Example 8 — Encrypting with the RSA Cryptosystem

Given: Key $(n, e) = (2537, 13)$, message `STOP`.

Step 1 — Convert to numerical form

$$\texttt{S T O P} \to 18\ 19\ 14\ 15$$

Group into blocks of four digits (since $2525 < 2537 < 252525$):

$$1819 \quad 1415.$$

Step 2 — Apply RSA encryption

RSA uses:

$$c \equiv m^{13} \pmod{2537}.$$

Compute each block using fast modular exponentiation (square-and-multiply):

$$\begin{aligned} 1819^{13} &\equiv ((1819^2 \bmod 2537)^6 \times 1819) \bmod 2537 \\ &\equiv (1390^6 \times 1819) \bmod 2537 \\ &\equiv 2081, \\ 1415^{13} &\equiv 2182. \end{aligned}$$

Encrypted message: $\boxed{2081\ 2182}$.

Verification (optional)

If we compute the private key d satisfying

$$ed \equiv 1 \pmod{(p-1)(q-1)} = 1 \pmod{42 \times 58 = 2436},$$

we find $d = 937$. Decryption would be $m \equiv c^{937} \pmod{2537}$, recovering the original `STOP`.

Why it works

Because of Euler's theorem:

$$m^{\varphi(n)} \equiv 1 \pmod{n}, \quad \text{where } \varphi(n) = (p-1)(q-1),$$

and since $ed \equiv 1 \pmod{\varphi(n)}$, we have:

$$(m^e)^d \equiv m^{ed} \equiv m \pmod{n}.$$

That's the mathematical backbone of RSA.

Common pitfalls

- Forgetting that `A=00` (not 1). Off-by-one ruins all blocks.
- Using too large a block size (must keep $m < n$).
- Mismanaging modular exponentiation — use reduction at each step!

Practice Solutions

Problem A. Encrypt `GO` with $(2537, 13)$. `G O` → 06 14 ⇒ 0614. Compute $0614^{13} \bmod 2537 = 1097$. $\boxed{1097}$

Problem B. Encrypt `HELP` with $(2537, 13)$. `H E L P` → 07 04 11 15 ⇒ 0704, 1115.

$$0704^{13} \bmod 2537 = 1954, \quad 1115^{13} \bmod 2537 = 1730.$$

$\boxed{1954\ 1730}$

Problem C. Encrypt `SAVE THE PLANET`. Break into 4-digit blocks and repeat; results will vary depending on spacing method.

$$\boxed{Eachblockencryptedvia} c_i = m_i^{13} \pmod{2537}.$$

(For longer strings, an algorithmic approach or Python helper script is recommended.)

Historical Spotlight — Clifford Cocks, the Hidden Father of RSA

Clifford Cocks (born 1950, Cheshire, England) quietly invented what we now call the **RSA cryptosystem** in 1973 — three years before Rivest, Shamir, and Adleman. Working for Britain's Government Communications Headquarters (GCHQ), he realized that public key cryptography could be built on the difficulty of reversing multiplication of large primes.

However, his discovery remained classified until 1997. For over two decades, the world credited RSA to the MIT trio, unaware that Cocks had already found the same mathematical structure. When his work was declassified, the cryptographic community celebrated him as a humble genius — the mathematician who built a revolution and quietly went back to work.

Today, the core of his insight powers nearly all digital security: secure emails, credit card transactions, and even the HTTPS padlock on your browser.

Fun fact: Cocks also developed early ideas for identity-based encryption — letting your name or email serve as part of a public key!

Teacher Reflection. This example unites number theory, modular arithmetic, and human ingenuity. Encourage students to appreciate both the mathematics *and* the people who dared to imagine a new kind of secrecy — one where publishing your key could actually make you safer.