University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 4

Due at the *beginning* of class on Oct. 17

In this homework, you get to break stuff.... Remember to describe your attacks in enough detail to make them clear; you may want to use pseudocode in some cases. Also analyze the success probability of your attacks, using the relevant definition in each case. F always denotes a length-preserving pseudorandom function.

1. In class, the following private-key encryption scheme was suggested by a student: The shared key is $k \in \{0,1\}^n$. To encrypt message $m \in \{0,1\}^n$, choose random $r \in \{0,1\}^n$ and output $\langle r, F_r(k) \oplus m \rangle$. Show that if F is a *block cipher* then this scheme is not secure against chosen-plaintext attacks.

2. Show that CBC-mode encryption is not secure against chosen-ciphertext attacks.

3. Consider the following variants of the inefficient MAC shown in class (cf. Construction 4.5). In each case, state whether the variant is secure or insecure. If it is secure, sketch a proof (a formal proof is not needed); if it is insecure, describe an attack.

   (a) To authenticate the message $m_1, \ldots, m_\ell$, where each m_i is a block of length $n/3$, choose random $r \leftarrow \{0,1\}^{n/3-1}$ and set

   $$\begin{aligned} t_i &:= F_k(r \| 0 \| i \| m_i) \quad 1 \le i < \ell \\ t_\ell &:= F_k(r \| 1 \| \ell \| m_\ell). \end{aligned}$$

   (Above, i is encoded using $n/3$ bits, and the second field is just a single bit.) Output the tag $\langle r, t_1, \ldots, t_\ell \rangle$.

   (b) To authenticate the message $m_1, \ldots, m_\ell$, where each m_i is a block of length $n/3$, choose random $r \leftarrow \{0,1\}^{n/3}$ and set $t_i := F_k(i \| \ell \| (m_i \oplus r))$ (again, i is encoded using $n/3$ bits). Output the tag $\langle r, t_1, \ldots, t_\ell \rangle$.

4. Show that the following variants of CBC-MAC encryption are insecure:

   (a) Basic CBC-MAC as described in class, but where the sender authenticates messages of different lengths.

   (b) Basic CBC-MAC, for fixed-length messages, but where $t_0 \in \{0,1\}^n$ is chosen at random and sent as part of the tag along with t_ℓ.

   (c) Basic CBC-MAC, for fixed-length messages, but where the tag includes all the values $t_1, \ldots, t_\ell$.

   (d) (**Extra credit – this is hard**:) CBC-MAC for variable length messages, where the message length is *appended* to the message before running basic CBC-MAC on the result. (*Note*: The exact way the message length is encoded is unimportant for the attack.)