

INSTITUTE OF COMPUTER TECHNOLOGY
B-TECH COMPUTER SCIENCE ENGINEERING 2025-26
SUBJECT:-CRYPTOGRAPHY

NAME: Rahul Prajapati

ENRLL NO: 23162171020

BRANCH: CYBER SECURITY

BATCH: 52

PRACTICAL_9

Aim: To understand the fundamentals of Public Key Cryptography by implementing the RSA algorithm for encryption and decryption, where a public key is used to encrypt a user-inputted message and a private key is used to decrypt it back to its original form, displaying both ciphertext and decrypted text in the console.

CODE:

practical9_1.py > is_prime

```
1 def gcd(a, b):
2     while b:
3         a, b = b, a % b
4     return a
5
6 def is_prime(n):
7     if n <= 1:
8         return False
9     if n <= 3:
10        return True
11    if n % 2 == 0 or n % 3 == 0:
12        return False
13    i = 5
14    while i * i <= n:
15        if n % i == 0 or n % (i + 2) == 0:
16            return False
17        i += 6
18    return True
19
20 def modinv(a, m):
21     m0 = m
22     x0, x1 = 0, 1
23     while a > 1:
24         q = a // m
25         a, m = m, a % m
26         x0, x1 = x1 - q * x0, x0
27     if x1 < 0:
28         x1 += m0
29     return x1
30
31 def generate_keypair(p, q):
32     n = p * q
33     phi = (p - 1) * (q - 1)
34     e = 3
35     while gcd(e, phi) != 1:
36         e += 2
37     d = modinv(e, phi)
38     return ((e, n), (d, n))
39
40 def encrypt(public_key, plaintext):
41     e, n = public_key
42     cipher = [pow(ord(char), e, n) for char in plaintext]
43     return cipher
44
45 def decrypt(private_key, ciphertext):
46     d, n = private_key
47     plain = [chr(pow(char, d, n)) for char in ciphertext]
48     return ''.join(plain)
49
```

