Instructions Before attempting this homework, be sure to review the course's Academic Honesty policy on `the course syllabus`, and be certain to abide by it and the homework policies discussed in class. This homework is due on **Friday, February 8th** at **11:59pm**, by which time you should have submitted your solutions as a PDF to `Gradescope`. Since we aren't using real paper here, please use at least **one page per solution** (in this case at least four pages: at least one each for Problem 1, Problem 2A, Problem 2B, and Problem 2C). Please also **label your solution pages correctly on Gradescope**! If you do not, you will be **deducted up to 10 points**, so make sure you leave yourself about five minutes to upload, especially if you are unfamiliar with the process.

Problem 1. (30 points.) In a recent interview with astrophysicist Neil Degrasse Tyson,[1] Edward Snowden suggested a reason why humans have not observed alien communication is that aliens' use of "good" encryption would make such communication look random and therefore indistinguishable from cosmic background radiation. (NB: He is talking about aliens communicating amongst themselves, not attempts to contact humans.) Critique this argument from a cryptographic standpoint.

Problem 2. (70 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 are 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 -10 points.) Finish the description of SE. That is, specify a decryption algorithm $\mathcal{D}$ such that $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a *correct* symmetric-key encryption scheme with $\mathcal{K}, \mathcal{E}$ as defined above.

(Part B - 30 points.) Is SE a substitution cipher? Why or why not?

(Part C - 30 points.) Is SE a Shannon-secure? Why or why not?

[1] See `http://www.startalkradio.net/show/a-conversation-with-edward-snowden-part-1/`.