HOMEWORK 1 Due Jan 30 11:59PM on Gradescope.

Problem 1. (100 points.) Let $\mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$. Consider the symmetric-key encryption scheme $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ with message-space $(\mathbb{Z}_{10})^4$ (that is, messages must consist of exactly four decimal digits) defined as follows. Key-generation algorithm $\mathcal{K}$ outputs a uniformly random $\pi \in \mathsf{Perm}(\mathbb{Z}_{10})$, where $\mathsf{Perm}(\mathbb{Z}_{10})$ is the set of permutations on $\mathbb{Z}_{10}$, and encryption algorithm $\mathcal{E}$ is defined by

Algorithm $\mathcal{E}_\pi(M)$:
Parse M as $M[1]M[2]M[3]M[4]$ where each $M[i] \in \mathbb{Z}_{10}$
For $i = 1$ to 4 do:
$P[i] \leftarrow M[i] + i \bmod 10$
$C[i] \leftarrow \pi(P[i])$
Return $C[1]C[2]C[3]C[4]$

(Part A - 20 points.) Finish the description of SE by specifying a correct decryption algorithm (meaning it outputs the right message). Your answer should be in pseudocode with the same format as the encryption algorithm above; other answers may not receive any points.

(Part B - 40 points.) Is SE a substitution cipher according to the definition given in class? Your answer should either write equivalent key-generation, encryption, and decryption algorithms in the required format of a substitution cipher, or argue that this cannot be done; other answers may not receive any points. To clarify, in such an equivalent scheme $\mathsf{SE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$, each key would also be from $\mathsf{Perm}(\mathbb{Z}_{10})$, and for all $\pi \in \mathsf{Perm}(\mathbb{Z}_{10})$ there would be a $\pi' \in \mathsf{Perm}(\mathbb{Z}_{10})$ such that $\mathcal{E}_\pi(M) = \mathcal{E}'_{\pi'}(M)$ for all $M \in (\mathbb{Z}_{10})^4$.

(Part C - 40 points.) Is SE perfectly-secure according to the definition given in class? Why or why not? Your answer should either prove that the equality given in class holds for all message pairs and ciphertexts, or give an example of a message pair and ciphertext for which it is violated (as well as argue this is so); other answers may not receive any points.