if (tex.outputmode or tex.pdfoutput or 0) ≠ 0 then tex.print("pdftrue") end
COSC-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 $SE = (K, E, D)$ with message-space $(\mathbb{Z}_3)^2$ defined as follows. Key-generation algorithm $K$ outputs a uniformly random $k \in \mathbb{Z}_3^*$ and encryption algorithm $E$ is defined by

Algorithm $E_{\pi}(M)$:
parse $M$ as $M[1], M[2]$ where each $M[i] \in \mathbb{Z}_3$
for $i = 1, 2$ do:
$C[i] \leftarrow M[i] \cdot k \mod 3$
return $C[1], C[2]$

(Part A.) Finish the description of $SE$. That is, specify a decryption algorithm $D$ such that $SE = (K, E, D)$ is a correct symmetric-key encryption scheme with $K, E$ 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 $E: \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a blockcipher. Define $F: \{0, 1\}^{2n+k} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ as follows for any $K_2 \in \{0, 1\}^k$ and $K_1, K_3, X \in \{0, 1\}^n$:

Algorithm $F_{K_1||K_2||K_3}(M)$:
$W \leftarrow K_1 \oplus M$; $X \leftarrow E^{-1}_{K_2}(W)$
$Y \leftarrow K_3 \oplus X$
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 $F: \{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ 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 $F_K(x) = F_{\overline{K}}(x)$. 

2
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 $SE = (K, E, D)$ where $K$ returns a random 128-bit key $K$ and

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

If $|M| \neq 256$ then return $\perp$


$C[0] \leftarrow AES_K(M[1])$

For $i = 1, 2$
do:

$C[i] \leftarrow AES_K(C[0][i - 1] \oplus M[i])$


(Part A.) Define a decryption algorithm $D$ such that $SE = (K, E, D)$ 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.