TW2: RSA Algorithm

**Instructions:** (Put Instruction)

|  |
| --- |
| import random  import math  # Function to check if a number is prime  def is\_prime(num):  if num <= 1:  return False  for i in range(2, int(math.sqrt(num)) + 1):  if num % i == 0:  return False  return True  # Function to generate random prime numbers  def generate\_prime(bits):  while True:  num = random.getrandbits(bits)  if is\_prime(num):  return num  # Function to compute the greatest common divisor (GCD)  def gcd(a, b):  while b:  a, b = b, a % b  return a |
| # Function to find the modular multiplicative inverse  def mod\_inverse(a, m):  m0, x0, x1 = m, 0, 1  while a > 1:  q = a // m  m, a = a % m, m  x0, x1 = x1 - q \* x0, x0  return x1 + m0 if x1 < 0 else x1  # Function to generate RSA key pairs  def generate\_key\_pair(bits):  p = generate\_prime(bits)  q = generate\_prime(bits)  n = p \* q  phi = (p - 1) \* (q - 1)  while True:  e = random.randint(2, phi - 1)  if gcd(e, phi) == 1:  break  d = mod\_inverse(e, phi)  public\_key = (n, e)  private\_key = (n, d)  return public\_key, private\_key  # Function to encrypt a message  def encrypt(public\_key, message):  n, e = public\_key  cipher\_text = [pow(ord(char), e, n) for char in message]  return cipher\_text |
| # Function to decrypt a message  def decrypt(private\_key, cipher\_text):  n, d = private\_key  decrypted\_message = ''.join([chr(pow(char, d, n)) for char in cipher\_text])  return decrypted\_message  # Main program  if \_\_name\_\_ == "\_\_main\_\_":  bits = 8 # Adjust the number of bits for your desired security level  public\_key, private\_key = generate\_key\_pair(bits)  print(f" Generated Public Key : {public\_key} \n Generated Private Key : {private\_key}")  message = eval(input(" Enter the Message to be Encrypted : "))  print(" Original message:", message)  encrypted\_message = encrypt(public\_key, message)  print(" Encrypted message:", encrypted\_message)  decrypted\_message = decrypt(private\_key, encrypted\_message)  print(" Decrypted message:", decrypted\_message) |
|  |

TW3: UDP Connectionless Transport

**Instructions:** (Put Instruction)

|  |
| --- |
| **#UDP Server Code**  import socket  # Create a UDP socket  server\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)  # Bind the socket to an address and port  server\_address = ('localhost', 12345)  server\_socket.bind(server\_address)  print('UDP server is waiting for messages...')  while True:  # Receive data from the client  data, client\_address = server\_socket.recvfrom(1024)  print(f'Received message from {client\_address}: {data.decode()}')  # Close the socket (this will never be reached in this example)  server\_socket.close() |
| **UDP Client Code**  import socket  # Create a UDP socket  client\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)  # Server address and port  server\_address = ('localhost', 12345)  while True:  message = input('Enter a message: ')  # Send data to the server  client\_socket.sendto(message.encode(), server\_address)  # Close the socket (this will never be reached in this example)  client\_socket.close() |

**Note: A separate Terminals need to be opened for Server and Client**

|  |
| --- |
|  |
|  |

TW4: TCP Connection-Oriented Transport

**Instructions:** (Put Instruction)

|  |
| --- |
| **# TCP Server Code**  import socket  # Define the server address and port  server\_address = ('127.0.0.1', 12345)  # Create a socket object  server\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)  # Bind the socket to the server address and port  server\_socket.bind(server\_address)  # Listen for incoming connections  server\_socket.listen(4)  print("Server is listening for incoming connections...")  # Accept a connection  client\_socket, client\_address = server\_socket.accept()  print(f"Connected to {client\_address}")  # Receive data from the client  data = client\_socket.recv(1024)  print(f"Received data from client: {data.decode('utf-8')}")  # Send a response to the client  response = "Hello, client!"  client\_socket.send(response.encode('utf-8'))  # Close the sockets  client\_socket.close()  server\_socket.close() |
| **# TCP Client Code**  import socket  # Define the server address and port  server\_address = ('127.0.0.1', 12345)  # Create a socket object  client\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)  # Connect to the server  client\_socket.connect(server\_address)  # Send a message to the server  message = "Hello, server!"  client\_socket.send(message.encode('utf-8'))  # Receive a response from the server  data = client\_socket.recv(1024)  print(f"Received response from server: {data.decode('utf-8')}")  # Close the socket  client\_socket.close() |

**Note: A separate Terminals need to be opened for Server and Client**

|  |
| --- |
|  |
|  |