Problem Set 2

Due: Tuesday January 31, 2017, in class.

By $a \| b$ we denote the concatenation of strings $a, b \in \{0,1\}^*$. (For example $010 \| 01 = 01001$.) If E is a family of functions, then T_E denotes the time to compute it. If E is a blockcipher, T_E is also the time to compute E^{-1}. All times are worst case. Justifications are expected for all answers.

Problem 1 [50 points] Let $G\colon \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a family of functions and let $r \geq 1$ be an integer. The *r-round Feistel cipher associated to G* is the family of functions $G^{(r)}\colon \{0,1\}^k \times \{0,1\}^{2l} \to \{0,1\}^{2l}$, defined as follows for any key $K \in \{0,1\}^k$ and input $x \in \{0,1\}^{2l}$:

Alg $G^{(r)}(K, x)$
$L_0 \| R_0 \leftarrow x$
For $i = 1, \ldots, r$ do
  $L_i \leftarrow R_{i-1}$; $R_i \leftarrow G(K, R_{i-1}) \oplus L_{i-1}$
Return $L_r \| R_r$

In the first line, we are parsing x as $x = L_0 \| R_0$ with $|L_0| = |R_0| = l$, meaning L_0 is the first l bits of x and R_0 is the rest.

1. **[20 points]** Show that $G^{(1)}$ is not a secure PRF by presenting in pseudocode a $\mathcal{O}(T_G + k + l)$-time adversary A making one query to its **Fn** oracle and achieving $\mathbf{Adv}^{\mathrm{prf}}_{G^{(1)}}(A) = 1 - 2^{-l}$.

2. **[30 points]** Show that $G^{(2)}$ is not a secure PRF by presenting in pseudocode a $\mathcal{O}(T_G + k + l)$-time adversary A making two queries to its **Fn** oracle and achieving $\mathbf{Adv}^{\mathrm{prf}}_{G^{(2)}}(A) = 1 - 2^{-l}$.

Problem 2 [50 points] Let $k, n \geq 4$ be integers and let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Let $\mathcal{K}$ be the key-generation algorithm that returns a random 128-bit string as the key K. Let $\mathcal{E}$ be the following encryption algorithm:

Alg $\mathcal{E}_K(M)$
$M[1] \ldots M[m] \leftarrow M$
$R \xleftarrow{\$} \{0,1\}^n$; $C[0] \leftarrow R$

for $i = 1, \ldots, m$ do
  $W[i] \leftarrow (R + i) \bmod 2^n$; $C[i] \leftarrow E_K(M[i] \oplus W[i])$
$C \leftarrow C[0]C[1] \ldots C[m]$
return C

Above $W[i] \leftarrow (R+i) \bmod 2^n$ means we regard R as an integer, add i to it, take the result modulo 2^n, view this as a n-bit string, and assign it to $W[i]$. (For example if $n = 4$ and $R = 1110$ and $i = 3$ then $W[i] = 0001$.) The message space is the set of all strings whose length is a positive multiple of n, meaning these are the allowed messages. The first line above indicates that M is broken into n-bit blocks, with $M[i]$ denoting the i-th block and m the number of blocks. (For example if $n = 4$ and $M = 01101011$ then $M[1] = 0110$ and $M[2] = 1011$ and $m = 2$.)

1. [**10 points**] Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme satisfying the correct decryption condition of Slide 3.

2. [**40 points**] Show that this scheme is not IND-CPA secure by presenting a $\mathcal{O}(T_E + k + n)$-time adversary A making one query to its **LR** oracle and achieving $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 1$.
