# IMPLEMENTATION OF RSA ALGORITHM

R V S TEJA KRISHNA(17MIS7085)
K VARUN TEJA(17MIS7156)

# INTRODUCTION

- The RSA algorithm enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.
- Public key cryptography also known as Asymmetric cryptography uses two different linked keys – one public and one private keys.
- The public key can be shared with everyone, where as the private key must be kept secret.

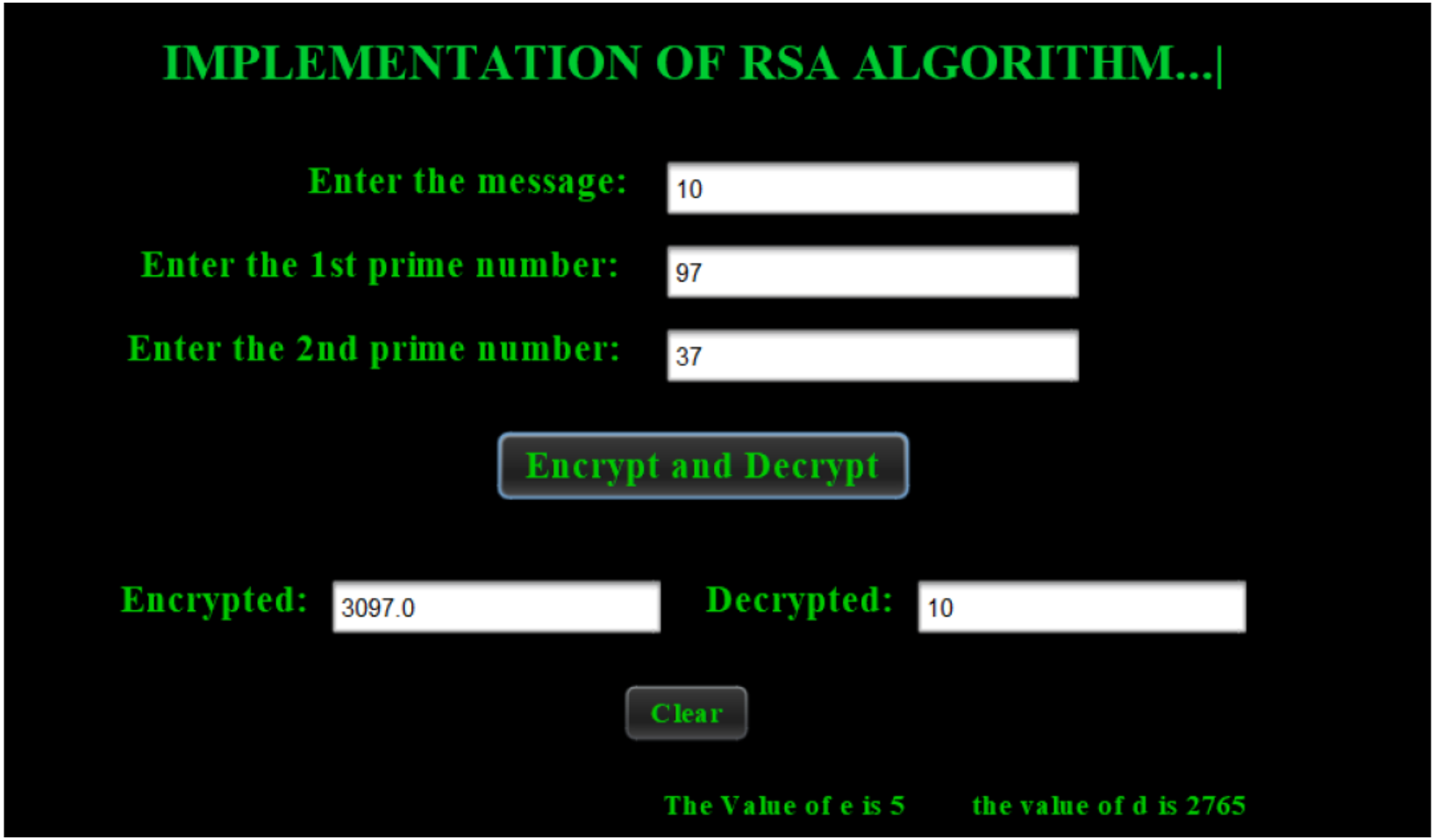
# PROBLEM DEFNITION

- Two large prime numbers, p and q, are generated.
- A modulus n is calculated by multiplying p and q.
- This number is used by both the public and private keys and provides the link between them.
- The public key consists of the modulus n, and a public exponent, e as it’s a prime number that is not too large.
- The e figure doesn’t have to be a secretly selected prime number as the private exponent d, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n.

# METHODOLGY AND PROCEDURE

- Take two large prime numbers p and q.
- Compute their product n. Also compute the Euler function $\Phi(n) = (p - 1)(q - 1)$
- Choose a large random number e ($e > 1$) such that GCD $(e, \Phi(n)) = 1$
- Compute the number d, $1<d< \Phi(n)$ such that $ed \equiv 1 \bmod \Phi(n)$
- Encryption c= (plain text)e mod n
- Decryption p= (cipher text)d mod n

# SCREENSHOT


IMPLEMENTATION OF RSA ALGORITHM...|
Enter the message:
10
Enter the 1st prime number:
97
Enter the 2nd prime number:
37
Encrypt and Decrypt
Encrypted:
3097.0
Decrypted:
10
Clear
The Value of e is 5
the value of d is 2765