Problem 1. (30 points.) In a recent interview with astrophysicist Neil Degrasse Tyson, 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. Critique this argument from a cryptographic standpoint (assuming aliens do use “good” encryption).

Problem 2. (70 points.) Define key-generation algorithm $K$ to output a random 128-bit key $K$ and define encryption algorithm $E$ by

Algorithm $E_K(M)$:

\[
\begin{align*}
C[0] &\leftarrow \{0, 1\}^{128} \\
\text{For } i = 1 \text{ to } m \text{ do:} \\
W[i] &\leftarrow C[0] + i \\
C[i] &\leftarrow \text{AES}_K(M[i] \oplus W[i]) \\
C &\leftarrow C[0] || \ldots || C[m] \\
\text{Return } C
\end{align*}
\]

Recall above that we regard the message $M$ as consisting of $m$ blocks of 128-bits each, and ‘$W[i] \leftarrow C[0] + i$’ denotes regarding $C[0]$ and $i$ as encoding 128-bit integers, taking their sum modulo $2^{128}$, and then encoding the result as another 128-bit string $W[i]$.

(Part A - 10 points.) Define a decryption algorithm $D$ such that $SE = (K, E, D)$ is a symmetric-key encryption scheme (i.e., satisfying the correctness condition we gave in class).

(Part B - 60 points.) Show that $SE$ is not IND-CPA secure by giving a practical adversary $A$ such that its advantage $\text{Adv}_{SE}^{\text{ind-cca}}(A)$ is high. Your adversary should be given in concise pseudo-code. State and prove the advantage achieved by your adversary, the number of oracle queries it makes, and its running-time.

---

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