Example 10 (Solutions) — RSA Digital Signatures

Quick reminders

- Letter↔number map (used by the text): A→00, B→01, ..., I→08, J→09, ..., Z→25.
- Make fixed-size blocks so each block m satisfies $0 \le m < n$.
- **Sign** one block: $s \equiv m^d \pmod{n}$. **Verify**: $m' \equiv s^e \pmod{n}$; accept iff $m' = m$.
- **Fast modular exponentiation (square–and–multiply)** is the tool for computing $a^b \bmod n$ efficiently.

Textbook walkthrough (signature for "MEET AT NOON")

Public key $(n, e) = (2537, 13)$ and private key $d = 937$ (from Ex. 9). Blocks of the message (using A=00,...,Z=25): 1204 0419 0019 1314 1413.

Signer (Alice) computes the signature blocks

$$s_i \equiv m_i^d \pmod{2537}.$$

With fast modular exponentiation (or a calculator), this yields

$$\boxed{0817\ 0555\ 1310\ 2173\ 1026}.$$

Verifier (anyone) checks

$$m_i' \equiv s_i^e \pmod{2537}.$$

Raising each block above to the 13th power modulo 2537 gives back

$$1204\ 0419\ 0019\ 1314\ 1413,$$

which matches Alice's original blocks, so the signature is *valid*. Because only the holder of d can produce blocks that verify under e, recipients are convinced the message came from Alice.

Practice Solutions

Problem A (easier)

Task. With $(n, e, d) = (77, 13, 37)$, sign the message `HI` and verify.

Block set-up. Since $n = 77 < 100$, we must use *two-digit* blocks:

$$\texttt{HI} \longrightarrow 07\ 08 \quad (\text{A} = 00, \ldots, \text{I} = 08).$$

Sign each block: $s \equiv m^{37} \pmod{77}$.

$\underline{m = 07}$. Write $37 = 32 + 4 + 1$. Square–and–multiply (all mod 77):

$$7^1 = 7, \quad 7^2 = 49, \quad 7^4 = 14, \quad 7^8 = 42, \quad 7^{16} = 70, \quad 7^{32} = 49.$$

So $7^{37} \equiv 7^{32} \cdot 7^4 \cdot 7 \equiv 49 \cdot 14 \cdot 7 \equiv 28 \pmod{77}$.

$\underline{m = 08}$. Powers (mod 77):

$$8^1 = 8,\ 8^2 = 64,\ 8^4 = 15,\ 8^8 = 71,\ 8^{16} = 36,\ 8^{32} = 64.$$

Hence $8^{37} \equiv 8^{32} \cdot 8^4 \cdot 8 \equiv 64 \cdot 15 \cdot 8 \equiv 57 \pmod{77}$.

Signature blocks: $\boxed{28\ 57}$.

Verify: compute $m' \equiv s^{13} \pmod{77}$. One can reuse the tables above or a calculator:

$$28^{13} \equiv 7 \pmod{77} \quad \text{and} \quad 57^{13} \equiv 8 \pmod{77}.$$

Thus we recover 07 08 $\Rightarrow$ `HI`. ✓

Problem B (similar)

Task. With $(n, e, d) = (2537, 13, 937)$, sign `OK` and verify.

Blocks. $n = 2537$ allows 4-digit blocks. `OK` $\to$ 14 10 $\Rightarrow m = 1410$.

Sign: $s \equiv 1410^{937} \pmod{2537} = \boxed{0802}$.

Verify: $s^{13} \equiv 802^{13} \equiv 1410 \pmod{2537} \Rightarrow$ back to `OK`. ✓

(Computation notes.) A short binary-exponent table for $1410^{2^k} \bmod 2537$ plus multiply on 1-bits of 937 (binary $= 1110101001_2$) reproduces the result efficiently; a CAS or Python also confirms 802.

Problem C (harder)

Task. Using public key $(2537, 13)$, check whether the claimed signature

$$\boxed{0817\ 0555\ 1310\ 2173\ 1026}$$

matches the message "`MEET AT NOON`".

Verification. Raise each s_i to the 13th power mod 2537:

$$0817^{13} \equiv 1204,\ 0555^{13} \equiv 0419,\ 1310^{13} \equiv 0019,\ 2173^{13} \equiv 1314,\ 1026^{13} \equiv 1413 \pmod{2537}.$$

These are exactly the blocks for "MEET AT NOON," so the signature is valid. *If even one block failed to match, we would reject the signature immediately.*

Teaching notes, tips, and gotchas (for review)

- **Block sizing matters.** Always choose the largest even number of digits so each block m is $< n$. Small n (like 77) means 2-digit blocks; $n = 2537$ allows 4-digit blocks.
- **Signature vs. encryption.** Sign with the *private* exponent d; anyone verifies with the *public* exponent e. (Encrypting for secrecy goes the other way.)
- **Square–and–multiply** is your friend: precompute $a^1, a^2, a^4, a^8, \ldots$ mod n and multiply the powers that correspond to 1-bits of the exponent.
- **Common mistakes:**
  - Mixing the A=0 mapping (00–25) with A=1. Stick to A=00,...,Z=25 for RSA in this section.
  - Building a block $\geq n$. If that happens, reduce the block size.
  - Forgetting leading zeros when translating back (e.g., 0419 not 419).