

# DAY 3

Q12. Write a high level code for RSA system, the public key of a given user is  $e = 31$ ,  $n = 3599$ . What is the private key of this user?

## PROGRAM:

```
e = 31

n = 3599

def generate_private_key(e, n):

    p = 61

    q = 59

    phi = (p - 1) * (q - 1)

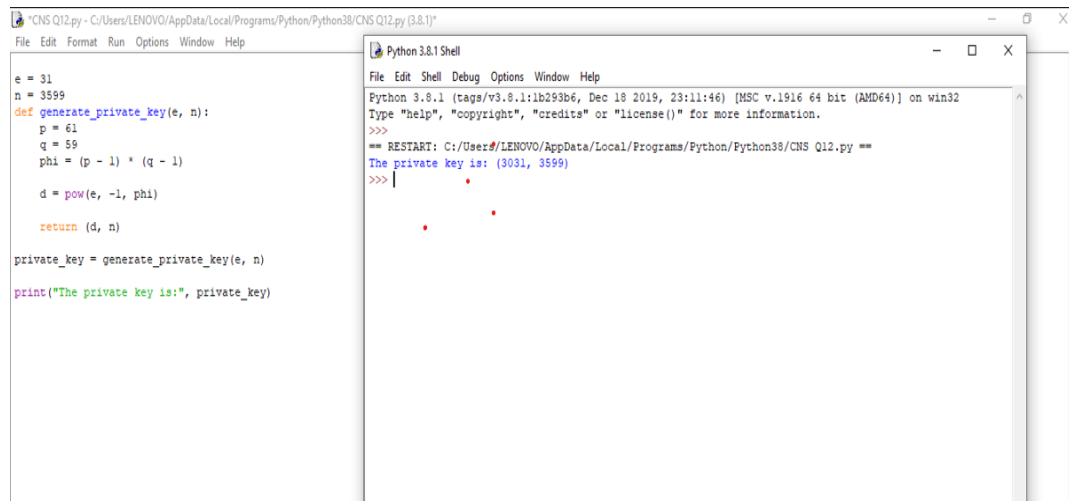
    d = pow(e, -1, phi)

    return (d, n)

private_key = generate_private_key(e, n)

print("The private key is:", private_key)
```

## RESULT:



```
*CNS Q12.py - C:/Users/LENOVO/AppData/Local/Programs/Python/Python38/CNS Q12.py (3.8.1)*
File Edit Format Run Options Window Help

e = 31
n = 3599
def generate_private_key(e, n):
    p = 61
    q = 59
    phi = (p - 1) * (q - 1)
    d = pow(e, -1, phi)
    return (d, n)

private_key = generate_private_key(e, n)

print("The private key is:", private_key)
```

```
Python 3.8.1 Shell
File Edit Shell Debug Options Window Help
Python 3.8.1 (tags/v3.8.1:1b293b6, Dec 18 2019, 23:11:46) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
== RESTART: C:/Users/LENOVO/AppData/Local/Programs/Python/Python38/CNS Q12.py ==
The private key is: (3031, 3599)
>>>
```

Q13. Write a high level code for set of blocks encoded with the RSA algorithm and we don't have the private key. Assume  $n = pq$ ,  $e$  is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with  $n$ . Does this help us in any way?

**PROGRAM:**

```
# Define the public key values

n = 3599 # Assuming n is a composite number

e = 31

# Define a list of encoded blocks

encoded_blocks = [1221, 1335, 1765, 1963, 2345]

# Define a function to check for common factors

def check_common_factor(block):

    # Check if block has a common factor with n

    if n % block == 0:

        # If yes, return True and the common factor

        return True, n // block

    else:

        # If no, return False and None

        return False, None

# Loop through each encoded block

for block in encoded_blocks:

    # Check for common factors

    has_common_factor, factor = check_common_factor(block)

    # If a common factor is found, print the result and exit the loop

    if has_common_factor:

        print("Block {} has a common factor with n: {}".format(block, factor))

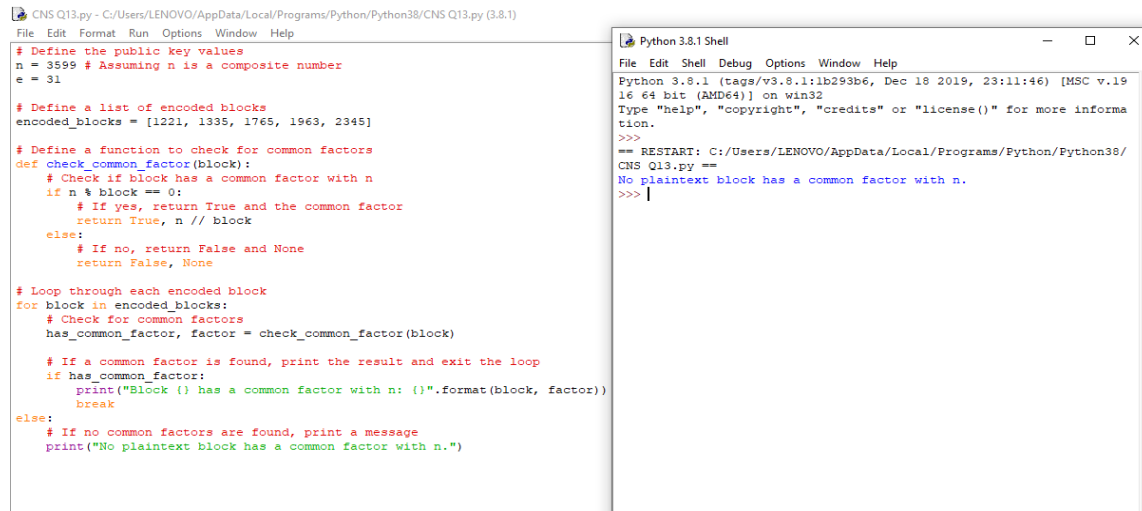
        break
```

else:

# If no common factors are found, print a message

print("No plaintext block has a common factor with n.")

## RESULT:



The image shows a screenshot of a Python script and its execution output. On the left, a text editor window titled 'CNS Q13.py' displays the code. The code defines a function to check for common factors between a block and a number n, and then iterates through a list of encoded blocks to find a common factor. On the right, a 'Python 3.8.1 Shell' window shows the execution output, which includes the restart command and the final message: 'No plaintext block has a common factor with n.'

```
CNS Q13.py - C:/Users/LENOVO/AppData/Local/Programs/Python/Python38/CNS Q13.py (3.8.1)
File Edit Format Run Options Window Help

# Define the public key values
n = 3599 # Assuming n is a composite number
e = 31

# Define a list of encoded blocks
encoded_blocks = [1221, 1335, 1765, 1963, 2345]

# Define a function to check for common factors
def check_common_factor(block):
    # Check if block has a common factor with n
    if n % block == 0:
        # If yes, return True and the common factor
        return True, n // block
    else:
        # If no, return False and None
        return False, None

# Loop through each encoded block
for block in encoded_blocks:
    # Check for common factors
    has_common_factor, factor = check_common_factor(block)

    # If a common factor is found, print the result and exit the loop
    if has_common_factor:
        print("Block {} has a common factor with n: {}".format(block, factor))
        break
else:
    # If no common factors are found, print a message
    print("No plaintext block has a common factor with n.")

Python 3.8.1 Shell
File Edit Shell Debug Options Window Help

Python 3.8.1 (tags/v3.8.1:1b293b6, Dec 18 2019, 23:11:46) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
== RESTART: C:/Users/LENOVO/AppData/Local/Programs/Python/Python38/CNS Q13.py ==
No plaintext block has a common factor with n.
>>>
```