COMPSCI 466: Homework 4

Problem 1. (50 points.) Define key-generation algorithm $\mathcal{K}$ to output a random 128-bit key K and define encryption algorithm $\mathcal{E}$ by

```
Algorithm $\mathcal{E}_K(M)$:
    $C[0] \leftarrow\!\!{\scriptstyle\$}\ \{0,1\}^{128}$
    For $i = 1$ to $m$ do:
        $W[i] \leftarrow C[0] + i \bmod 2^{128}$
        $C[i] \leftarrow \mathsf{AES}_K(M[i] \oplus W[i])$
    $C \leftarrow C[0] \| \ldots \| C[m]$
    Return $C$
```

Above we parse M as consisting of m blocks of 128-bits each, and '$W[i] \leftarrow C[0] + i \bmod 2^{128}$' 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 $\mathcal{D}$ such that $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric-key encryption scheme (i.e., satisfying the correctness condition we gave in class).

(Part B - 40 points.) Show that SE is not IND-CPA secure by giving a practical adversary A such that its advantage $\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A)$ is high. As usual, your adversary should be given in concise pseudocode and you should formally analyze its advantage and resource usage. NB: Your adversary should break the encryption scheme without breaking the underlying blockcipher as a PRF (no birthday attack or exhaustive key search). Such attacks against the underlying blockcipher are not practical and will not receive any points.