CS4390/5390 Fall 2013
Shirley Moore, Instructor
Homework 7
Due Thursday, December 5

1. Let $F:\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRF (e.g., a PRF where the key space, input space, and output space are all $\{0,1\}^n$ and say $n=128$). Tell which of the following is a secure PRF and which is not. Explain your answers.

a. $F'((k_1,k_2),x) = F(k_1,x) \oplus F(k_2,x)$
b. $F'(k,x) = k \oplus x$
c. $F'(k,x) = reverse(F(k,x))$ where *reverse(y)* reverses the string *y*.
d. $F'(k,x) = F(k, x \oplus 1^n)$
e. $F'(k,x) = \begin{cases} F(k,x) \text{ if } x \neq 0^n \\ k \quad otherwise \end{cases}$
f. $F'(k,x) = \begin{cases} F(k,x) \text{ if } x \neq 0^n \\ 0^n \quad otherwise \end{cases}$

2. As far as we know, AES is a perfectly good 128-bit block cipher $AES : K \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$. But suppose we want a 127-bit block cipher $E : K' \times \{0, 1\}^{127} \rightarrow \{0, 1\}^{127}$. Describe a construction E that you can prove will be a secure pseudorandom permutation, assuming only that AES is a secure pseudorandom permutation. Your scheme E should be such that we can compute $E_{K'}(x)$ efficiently: the expected running time to compute $E_{K'}(x)$ should be some small constant. Provide a proof of security for your construction.

Problems 3 and 4 refer to the following definition:

Cipher Block Chaining Message Authentication Code (CBC MAC)
Let $E: K \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a block cipher. The CBC MAC over block cipher E has key space K and is given by the following algorithm:

```
algorithm MAC_K(M)
  if M ∉ ({0, 1}^n )^+ then return ⊥
  Break M into n-bit blocks M_1 · · · M_m
  C_0 ← 0^n
  for i=1 to m do C_i ←E_K(C_{i−1} ⊕M_i)
  return C_m
```

3. Consider the following variant of the CBC MAC, intended to allow one to MAC messages of arbitrary length. The construction uses a block cipher $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$, which you should assume to be secure. The domain

for the MAC is $(\{0,1\}^n)^+$. To MAC M under key K compute $CBC_K(M \| |M|)$, where $|M|$ is the length of M, written in n bits and $\|$ means concatenation. Of course K has k bits. Show that this MAC is completely insecure: break it with a constant number of queries.

4. Consider the following variant of the CBC MAC, intended to allow one to MAC messages of arbitrary length. The construction uses a block cipher $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$, which you should assume to be secure. The domain for the MAC is $(\{0,1\}^n)^+$. To MAC M under key (K, K') compute $CBC_K(M) \oplus K'$. K has k bits and K' has n bits. Show that this MAC is completely insecure: break it with a constant number of queries.