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

CS 466: Practice Final Exam

Problem 1. Let $E\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Define $F\colon \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ as follows for any $K \in \{0,1\}^n, M \in \{0,1\}^{2n}$:

Algorithm $F_K(M_1 \| M_2)$:
  $W \leftarrow K \oplus M_1$
  $C \leftarrow E_{M_1}(M_2)$
  Return $C \| W$

(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 2. Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Let D be the set of all strings with length a positive multiple of n. Define $\mathcal{T}\colon \{0,1\}^k \times D \to \{0,1\}^n$ as follows for any $K_1 \in \{0,1\}^k$, $K_2 \in \{0,1\}^n$, $M \in D$:

Algorithm $\mathcal{T}_K(M)$:
  $T' \leftarrow \mathsf{CBC\text{-}MAC}_K(M)$
  $T \leftarrow E_K(T')$
  Return T

Above, $\mathsf{CBC\text{-}MAC}_K$ denotes the CBC-MAC function family using E as the underlying blockcipher with key K.

(10 points.) What is the difference between $\mathcal{T}$ and $\mathsf{ECBC\text{-}MAC}$?

(20 points.) Show that $\mathcal{T}$ is not a secure MAC by giving a practical UF-CMA adversary (making a few queries and doing minor additional computation) with high advantage (say, advantage 1). Formally state and prove the advantage and resource usage of your adversary.

Problem 3. Suppose your colleague asks you "how secure is $\mathsf{ECBC\text{-}MAC}$ based on DES as the underlying blockcipher?" Give a precise and full answer which includes an explanation of security models, attacks, and what has been proved. Your answer should be *succinct* — no more than a few sentences.

Problem 4. Let G be the group $\mathbb{Z}_7^*$ under the operation of multiplication modulo 7.

(Part A.) Why do we know that G is cyclic without doing any computation?

(Part B.) What is $\mathrm{DLog}_{G,3}(5)$?

Problem 5. Let $\mathcal{K}_{\mathrm{rsa}}$ be an RSA generator with modulus length k. Assume k is divisible by 4 and that if (N, p, q, e, d) is an output of $\mathcal{K}_{\mathrm{rss}}$ then $(p-1)/2$ and $(q-1)/2$ are primes larger than $2^{k/4}$. Consider the key-generation and encryption algorithms defined as follows, where $M \in \mathbb{Z}_N^*$:

Algorithm $\mathcal{K}$:	**Algorithm** $\mathcal{E}(N, M)$:
$(N, p, q, e, d) \leftarrow_{\$} \mathcal{K}_{\mathrm{rsa}}$	Do $z \leftarrow_{\$} \{0,1\}^{k/4}$
Return $(N, (N, p, q))$	Until z is an odd prime // can test primality efficiently
	$C \leftarrow M^z \bmod N$
	Return (C, z)

(Part A.) Specify an $O(k^3)$-time decryption algorithm $\mathcal{D}$ such that $\mathsf{PKE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a correct public-key encryption scheme. Formally prove both the claim about running-time and about correctness.

(Part B.) Show that PKE is not IND-CPA secure. Namely, present a $O(k)$-time adversary achieving advantage 1 and making 1 LR query. Formally analyze its advantage and resource usage.