Cryptography Project 3

Project 3: - *RSA Implementation*

ADITI ADHIKARY

PES1UG19EC013

6th Semester "A"

CODE: -

RSA.py - C:/Users/aditi/Documents/Semester 6/Cryptography Assignments/RSA.py (3.9.0)

File Edit Format Run Options Window Help

```
import random

def gcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a

def multiplicative_inverse(e, phi):
    d = 0
    x1 = 0
    x2 = 1
    y1 = 1
    temp_phi = phi

    while e > 0:
        temp1 = temp_phi//e
        temp2 = temp_phi - temp1 * e
        temp_phi = e
        e = temp2

        x = x2 - temp1 * x1
        y = d - temp1 * y1

        x2 = x1
        x1 = x
        d = y1
        y1 = y

    if temp_phi == 1:
        return d + phi


def is_prime(num):
    if num == 2:
        return True
    if num < 2 or num % 2 == 0:
        return False
    for n in range(3, int(num**0.5)+2, 2):
        if num % n == 0:
            return False
    return True
```

```python
def generate_key_pair(p, q):
    if not (is_prime(p) and is_prime(q)):
        raise ValueError('Both numbers must be prime.')
    elif p == q:
        raise ValueError('p and q cannot be equal')
    # n = pq
    n = p * q

    # Phi is the totient of n
    phi = (p-1) * (q-1)

    # Choose an integer e such that e and phi(n) are coprime
    e = random.randrange(1, phi)

    # Use Euclid's Algorithm to verify that e and phi(n) are coprime
    g = gcd(e, phi)
    while g != 1:
        e = random.randrange(1, phi)
        g = gcd(e, phi)

    # Use Extended Euclid's Algorithm to generate the private key
    d = multiplicative_inverse(e, phi)

    # Return public and private key_pair
    # Public key is (e, n) and private key is (d, n)
    return ((e, n), (d, n))


def encrypt(pk, plaintext):
    # Unpack the key into it's components
    key, n = pk
    # Convert each letter in the plaintext to numbers based on the character using a^b mod m
    cipher = [pow(ord(char), key, n) for char in plaintext]
    # Return the array of bytes
    return cipher
```

```python
def decrypt(pk, ciphertext):
    # Unpack the key into its components
    key, n = pk
    # Generate the plaintext based on the ciphertext and key using a^b mod m
    aux = [str(pow(char, key, n)) for char in ciphertext]
    # Return the array of bytes as a string
    plain = [chr(int(char2)) for char2 in aux]
    return ''.join(plain)


if __name__ == '__main__':


    p = int(input(" - Enter a prime number (17, 19, 23, etc): "))
    q = int(input(" - Enter another prime number (Not one you entered above): "))

    print(" - Generating your public / private key-pairs now . . .")

    public, private = generate_key_pair(p, q)
    print(" - Your public key is ", public, " and your private key is ", private)

    message = input(" - Enter a message to encrypt with your public key: ")
    encrypted_msg = encrypt(public, message)

    print(" - Your encrypted message is: ", ''.join(map(lambda x: str(x), encrypted_msg)))
    print(" - Decrypting message with private key ", private, " . . .")
    print(" - Your message is: ", decrypt(private, encrypted_msg))
```

<u>OUTPUT</u> :-

```
= RESTART: C:/Users/aditi/Documents/Semester 6/Cryptography Assignments/RSA.py =
 - Enter a prime number (17, 19, 23, etc): 17
 - Enter another prime number (Not one you entered above): 29
 - Generating your public / private key-pairs now . . .
 - Your public key is  (401, 493)  and your private key is  (305, 493)
 - Enter a message to encrypt with your public key: PESUNIVERSITY
 - Your encrypted message is:  3862052196819734586205286219345356106
 - Decrypting message with private key  (305, 493)  . . .
 - Your message is:  PESUNIVERSITY
>>> 
```