Assignment No : 4 - Implementation of RSA Cryptosystem for Secure Communication Between Client and Server Using Python

Introduction

In modern communication systems, securing data transmission between a client and a server is critical. One widely used cryptographic algorithm for ensuring secure communication is the RSA (Rivest-Shamir-Adleman) Cryptosystem. This public-key encryption method allows secure data transmission without prior key exchange, making it ideal for online communications.

RSA Algorithm

The RSA algorithm consists of three major steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation

1. Choose two large prime numbers p and q.
2. Compute $n = p \times q$.
3. Compute Euler's totient function $\varphi(n) = (p-1) \times (q-1)$.
4. Select a public exponent e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
5. Compute the private key d, the modular inverse of e modulo $\varphi(n)$.

Example RSA Problem

Given: p = 11, q = 17, e = 13, and Message M = 25

Step 1: Compute n and $\varphi(n)$

$n = 11 \times 17 = 187$
$\varphi(n) = (11-1) \times (17-1) = 10 \times 16 = 160$

Step 2: Compute d using the Extended Euclidean Algorithm OR Modular Multiplicative Inverse Method.

This is the calculation for finding the multiplicative inverse of **13 mod 160** using the Extended Euclidean Algorithm:

n	b	q	r	t1	t2	t3
160	13	12	4	0	1	-12
13	4	3	1	1	-12	37
4	1	4	0	-12	37	-160

Answer

So t = 37.

Now we still have to apply mod n to that number: 37 mod 160 ≡ 37

So the multiplicative inverse of 13 modulo 160 is 37.

multiplicative inverse of **13 mod 160** using the Extended Euclidean Algorithm: d = 37

Step 3: Encrypt the Message

C = 25^13 mod 187 = 106

Step 4: Decrypt the Ciphertext

M = 106^37 mod 187 = 25

Conclusion

This implementation successfully establishes secure communication between a client and a server using the RSA cryptosystem. The Python program generates RSA keys, encrypts messages on the client side, and decrypts messages on the server side. This demonstrates the practical application of RSA in securing client-server communication.

Solve the following five problems as lab assignments. Include the provided write-up above. Use the multiplicative inverse with the Extended Euclidean Algorithm to compute d (the private key).

Given	P	Q	E (Public Key)	D (Private Key)	M Message	C (Cipher Text)
1.	**11**	**17**	**7**		**45**	
2.	**13**	**19**	**11**		**32**	
3.	**23**	**29**	**17**		**51**	
4.	**31**	**37**	**13**		**27**	
5.	**41**	**17**	**23**		**63**	