Solutions — Example 6 Practice (Transposition, $\sigma = [3, 1, 4, 2]$)

Permutation recap. Encryption (per block): $c_1c_2c_3c_4 = p_2\,p_4\,p_1\,p_3$. Decryption uses σ^{-1}: $c_1 \to p_2,\ c_2 \to p_4,\ c_3 \to p_1,\ c_4 \to p_3$.

Problem A (easier) — Encrypt `MATH NERD`

Remove space and block: `MATH` `NERD`.

$$\begin{aligned} \texttt{MATH}: &\quad p = \texttt{M,A,T,H} \Rightarrow c = \texttt{A H M T}, \\ \texttt{NERD}: &\quad p = \texttt{N,E,R,D} \Rightarrow c = \texttt{E D N R}. \end{aligned}$$

$$\boxed{\texttt{AHMT EDNR}}$$

Problem B (similar) — Decrypt `OEHM OKWR`

Blocks: `OEHM` `OKWR`. Use σ^{-1}.

$$\texttt{OEHM} : c_1 \to p_2 = O,\ c_2 \to p_4 = E,\ c_3 \to p_1 = H,\ c_4 \to p_3 = M \Rightarrow \texttt{HOME}.$$

$$\texttt{OKWR} : c_1 \to p_2 = O,\ c_2 \to p_4 = K,\ c_3 \to p_1 = W,\ c_4 \to p_3 = R \Rightarrow \texttt{WORK}.$$

$$\boxed{\texttt{HOME WORK}}$$

Problem C (harder) — Encrypt `DATA SCIENCE` (pad with X)

Normalize: `DATASCIENCE` (11 letters) → pad: `DATASCIENCEX`. Blocks: `DATA` `SCIE` `NCEX`.

$$\begin{aligned} \texttt{DATA}: &\quad p = \texttt{D,A,T,A} \Rightarrow c = \texttt{A A D T}, \\ \texttt{SCIE}: &\quad p = \texttt{S,C,I,E} \Rightarrow c = \texttt{C E S I}, \\ \texttt{NCEX}: &\quad p = \texttt{N,C,E,X} \Rightarrow c = \texttt{C X N E}. \end{aligned}$$

$$\boxed{\texttt{AADT CESI CXNE}}$$

Key takeaways.

- Transposition ciphers permute positions, not letters—so frequencies are unchanged.
- Always decrypt with the inverse permutation σ^{-1}.
- Padding guarantees all blocks are full; document your padding rule (e.g., use `X`).