Example 6 (Worksheet) — Transposition Cipher with a Permutation

Cipher rule (why it's cool). A *transposition* cipher keeps the letters but shuffles their *positions.* We split plaintext into blocks of 4 and apply the permutation

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix}.$$

That is: $\underline{\text{1st}}\to$3rd, $\underline{\text{2nd}}\to$1st, $\underline{\text{3rd}}\to$4th, $\underline{\text{4th}}\to$2nd. (So for plaintext block $p_1p_2p_3p_4$ the ciphertext block is $c_1c_2c_3c_4 = p_2\,p_4\,p_1\,p_3$.)

(a) Encrypt PIRATE ATTACK

Step 1 — Normalize and block (remove spaces, then group 4).

$$\texttt{PIRATEATTACK} \;\Rightarrow\; \texttt{PIRA TEAT TACK}.$$

Step 2 — Apply σ to each block.

$$\begin{aligned} &\texttt{PIRA}: \; p_1 = P,\; p_2 = I,\; p_3 = R,\; p_4 = A \Rightarrow c = p_2\,p_4\,p_1\,p_3 = \texttt{IAPR}, \\ &\texttt{TEAT}: \; p = \texttt{T,E,A,T} \Rightarrow c = \texttt{E T T A}, \\ &\texttt{TACK}: \; p = \texttt{T,A,C,K} \Rightarrow c = \texttt{A K T C}. \end{aligned}$$

Ciphertext: $\boxed{\texttt{IAPR ETTA AKTC}}$.

(b) Decrypt SWUE TRAE OEHS

To undo the shuffle, use σ^{-1}:

$$\sigma^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix} \quad (\text{so } c_1 \to p_2,\; c_2 \to p_4,\; c_3 \to p_1,\; c_4 \to p_3).$$

Block and apply σ^{-1}:

$$\texttt{SWUE} \to \texttt{USEW}, \qquad \texttt{TRAE} \to \texttt{ATER}, \qquad \texttt{OEHS} \to \texttt{HOSE}.$$

Plaintext (grouped): $\boxed{\texttt{USE WATER HOSE}}$.

Tips & pitfalls

- **Always block first.** Remove spaces, then group in 4s. If the last block is short, pad (e.g., with `X`).
- **Keep "from" vs "to" straight:** here σ says where each *plaintext position* lands in ciphertext.
- **Decrypt with σ^{-1}:** move each ciphertext position back to the correct plaintext spot.

Practice — Your Turn

Use the same permutation $\sigma = [3, 1, 4, 2]$. Work neatly: show the block, show $p_1p_2p_3p_4$, then the rearranged $c_1c_2c_3c_4$.

Problem A (easier). Encrypt `MATH NERD`. (No padding needed.)

Problem B (similar). Decrypt the ciphertext `OEHM OKWR`.

Problem C (harder). Encrypt `DATA SCIENCE`. If needed, *pad the last block with X* to fill 4 letters. Show every block and the final ciphertext.

Reflection. Why does transposition preserve letter frequencies but still hide the message structure?