Instructor: Adam O'Neill
adamo@cs.umass.edu

COMPSCI-466: Practice Midterm Exam

This is longer than the actual midterm will be!

Problem 1. Let $\mathbb{Z}_3 = \{0, 1, 2\}$ and $\mathbb{Z}_3^* = \{1, 2\}$. Consider the symmetric-key encryption scheme $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ with message-space $(\mathbb{Z}_3)^2$ defined as follows. Key-generation algorithm $\mathcal{K}$ outputs a uniformly random $k \in \mathbb{Z}_3^*$ and encryption algorithm $\mathcal{E}$ is defined by

Algorithm $\mathcal{E}_\pi(M)$:
  Parse M as $M[1]M[2]$ where each $M[i] \in \mathbb{Z}_3$
  For $i = 1, 2$ do:
    $C[i] \leftarrow M[i] \cdot k \bmod 3$
  Return $C[1]C[2]$

(Part A.) Finish the description of SE. That is, specify a decryption algorithm $\mathcal{D}$ such that $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a *correct* symmetric-key encryption scheme with $\mathcal{K}, \mathcal{E}$ as defined above.

(Part B.) Is SE a substitution cipher? Why or why not?

(Part C.) Is SE a Shannon-secure? Why or why not?

Problem 2. Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Define $F\colon \{0,1\}^{2n+k} \times \{0,1\}^n \to \{0,1\}^n$ as follows for any $K_2 \in \{0,1\}^k$ and $K_1, K_3, X \in \{0,1\}^n$:

Algorithm $F_{K_1 \| K_2 \| K_3}(M)$:
  $W \leftarrow K_1 \oplus \overline{M}$; $X \leftarrow E^{-1}_{K_2}(W)$
  $Y \leftarrow K_3 \oplus X$
  Return Y

(Part A.) Is F blockcipher? Prove your answer.

(Part B.) What is the running-time of a 3-query exhaustive key search adversary against F?

(Part C.) Give the most efficient 3-query key recovery adversary that you can having advantage 1 against F. State and prove your adversary's advantage and resource usage.

Problem 3. Let $F\colon \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ be a function family. For each of the following properties below, say whether that property contradicts F being a good PRF.

1. F is not invertible — for most $K \in \{0,1\}^{128}$, $F_K(\cdot)$ is *not* a permutation.

2. For every $K, x \in \{0,1\}^{128}$, we have $F_{\overline{K}}(x) = \overline{F_K(x)}$.

3. For every $K, x \in \{0,1\}^{128}$, we have $F_K(x) = F_K(\overline{x})$.

4. For every $K, x \in \{0,1\}^{128}$, the fourth bit of K is never used in the computation of $F_K(x)$.

Problem 4. Define symmetric-key encryption scheme $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where $\mathcal{K}$ returns a random 128-bit key K and

Algorithm $\mathcal{E}_K(M)$:
  If $|M| \neq 256$ then return $\perp$
  $M[1] \| M[2] \leftarrow M$
  $C[0] \leftarrow \mathsf{AES}_K(M[1])$
  For $i = 1, 2$ do:
    $C[i] \leftarrow \mathsf{AES}_K(C_0[i-1] \oplus M[i])$
  Return $C[0]C[1]C[2]$

(Part A.) Define a decryption algorithm $\mathcal{D}$ such that $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric-key encryption scheme satisfying the correctness condition.

(Part B.) Show that SE is not IND-CPA secure. Your adversary should break the encryption scheme *without* breaking AES. State and prove your adversary's advantage and resource usage.