LAB DAY3-CRYPTOGRAPHY AND NETWORK SECURITY

QUESTION:

Q.No.12 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?

CODE:

# Define the public key values

e = 31

n = 3599

# Define a function to calculate the greatest common divisor

def gcd(a, b):

while b != 0:

a, b = b, a % b

return a

# Define a function to calculate the modular multiplicative inverse

def mod\_inv(a, m):

for x in range(1, m):

if (a \* x) % m == 1:

return x

return None

# Calculate phi(n)

phi\_n = 1

for i in range(2, n):

if gcd(i, n) == 1:

phi\_n += 1

# Calculate the private key

d = mod\_inv(e, phi\_n)

# Print the private key

print("Private key:", d)

RESULT:

OUTPUT: private key is 3031

QUESTION 13:

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?

CODE:

# 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.")

OUTPUT:

No plaintext block has a common factor with n