COSC-260: Homework 3

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

$$\text{Algorithm } E_K(M):$$


$C[0] \leftarrow \{0, 1\}^{128}$

For $i = 1$ to $m$ do:

$W[i] \leftarrow C[0] + i \mod 2^{128}$

$C[i] \leftarrow \text{AES}_K(M[i] \oplus W[i])$

$C \leftarrow C[0] \parallel \ldots \parallel C[m]$

Return $C$

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

(Part B - 40 points.) Show that $SE$ is not IND-CPA secure by giving a practical adversary $A$ such that its advantage $\text{Adv}_{\text{ind-CPA}}^{SE}(A)$ 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. Such attacks against the underlying blockcipher are not practical and will not receive any points.

**Problem 2.** (40 points.) Let $D$ be the set of all strings whose length is a positive multiple of 128. Define hash function $H: \{0, 1\}^{128} \times D \rightarrow \{0, 1\}^{128}$ as follows:

$$\text{Algorithm } H_K(M):$$

Parse $M$ as $M[1]M[2] \ldots M[m]$

$C[0] \leftarrow 0^{128}$

For $i = 1$ to $m$ do:

$B[i] \leftarrow \text{AES}_K(C[i - 1] \oplus M[i])$

$C[i] \leftarrow \text{AES}_K(B[i] \oplus M[i])$

Return $C[m]$

As before, above we parse $M$ as consisting of $m$ blocks of 128-bits each. Show that $H$ is not CR by giving a practical adversary $A$ such that its advantage $\text{Adv}_{\text{CR}}^{H}(A)$ 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 hash function without breaking the underlying blockcipher as a PRF. Such attacks against the underlying blockcipher are not practical and will not receive any points.
Problem 3. (10 points.) Read and provide a short reaction statement to the recent open letter by Apple CEO Tim Cook at http://www.apple.com/customer-letter/. I would like you to focus on the technical rather than political/philosophical content. In particular, does this letter accurately depict cryptographic technology? Why or why not?