M1  
5LY24jwIDAQAB

RSA Key Type: ☒ Public key ☐ Private Key

Select Encryption Algorithm ?

RSA/ECB/PKCS1Padding

Encrypt

Encrypted Output (Base64):

Result goes here

Enter Public/Private key ?

-----BEGIN RSA PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQCIGZ  
nxvFONHz99ab6jGsWhYc6Mc3cTeSQxQrNsBMBbm5ffkCakXj3Jactz  
AB6xOBPv2n8OiTROroKJmBP8Ym2WChSZJi3bjn8Y5Vs6uGoE5Qz9  
mSc8a2Y5zNj9cYV9zqyxlMSXQUjg3Uem913FGulAgqXfk53h/EWPwP  
eTIJZXo+DlwSMzDseTKYnxY5avMJJP/KDqgCzk//S6v/aHPxU7WhQ6

RSA Key Type: ☐ Public key ☒ Private Key

Select Decryption Algorithm ?

RSA/ECB/PKCS1Padding

Decrypt

Decrypted Output:

Result goes here

Step 7: Then decrypt.

Enter Public/Private key 🗑

```
2Xb18bQb7M+b0ciG+iXSI/vYLlaDnev1mFf5MeYpvjIqGRMD/NRPQilQ
fidZOcfW4PUH63flxC9zP93AjLu0j213xNPF71Ame/w7LCrgl8CvTVFG
ZYuBrKzIHrmEuQBczTKgxBZmTS7BqJhRqxDm75VMKP73nNNI639x
M9H9SBW428G59QnEv9ANnaYuiMMGcy2kuTAYQRYq3OQIQcQBraq
wJ0hKwIDAQAB
-----END PUBLIC KEY-----
```

RSA Key Type: ? ☒ Public key ☐ Private Key

Select Encryption Algorithm ?

RSA/ECB/PKCS1Padding

**Encrypt**

Encrypted Output (Base64):

```
NQ/WHqP/JkWGnHM0mBktQZzMuBCKGA2b3hBwTzRkP/xsuu/iyeny
+mIjO0NuUKwtbWXmyLXY+yopbqQXCFKiKwI4U2ppi6MHCdVqJAKT1
a1ZaoeGvmKDNzeocFYQZPIBexKR6MhhgJveeJBSv8KrsOJ38l5/nAys
CPyRr2NHpMBlo5KeutMxAGaXSilGdniSp4DeqVPx79oMP8QQkG+Bk
QUczPQg9YwGln5EtBSwQ==
```

```
81E9CihB+J1k5x9bg9Qfrd8jEL3M/3cCMu7SPbXfE08XvUCZ7/DssKu
```

RSA Key Type: ? ☐ Public key ☒ Private Key

Select Decryption Algorithm ?

RSA/ECB/PKCS1Padding

**Decrypt**

Decrypted Output:

ASHMITH