

# Cryptography

## Problem set 5 - 8-9 IV 2015

**Problem 1** Say  $\Pi = \langle \text{Gen}, \text{Mac}, \text{Vrfy} \rangle$  is a secure MAC and for  $k \in \{0, 1\}^n$  the tag-generation algorithm  $\text{Mac}_k$  always outputs tags of length  $t(n)$ . Prove that  $t$  must be super-logarithmic or, equivalently, that if  $t(n) = \mathcal{O}(\log n)$  then  $\Pi$  cannot be a secure MAC.

Hint: consider the probability of randomly guessing a valid tag.

**Problem 2** Let  $F$  be a pseudorandom function. Show that the following MAC for messages of length  $2n$  is secure/insecure.

The shared key is a random  $k \in \{0, 1\}^n$ . To authenticate a message  $m_1 || m_2$  with  $|m_1| = |m_2| = n$ , compute the tag  $\langle F_k(m_1), F_k(F_k(m_2)) \rangle$ .

**Problem 3** Let  $F$  be a pseudorandom function. Show that each of the following message authentication codes is insecure.

1. To authenticate a message  $m = m_1 || \dots || m_l$ , where  $m_i \in \{0, 1\}^n$ , compute  $t \leftarrow F_k(m_1) \oplus \dots \oplus F_k(m_l)$ .
2. To authenticate a message  $m = m_1 || \dots || m_l$ , where  $m_i \in \{0, 1\}^n$ , choose  $r \leftarrow \{0, 1\}^n$  at random, compute  $t \leftarrow F_k(r) \oplus F_k(m_1) \oplus \dots \oplus F_k(m_l)$  and send  $\langle r, t \rangle$ .
3. To authenticate a message  $m = m_1 || \dots || m_l$ , where  $m_i \in \{0, 1\}^{n/2}$ , choose  $r \leftarrow \{0, 1\}^n$  at random, compute  $t \leftarrow F_k(r) \oplus F_k(\langle 1 \rangle || m_1) \oplus \dots \oplus F_k(\langle l \rangle || m_l)$  where  $\langle i \rangle$  is an  $n/2$ -bit encoding of the integer  $i$  and send  $\langle r, t \rangle$ .

**Problem 4** Show that  $\text{Mac}_k(m) = H^s(k || m)$  is not a secure MAC when  $H$  is constructed via Merkle-Damgard transform even if  $H$  is a collision-resistant hash function.

**Problem 5** Let  $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$  be a random function. Consider a sequence  $(x_i)$  defined as  $x_{i+1} = F(x_i)$ , we say that  $j - i$  is a period of  $(x_i)$  if  $j - i = \min\{j - i > 0 : x_i = x_j\}$ . Show that the average period is  $2^{n-1} + 1/2$  if the initial value  $x_1 \in \{0, 1\}^n$  is chosen at random.

How this property influences OFB mode of encryption?

**Problem 6** Let  $\langle G_1, H_1 \rangle$  and  $\langle G_2, H_2 \rangle$  be two hash functions. Define  $\langle G, H \rangle$  so that  $G$  runs  $G_1$  and  $G_2$  to obtain keys  $s_1$  and  $s_2$  respectively. Then define  $H^{s_1, s_2}(x) = H^{s_1}(x) || H^{s_2}(x)$ .

1. Prove that if at least one of  $\langle G_1, H_1 \rangle$  and  $\langle G_2, H_2 \rangle$  is collision resistant, then  $\langle G, H \rangle$  is collision resistant.
2. Determine whether an analogous claim holds for second pre-image resistance and pre-image resistance respectively. Prove your answer in each case.

**Problem 7** Let  $\langle \text{Gen}, H \rangle$  be a collision resistant hash function. Is  $\langle \text{Gen}, G \rangle$  defined by  $G^s(x) = H^s(H^s(x))$  necessarily collision resistant?