COSC-530: Homework 2

Problem 1. (100 points.) Define key-generation algorithm $K$ to output a random 128-bit key $K$ and define encryption algorithm $E$ by

**Algorithm $E_K(M)$:**

\[
C[0] \leftarrow \{0,1\}^{128} \\
\text{For } i = 1 \text{ to } m \text{ do:} \\
W[i] \leftarrow C[0] + i \mod 2^{128} \\
C[i] \leftarrow \text{AES}_K(M[i] \oplus W[i]) \\
C \leftarrow C[0] \parallel \ldots \parallel C[m] \\
\text{Return } C
\]

Above we regard the $M$ 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 in the natural way, taking their sum modulo $2^{128}$, and then encoding the result as another 128-bit string $W[i]$.

(Part A - 20 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 - 80 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. 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.

Problem 2. (100 points.) Prove the following theorem.

**Theorem 0.1** Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $SE = (K, E, D)$ be the corresponding CBC$\$ symmetric encryption scheme. Let $A$ be an IND-CPA adversary against $SE$ having running-time $t$ and making at most $q$ LR oracle queries, with messages totaling at most $\sigma$ blocks. Then there is a PRF adversary $B$ against $E$ such that

\[
\text{Adv}^{\text{ind-CPA}}_{SE}(A) \leq 2 \cdot \text{Adv}^{\text{prf}}_{E}(B) + \frac{\sigma^2}{2^n}.
\]

Furthermore, $B$ makes at most $\sigma F_n$ oracle queries and has running-time $t + \Theta(\sigma \cdot n)$.

Problem 3. (100 points.) You are hired at a startup in the local DC area. Since you know about cryptography, the CEO asks you how secure CBC$\$ based on AES is. Give a clear and full answer which includes an explanation of security models, their merits, attacks, and proofs. This should include an interpretation of Theorem 0.1. Your description should cover both the value and the limitations of this theorem and give a realistic picture of security aimed at someone with little understanding of cryptography.