Example 8 (Worksheet) — Encrypting with the RSA Cryptosystem

Goal. Encrypt the message `STOP` using the RSA cryptosystem with key $(n, e) = (2537, 13)$.

Background idea

RSA is a **public key cryptosystem**. Anyone can use the public key (n, e) to encrypt, but only the private key (involving d) can decrypt. Each letter is first turned into a number (A=00, B=01, ..., Z=25), grouped into blocks that fit under n, and then encrypted using

$$c \equiv m^e \pmod{n}.$$

Step 1 — Convert letters to numbers

We map `STOP` as:

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

Group into four-digit blocks:

$$1819 \quad 1415$$

(because $2525 < 2537 < 252525$, so 4 digits per block fits safely).

Step 2 — Apply RSA encryption

For each block m, compute

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

You can use fast modular exponentiation (successive squaring) to simplify:

$$1819^{13} \pmod{2537} = 2081, \qquad 1415^{13} \pmod{2537} = 2182.$$

Hence, the ciphertext is:

$$\boxed{\texttt{2081 2182}}.$$

Step 3 — Interpretation

We transmit `2081 2182`. Only someone with the private key d (that satisfies $ed \equiv 1 \pmod{(p-1)(q-1)}$) can decrypt the message.

Tips & tricks

- **Why 13?** — Because $\gcd(13, (p-1)(q-1)) = 1$, ensuring encryption is reversible.
- **Always check block size.** m must be smaller than n.
- **Decryption uses the inverse of** e — It "undoes" the exponentiation by modular arithmetic symmetry.
- **RSA loves primes.** Choosing p, q large keeps n hard to factor.

Practice — Your Turn

Problem A (easier). Encrypt `GO` using RSA with $(n, e) = (2537, 13)$. Hint: Convert `GO` $\rightarrow$ 06014 $\rightarrow$ use 4-digit block 0601, compute $c \equiv m^{13} \pmod{2537}$.

Problem B (similar). Encrypt `HELP` using RSA with $(n, e) = (2537, 13)$. Show all modular exponentiation steps clearly.

Problem C (challenge). Encrypt `SAVE THE PLANET` using RSA with $(n, e) = (2537, 13)$. Break your message into 4-digit blocks and compute each ciphertext block. (Hint: spaces can be ignored or replaced by 26.)

Reflection. In one or two sentences, explain *why* RSA's security depends on factoring large primes.