Encrypt and Decrypt a Message Using RSA

Scribe

1   Navigate to **http://localhost:5173/**
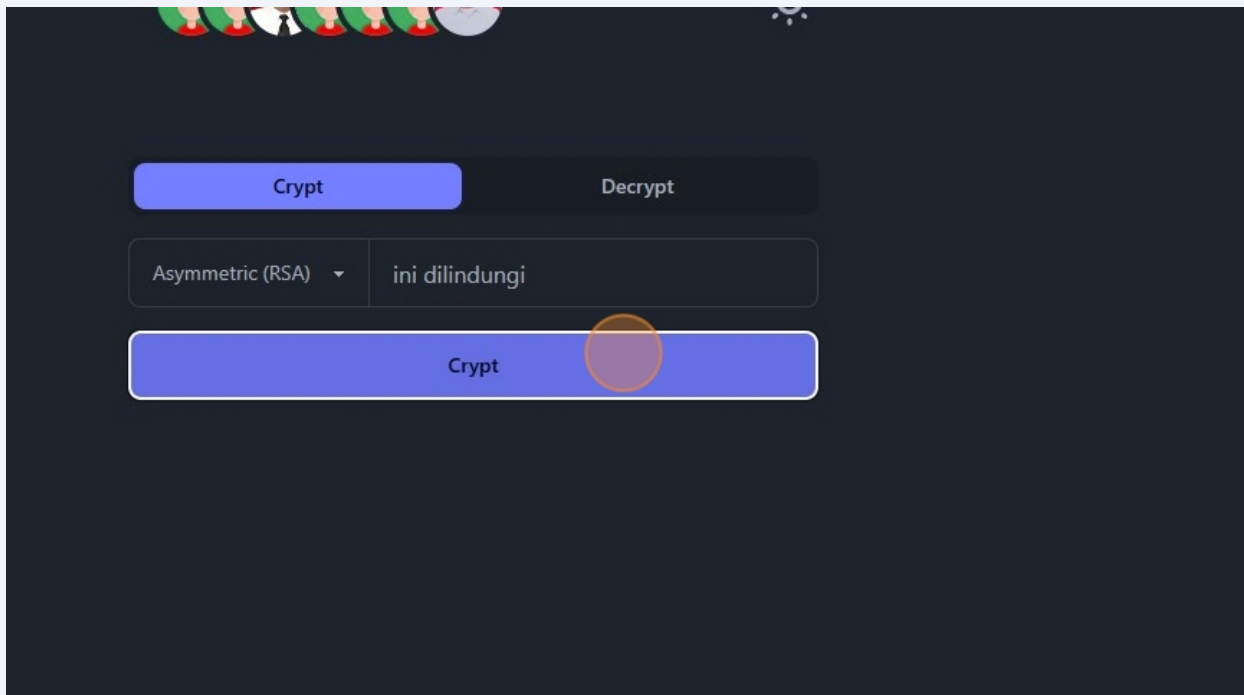
2   Select the "rsa" option.
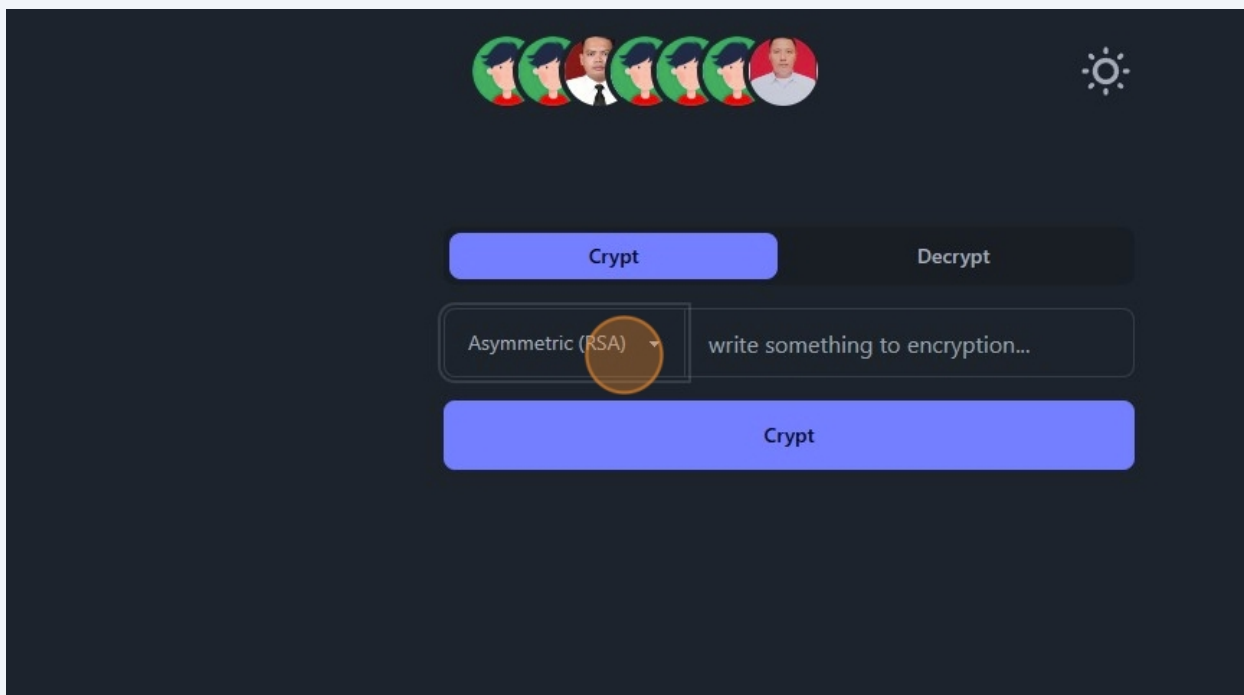
3 Click the "write something to encryption..." field.
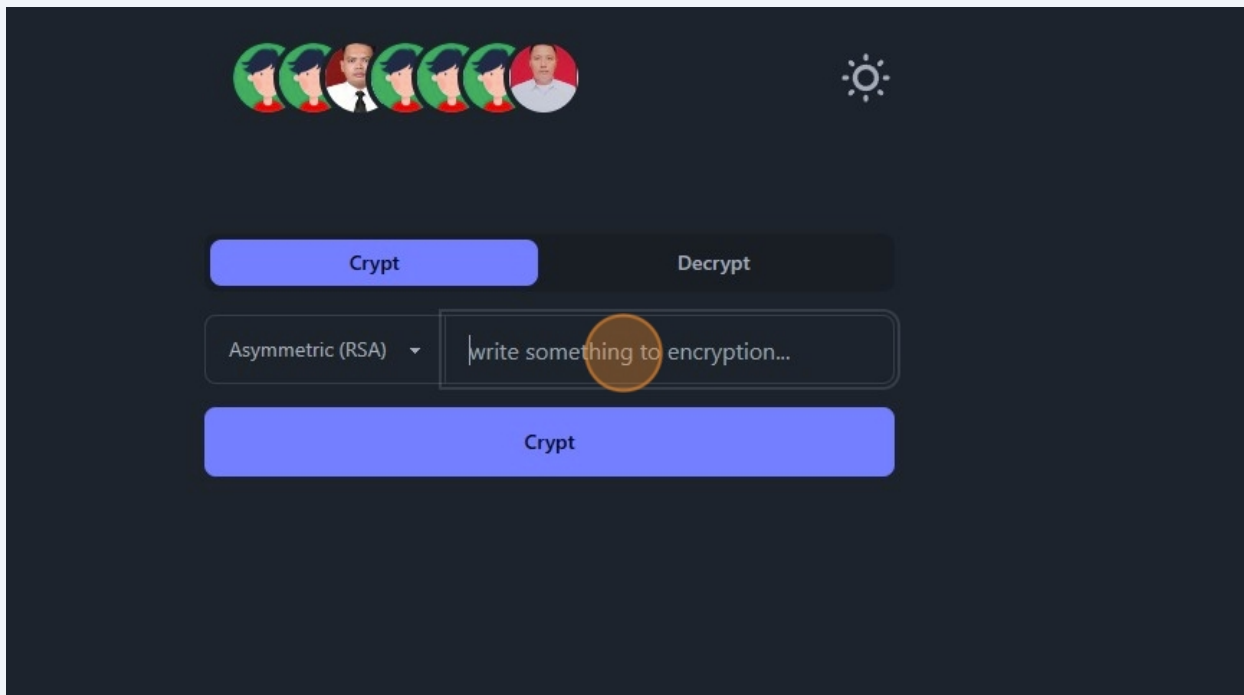
4 Type "ini dilindungi"

5 Click "Crypt"

6 Click "Download"

7 Click "Download"

PKCS OLAP
PKCS#1 OAEP is an asymmetric
cipher based on RSA and the
OAEP padding

Generate ✓
Generate encryption value
using PKCS1_OAEP

Export message ✓
RSA exporting message,
download file
Download

Encryption ✓
Encryption from
[original_value] to
[encryption_value]

8 Click "Decrypt"

Crypt   Decrypt

Reset

Initialize ✓
System will be convert ini
dilindungi
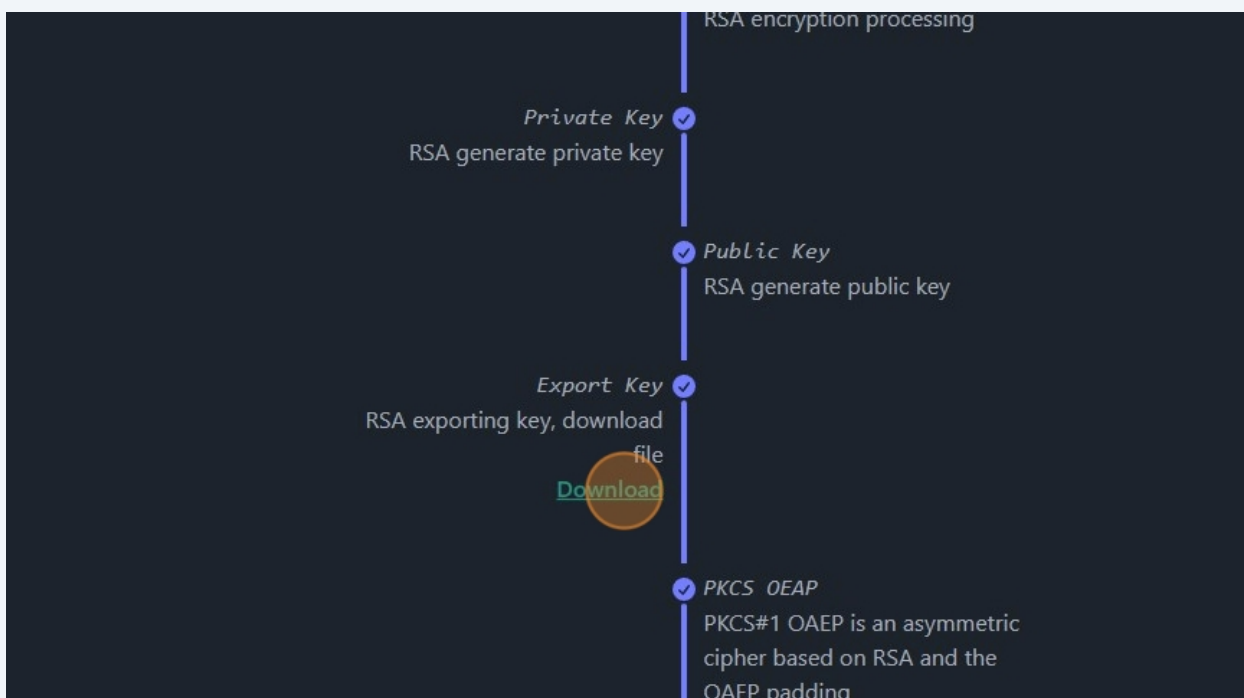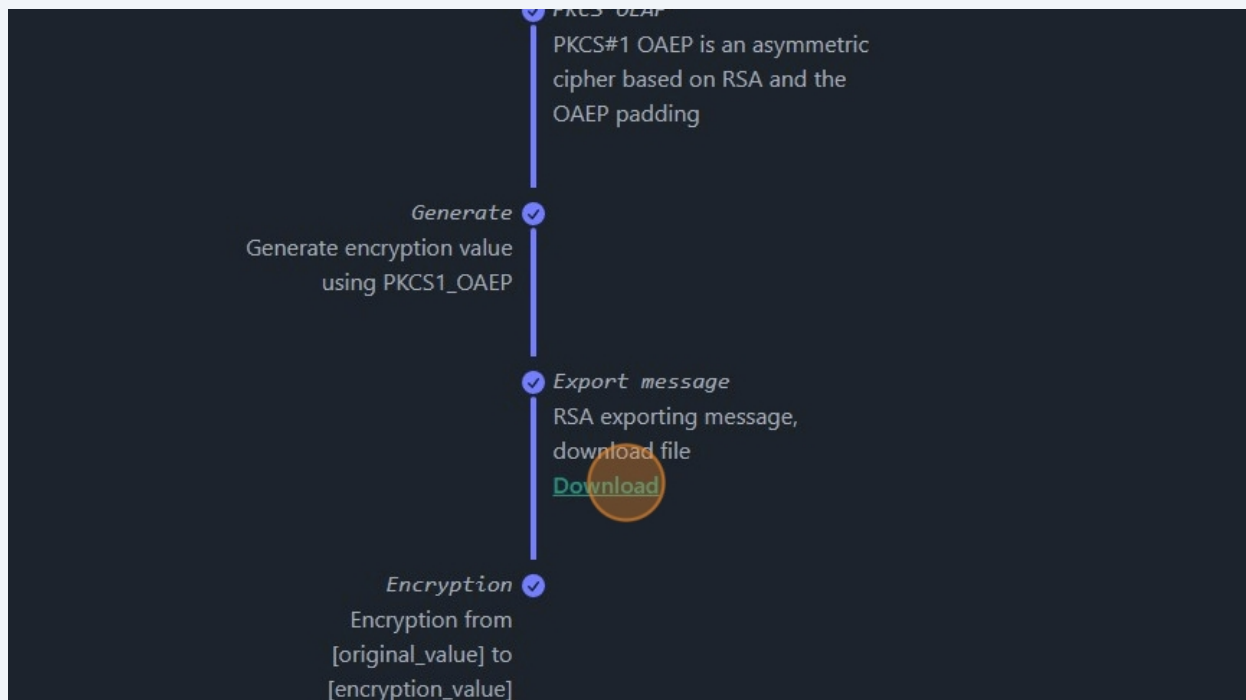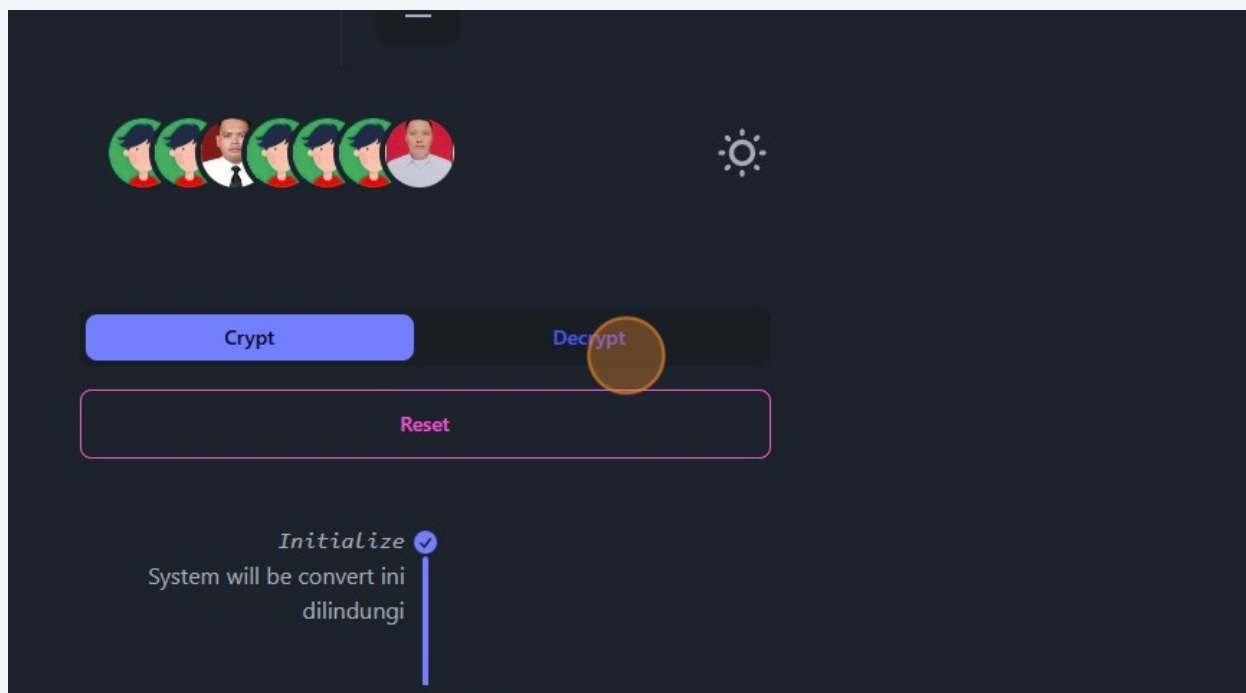
9 Select the "rsa" option.
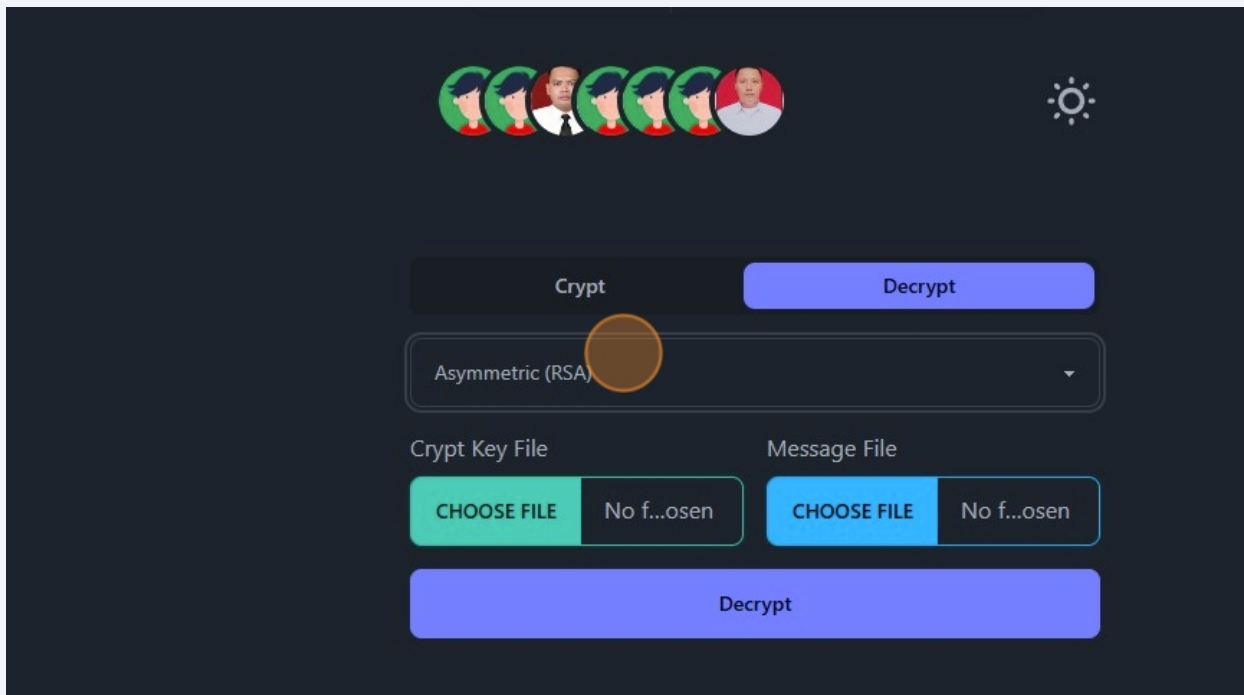
10 Click the "Insert encryption file" field.

11 Click this file field.

Crypt | Decrypt

Asymmetric (RSA)

Crypt Key File
CHOOSE FILE | priv....pem

Message File
CHOOSE FILE | No f...osen

Decrypt

12 Click "Decrypt"

Crypt | Decrypt

Asymmetric (RSA)

Crypt Key File
CHOOSE FILE | priv....pem

Message File
CHOOSE FILE | encr...e.txt
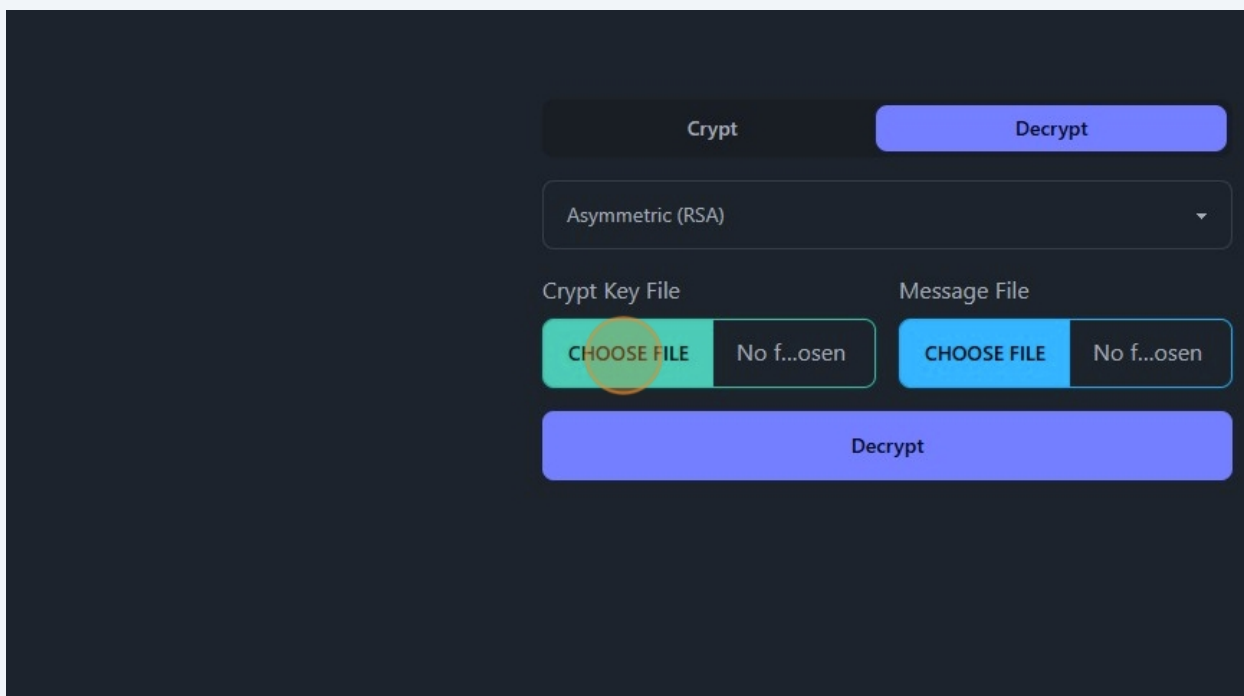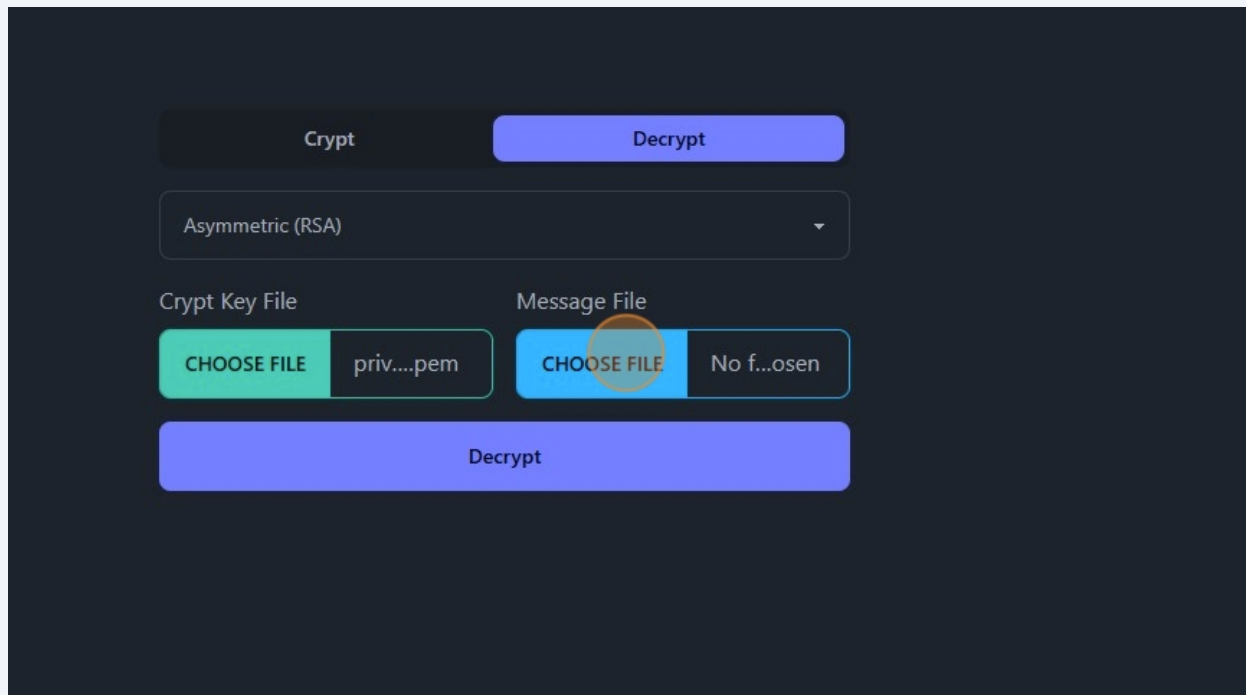
Decrypt
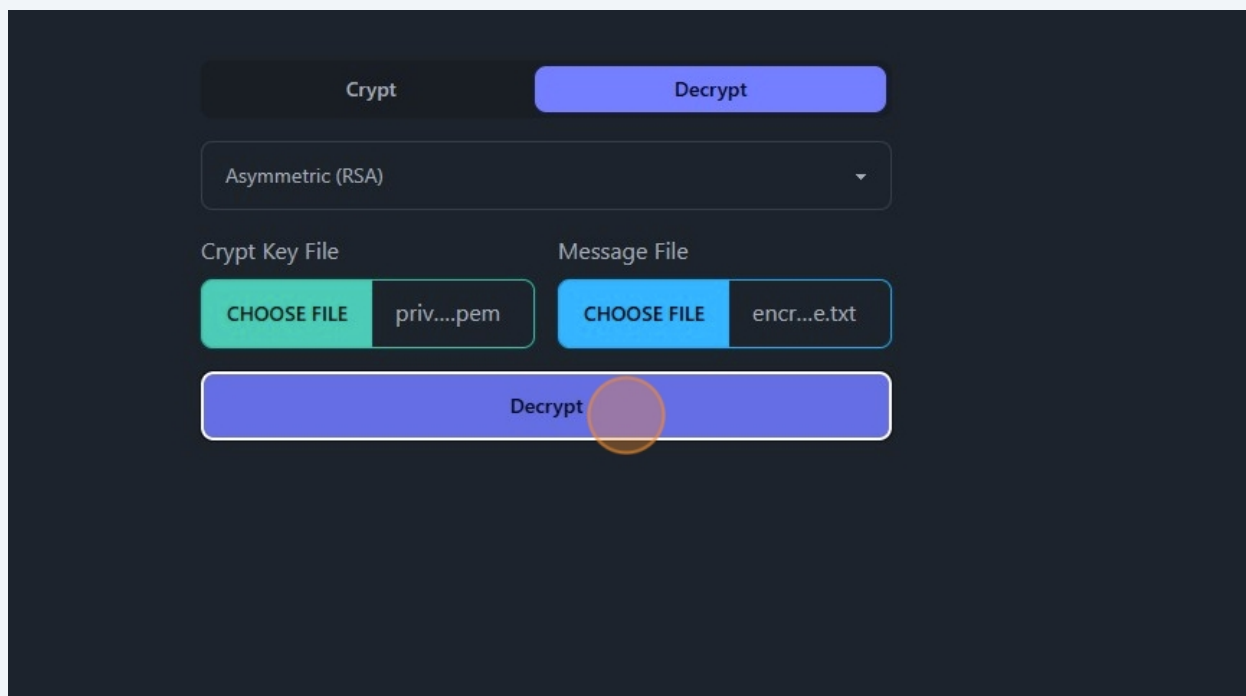
13 Click "Encryption value using aes success, encrypt value is 'ini dilindungi'"