Introduction to Cyber Security

Homework 3

Due by 30.6.2020

1. Define a PRF F in the following way. The input and output are m bit long. The key k contains 2m random strings, each of length m. Denote these strings as k[i,b], for i=1,…,m, and b=0,1.
   The output of F for an input $x=x_1,\dots,x_m$ (where $x_1,\dots,x_m$ are the bits of the input) is computed as
   $F(k,x) = k[1,x_1] \oplus k[2,x_2] \oplus \dots \oplus k[m,x_m]$

   Prove that F is not a secure PRF. Do this by showing a set of inputs, so that it is easy to distinguish between the case that you receive the output of F on these inputs, and the case where you receive the output of a completely random function on these inputs.

2. Consider the following MAC scheme, where F is a secure PRF for which the lengths of the input, of the output and of the key are 32 bytes.
   The message M is composed of n 32 byte blocks, $M=m_1,\dots,m_n$.
   MAC(k,M) is computed as $MAC(k,M) = F(k,m_1) \oplus F(k,m_2) \oplus \dots \oplus F(k,m_n)$.
   Is this a secure MAC? If so then prove this fact. If not, show how an attacker can break the security of this MAC scheme.

3. Compute 8^{100001} mod 1255. Explain how you can compute this number without a calculator. Use the Chinese remainder theorem and Euler’s theorem (Euler’s theorem states that for elements x which are not divisible by a prime p, it holds that $x^{p-1}=1 \bmod p$).