Example 9 (Worksheet) — RSA Decryption (work the process, not just the answer)

Problem. We receive the ciphertext blocks `0981 0461` produced by the RSA cryptosystem from Example 8. The public key was $(n, e) = (2537, 13)$ with $n = 43 \cdot 59$. Decrypt the message.

The big idea (the why)

RSA works in blocks. If a block c was encrypted with $c \equiv m^e \pmod{n}$, then anyone who knows the *private* exponent d (the inverse of e mod $\phi(n)$) can recover the plaintext block via

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

This is fast thanks to *repeated squaring*. After recovering each numeric block m, translate back to letters using two digits per letter: $A = 00, \ldots, Z = 25$. Leading zeros matter!

Step 1 — Compute the private exponent d

$$\phi(n) = (p-1)(q-1) = 42 \cdot 58 = 2436, \qquad \text{find } d \text{ with } 13d \equiv 1 \pmod{2436}.$$

Extended Euclid gives $d = 937$ (indeed $13 \cdot 937 = 12181 = 1 + 5 \cdot 2436$).

Step 2 — Decrypt each block with repeated squaring

Block 1: $c = 0981 \Rightarrow c = 981$.

$$m \equiv 981^{937} \pmod{2537}, \qquad 937 = 512 + 256 + 128 + 32 + 8 + 1.$$

Squares mod 2537:

power	1	2	4	8	16	32	64	128	256
512									
981^{power} mod 2537	981	838	1922	1325	450	441	322	2472	1688
293									

Multiply only the needed entries (powers $1, 8, 32, 128, 256, 512$):

$$\begin{aligned}
&r \leftarrow 1 \\
&r \cdot 981 \equiv 981 \\
&r \cdot 1325 \equiv 981 \cdot 1325 \equiv 1717 \\
&r \cdot 441 \equiv 1717 \cdot 441 \equiv 1251 \\
&r \cdot 2472 \equiv 1251 \cdot 2472 \equiv 282 \\
&r \cdot 1688 \equiv 282 \cdot 1688 \equiv 1292 \\
&r \cdot 293 \equiv 1292 \cdot 293 \equiv \boxed{704}
\end{aligned}$$

So $m_1 = 0704 \Rightarrow \texttt{07 04} = \texttt{H E}$.

Block 2: $c = 0461 \Rightarrow c = 461$.

$$m \equiv 461^{937} \pmod{2537}, \qquad 937 = 512 + 256 + 128 + 32 + 8 + 1.$$

Squares mod 2537:

power	1	2	4	8	16	32	64	128	256	512
461^{power} mod 2537	461	1950	2074	1261	1959	1737	676	316	913	1433

Multiply the needed entries (powers $1, 8, 32, 128, 256, 512$):

$$\begin{aligned}
&r \leftarrow 1 \\
&r \cdot 461 \equiv 461 \\
&r \cdot 1261 \equiv 461 \cdot 1261 \equiv 1327 \\
&r \cdot 1737 \equiv 1327 \cdot 1737 \equiv 1559 \\
&r \cdot 316 \equiv 1559 \cdot 316 \equiv 1122 \\
&r \cdot 913 \equiv 1122 \cdot 913 \equiv 82 \\
&r \cdot 1433 \equiv 82 \cdot 1433 \equiv \boxed{1115}
\end{aligned}$$

So $m_2 = 1115 \Rightarrow \texttt{11 15} = \texttt{L P}$.

Step 3 — Read the plaintext

Blocks 0704 1115 translate to $\boxed{\texttt{HELP}}$.

Tips, tricks, and common pitfalls

- Keep the two-digit mapping straight: $A = 00, \ldots, J = 09, \ldots, Z = 25$. Leading zeros are part of the block!

- Choose the block size so that each four–digit block m is $< \boldsymbol{n}$. Here $2N = 4$ works because $2525 < 2537 < 252525$.
- When doing repeated squaring, build a small table of $c^1, c^2, c^4, \ldots$ and then multiply only the powers that add up to d.
- Arithmetic gets easier if you reduce *often*. Every product should be brought back modulo n immediately.

Practice — Your Turn (use $n = 2537,\ e = 13,\ d = 937$)

Use the same key as above. Show your exponentiation steps and *keep* leading zeros when converting back to letters.

Problem A (easier). Decrypt the single block `2081`. What two letters do you get? *Hint:* compute $2081^{937} \bmod 2537$ and then split the result as __ __.

Problem B (similar). Decrypt the two–block ciphertext `2081 2182`. *Reminder:* convert each four–digit block separately, then map back to letters.

Problem C (harder). The ciphertext `0981 0724 1774` was made with the same key.

- Decrypt all three blocks.
- Translate to letters. If the last block ends with a padding letter `X`, circle it.

Reflection. In one or two sentences, explain why knowing e and n does *not* make decryption easy, but knowing d does. $\square$