Example 10 — Signing a Message with RSA

Scenario: Alice's public RSA cryptosystem uses $n = 43 \times 59 = 2537$ and $e = 13$. Her private key is $d = 937$, as computed in Example 9. She wishes to send the message "MEET AT NOON" to her friends so that they are *certain* it came from her.

Goal: Learn how RSA can be used to *sign* a message—proving authenticity, not just secrecy.

Step 1 — Translate the message into numbers

Using the standard letter-number system (A=00, B=01, ..., Z=25):

$$M = \text{MEET AT NOON} \Rightarrow 1204\ 0419\ 0019\ 1314\ 1413$$

(Verify this translation carefully! It's essential to the encryption and decryption process.)

Step 2 — Apply Alice's *private key* to each block

Alice uses her private key $d = 937$ to compute:

$$x^{937} \pmod{2537}$$

for each message block x. This operation produces a "digital signature" that can only be generated with Alice's private key.

Step 3 — Compute the results (with modular exponentiation)

Using fast modular exponentiation (as in Example 9):

$$\begin{aligned}
1204^{937} &\equiv 817 \pmod{2537} \\
0419^{937} &\equiv 555 \pmod{2537} \\
0019^{937} &\equiv 1310 \pmod{2537} \\
1314^{937} &\equiv 2173 \pmod{2537} \\
1413^{937} &\equiv 1026 \pmod{2537}
\end{aligned}$$

So, the message Alice sends (in blocks) is:

$$0817\ 0555\ 1310\ 2173\ 1026$$

Step 4 — Verification by the recipient

When her friends receive the message, they apply Alice's *public key* $e = 13$ to each block:

$$E_{(2537,13)}(c) = c^{13} \pmod{2537}$$

This reverses Alice's signature and recovers the plaintext. If the recovered message reads "MEET AT NOON," they know it truly came from Alice.

Key takeaway

Digital signatures use the *private key to sign* and the *public key to verify.* This is the opposite direction from encryption (where public encrypts and private decrypts). It guarantees message authenticity and integrity — no one else could have produced this result.

Practice — Your Turn!

Problem A (Warm-up): Alice's key is $n = 77$, $e = 13$, and $d = 37$. She wants to sign the message "HI," represented as 0708. Compute the signature block $c = m^d \pmod{77}$. Then, verify that $c^e \pmod{77}$ returns 0708.

Problem B (Moderate): Bob uses the same RSA parameters as Example 10: $n = 2537$, $e = 13$, $d = 937$. He signs the message "HELP" (encoded as 0704 1115). Compute $m^d \pmod{2537}$ for each block, and verify correctness.

Problem C (Challenge): Suppose Eve intercepts Alice's public key $(2537, 13)$ and one of her signed messages. Why can't Eve "fake" Alice's signature without knowing $d = 937$? Use your understanding of modular arithmetic and factorization to explain the barrier to forgery.

Reflection: Describe in your own words how digital signatures strengthen security compared to regular RSA encryption.

Quick Tips:

- Public key (n, e) — used to verify or encrypt.
- Private key d — used to sign or decrypt.
- Large primes p, q make $n = pq$ hard to factor, ensuring security.
- Modular arithmetic is your shield: it keeps numbers within manageable limits.