Discrete Structures **Chapter 4.6 — Cryptography**
Solutions: Example 9 (RSA Decryption)

Core facts for this example

Public key: $(n, e) = (2537, 13)$ with $n = 43 \cdot 59$.
Euler totient: $\phi(n) = (p-1)(q-1) = 42 \cdot 58 = 2436$.
Private exponent d is the inverse of e modulo $\phi(n)$:

$$13d \equiv 1 \pmod{2436} \quad \Rightarrow \quad d = 937.$$

Decryption works blockwise: for each ciphertext block c,

$$m \equiv c^d \pmod{n} \qquad \text{and then map } m \text{ back to letters with } A = 00, \ldots, Z = 25.$$

Textbook Example 9 — Full decryption

Ciphertext: `0981 0461`.

Block 1: $c = 0981 \Rightarrow 981$

We use repeated squaring (mod 2537) and write $d = 937 = 512 + 256 + 128 + 32 + 8 + 1$.

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 $1, 8, 32, 128, 256, 512$), reducing after each step:

$$981 \cdot 1325 \cdot 441 \cdot 2472 \cdot 1688 \cdot 293 \equiv \boxed{704} \pmod{2537}.$$

So $m_1 = 0704 \Rightarrow$ `07 04` $=$ `H E`.

Block 2: $c = 0461 \Rightarrow 461$

Again with $d = 937 = 512 + 256 + 128 + 32 + 8 + 1$:

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 $1, 8, 32, 128, 256, 512$):

$$461 \cdot 1261 \cdot 1737 \cdot 316 \cdot 913 \cdot 1433 \equiv \boxed{1115} \pmod{2537}.$$

So $m_2 = 1115 \Rightarrow$ `11 15` $=$ `L P`.

Plaintext: $\boxed{\texttt{HELP}}$.

Checks and teaching notes. Emphasize (i) mapping is two digits per letter with leading zeros preserved; (ii) block size 4 works because $2525 < n = 2537 < 252525$; (iii) reduce after *every* multiplication to keep numbers small.

Practice Solutions

Problem A (easier)

Prompt. Decrypt the single block `2081`.

Work. Compute $m \equiv 2081^{937} \pmod{2537}$. (Repeated squaring or any correct modular-pow tool is fine.) One clean path gives

$$2081^{937} \equiv \boxed{1819} \pmod{2537}.$$

Split to letters: $18 \to$ `S`, $19 \to$ `T`.
Answer: $\boxed{\texttt{ST}}$.

Problem B (similar)

Prompt. Decrypt the two blocks `2081 2182`.

Work. From part A, $2081^{937} \equiv 1819 \Rightarrow$ `ST`. Similarly,

$$2182^{937} \equiv \boxed{1415} \pmod{2537} \Rightarrow \texttt{14 15} = \texttt{O P}.$$

Answer: $\boxed{\texttt{STOP}}$.

Problem C (harder)

Prompt. Decrypt `0981 0724 1774`. Same key.

Work. Blockwise decryption:

$$\begin{aligned} 0981^{937} &\equiv \boxed{0704} \pmod{2537} \quad \Rightarrow \texttt{HE}, \\ 0724^{937} &\equiv \boxed{1111} \pmod{2537} \quad \Rightarrow \texttt{LL}, \\ 1774^{937} &\equiv \boxed{1423} \pmod{2537} \quad \Rightarrow \texttt{OX}. \end{aligned}$$

Answer: $\boxed{\texttt{HELLOX}}$ (final `X` is padding to complete a two-letter block).

Coach's notes.

- When a message length is odd (in letters), a padding letter (commonly `X`) is appended so every numeric string splits cleanly into four-digit blocks.
- If students' intermediate residues differ, check two things: (1) their exponent decomposition of 937 and (2) that they reduced modulo 2537 after *every* multiply and square.

Quick reference: letter map (A=00,. . . ,Z=25).
$\{00, 01, \dots, 09\} \to \{\texttt{A}, \texttt{B}, \dots, \texttt{J}\},\ 10 \to \texttt{K},\ 11 \to \texttt{L},\ \dots,\ 25 \to \texttt{Z}.$