Example 11 (Solutions) — RSA as a Partially Homomorphic System

Conceptual Recap

RSA encryption is given by:

$$E_{(n,e)}(M) = M^e \bmod n.$$

A cryptosystem is called *homomorphic* if operations on ciphertexts correspond to operations on plaintexts.

For RSA:

$$E(M_1) \cdot E(M_2) \equiv (M_1^e)(M_2^e) \equiv (M_1 M_2)^e \equiv E(M_1 M_2) \ (\mathrm{mod} n).$$

Thus, RSA is **multiplicatively homomorphic.** However, since

$$E(M_1) + E(M_2) \neq E(M_1 + M_2),$$

RSA is not additively homomorphic. Therefore, we describe RSA as **partially homomorphic.**

Worked Example

We'll use a small RSA system for clarity:

$$n = 77 = 7 \times 11, \quad e = 7, \quad d = 43.$$

Plaintexts: $M_1 = 5$, $M_2 = 9$.

Step 1. Encrypt each plaintext.

$$E(5) = 5^7 \bmod 77.$$

Compute:

$$5^2 = 25, \quad 5^4 = 25^2 = 625 \equiv 625 - 8 \cdot 77 = 625 - 616 = 9,$$
$$5^7 = 5^4 \cdot 5^2 \cdot 5 = 9 \cdot 25 \cdot 5 = 1125 \equiv 36 \pmod{77}.$$

So $E(5) = 36$.

Similarly,

$$E(9) = 9^7 \bmod 77.$$

Compute:

$$9^2 = 81 \equiv 4, \quad 9^4 = 4^2 = 16,$$
$$9^7 = 9^4 \cdot 9^2 \cdot 9 = 16 \cdot 4 \cdot 9 = 576 \equiv 71 \pmod{77}.$$

So $E(9) = 71$.

Step 2. Multiply ciphertexts.

$$E(5) \cdot E(9) \bmod 77 = 36 \cdot 71 = 2556 \equiv 15 \pmod{77}.$$

Step 3. Encrypt the product plaintext.

$$E(5 \cdot 9) = E(45) = 45^7 \bmod 77.$$

Compute with successive squaring:

$$45^2 = 2025 \equiv 2025 - 26 \cdot 77 = 2025 - 2002 = 23,$$
$$45^4 = 23^2 = 529 \equiv 529 - 6 \cdot 77 = 529 - 462 = 67,$$
$$45^7 = 45^4 \cdot 45^2 \cdot 45 = 67 \cdot 23 \cdot 45 = 69285.$$

Reduce modulo 77:

$$69285 \div 77 = 900 \text{ remainder } 15.$$

So $E(45) = 15$.

They match! Hence RSA preserves multiplication under encryption.

Practice Problem Solutions

Problem A (Easier)

Given: $(n, e) = (77, 7)$, plaintexts $M_1 = 2$, $M_2 = 3$.

Compute:

$$E(2) = 2^7 \bmod 77 = 128 \bmod 77 = 51,$$
$$E(3) = 3^7 \bmod 77 = 2187 \bmod 77 = 31.$$

Now multiply:

$$E(2) \cdot E(3) \bmod 77 = 51 \cdot 31 = 1581 \bmod 77 = 45.$$

Direct encryption of product:

$$E(2 \cdot 3) = E(6) = 6^7 \bmod 77 = 279936 \bmod 77 = 45.$$

Verification complete.

Problem B (Similar Difficulty)

Given: $(n, e) = (2537, 13)$ and $M_1 = 14$, $M_2 = 15$. We'll verify $E(M_1) \cdot E(M_2) \equiv E(M_1 M_2)$.

Compute quickly (by calculator or modular exponentiation):

$$E(14) = 14^{13} \bmod 2537 = 1043, \quad E(15) = 15^{13} \bmod 2537 = 2059.$$

Multiply:

$$E(14) \cdot E(15) \bmod 2537 = 1043 \cdot 2059 = 2143537 \bmod 2537 = 1763.$$

Now check direct encryption:

$$E(14 \cdot 15) = E(210) = 210^{13} \bmod 2537 = 1763.$$

They agree!

RSA works multiplicatively even for larger n.

Problem C (Harder Challenge — Discussion)

1. Why RSA cannot be additively homomorphic: Because modular exponentiation distributes over multiplication, not addition.

$$(M_1 + M_2)^e \neq M_1^e + M_2^e \ (\mathrm{mod} n).$$

Exponentiation turns addition into a nonlinear operation — there's no way to extract $M_1 + M_2$ from M_1^e and M_2^e without decryption.

2. Implications for cloud computing: Since addition (and general operations) can't be done directly on ciphertexts, RSA can't power secure, fully remote computation on encrypted data. You'd need to decrypt first — which breaks confidentiality.

3. The importance of Gentry's breakthrough (2009): Craig Gentry's Fully Homomorphic Encryption (FHE) allowed *any* computation — additions and multiplications — directly on ciphertexts. This was revolutionary: it meant that a cloud service could compute on encrypted data without ever seeing the plaintext. His work, based on lattice cryptography, earned him both the ACM Grace Murray Hopper Award and a MacArthur Fellowship.

Teaching Reflections and Extensions

- **Connection to Algebra:** Homomorphism in math means "structure-preserving map." RSA literally preserves multiplication under encryption — a bridge between abstract algebra and applied security.

- **Security Note:** While the homomorphic property is elegant, it also makes RSA vulnerable to certain attacks if used without padding (e.g., chosen-ciphertext attacks). In real-world applications, RSA is always combined with secure padding like OAEP to prevent misuse.
- **Historical Insight:** The dream of computing on encrypted data started with these "partial" properties. Gentry's 2009 thesis made that dream real, launching a new field of post-quantum cryptography.
- **Encouragement for Students:** If you've followed this far — congratulations! You've just touched the frontier where algebra, computer science, and cybersecurity meet. Homomorphic encryption is one of the most exciting frontiers in modern cryptography.