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

CS-690C: Homework 1

Problem 1. (100 points.) We define target-key recovery in what is called the *ideal cipher model.* In this model, first proposed by Shannon, a blockcipher is modeled by a different, independent random permutation for *every* key. That is, the adversary in addition to its usual procedures gets access to oracles that implement a family of independent random permutations (called the *ideal cipher*) and their inverses. For simplicity, we do not give oracle access to their inverses below since it won't matter for this homework.

For key-length $k \in \mathbb{N}$, block-length $\ell \in \mathbb{N}$, and an adversary A, define *ideal-cipher target-key recovery game* $\text{IC-TKR}_{k,\ell}^{A}$ as follows:

<u>proc INITIALIZE</u>
$K \leftarrow_{\$} \{0,1\}^k$
 	
<u>proc FN(M)</u>
If $M \notin \{0,1\}^\ell$
    Return $\perp$
If $C \leftarrow \text{IC}(K, M)$
Return C
	<u>proc IC(K', M')</u>
	If $K' \notin \{0,1\}^k$ or $M' \notin \{0,1\}^\ell$
	    Return $\perp$
	If $T[K', M'] = \perp$
	    $T[K', M'] \leftarrow_{\$} \{0,1\}^\ell \setminus \{T[K', X] \ : \ T[K', X] \neq \perp\}$
	Return $T[K', M']$
	
	<u>proc FINALIZE(K')</u>
	Return $(K = K')$

Define the *IC-TKR-advantage* of A for key-length k and block-length ℓ as

$$\mathbf{Adv}_{k,\ell}^{\text{ic-tkr}}(A) = \Pr\left[\,\text{IC-TKR}_{k,\ell}^{A} \text{ outputs } 1\,\right] .$$

(20 points.) For $q \in \mathbb{N}$, define an appropriate notion of a q-query exhaustive key-search adversary $A_{\text{ic-eks}}^{q}$ in the ideal cipher model.

(60 points.) Prove that

$$\mathbf{Adv}_{k,\ell}^{\text{ic-tkr}}(A_{\text{ic-eks}}^{1}) \ \geq \ 1 - \frac{2^k - 1}{2^{\ell+1}} .$$

Hint: First prove

$$\mathbf{Adv}_{k,\ell}^{\text{ic-tkr}}(A_{\text{ic-eks}}^{1}) \ \geq \ 2^{\ell-k}\left(1 - \left(1 - \frac{1}{2^\ell}\right)^{2^k}\right)$$

and use the inequality

$$(1-x)^n \ \leq \ \sum_{i=0}^{m} \binom{n}{i} (-x)^i$$

for any $x \in \mathbb{R}$ and $m, n \in \mathbb{Z}$ such that $0 \leq x \leq 1$ and $0 \leq m \leq n$ and m is even.

(20 points.) What does a result in the ideal cipher model "mean" in practice? Is DES an ideal cipher? Is AES an ideal cipher? Discuss.