Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2018/2019
2018/11/23

Cryptography – Homework 3

Discussed on Wednesday, 28^{th} of November, 2018.

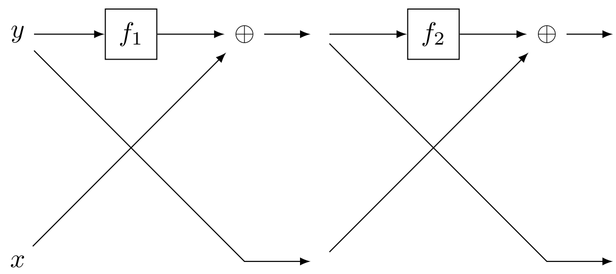
Exercise 3.1

Let F be a PRP.

(a) Show that F-rCBC is not CCA-secure.

(b) Show that F-CBC-CIV (with chained IV—see lecture slides) is *not* CPA-secure.

Exercise 3.2



Let $f : \{0,1\}^* \to \{0,1\}^*$ be some function s.t. $|f(x)| = |x|$ for all $x \in \{0,1\}^*$. A *single-round Feistel network* FN_f is defined by

$$\mathsf{FN}_f(x||y) := y||x \oplus f(y) \text{ for all } x, y \in \{0,1\}^* \text{ with } |x| = |y|\,.$$

Similarly, given functions $f_1, \ldots, f_j$ a *j-round Feistel network* is inductively defined by

$$\mathsf{FN}_{f_1,f_2,\ldots,f_j}(x||y) := \mathsf{FN}_{f_j}(\mathsf{FN}_{f_1,f_2\ldots,f_{j-1}}(x||y))$$

(a) Show that independent of the choice of $f_1, \ldots, f_j$ the function $\mathsf{FN}_{f_1,\ldots,f_j}$ is invertible if $f_1, \ldots, f_j$ are known.

(b) Let F be a PRF of key and block length n and $P_{k_1,k_2}(x||y) := \mathrm{FN}_{F_{k_1},F_{k_2}}(x||y)$ be a two-round Feistel network using F.

   i) Compute $P_{k_1,k_2}(0^n||y)$ and $P_{k_1,k_2}(F_{k_1}(0^n) \oplus z||0^n)$.

   ii) Show that PPT-Eve can compute $P^{-1}_{k_1,k_2}$ when given oracle access to P_{k_1,k_2}.

(c) Is $\mathrm{FN}_{F_{k_1},F_{k_2},F_{k_3}}$ with three independent keys $k_1, k_2, k_3 \overset{u}{\in} \{0,1\}^n$ a PRP? Is it a PRF? (y/n)

Exercise 3.3 MAC or no MAC?

(a) Does rOFB mode yield a secure MAC?

(b) Show that if the IV in the CBC-MAC-Algorithm is not fixed (but chosen randomly and pre-pended to the CBC-output), the MAC becomes insecure.

Exercise 3.4 MACs using hash-functions done wrong

Before NMAC and HMAC, several ad-hoc solutions for constructing MACs were used. For instance, given a (hash) function $H\colon \{0,1\}^* \to \{0,1\}^l$, the tag was defined to be $\mathsf{Mac}_k(m) := H(k||m)$, i.e. the outer encryption used in NMAC and HMAC is missing.

Assume a PRF F with (for simplicity) $n = l_{\text{in}}(n) = l_{\text{out}}(n)$. Using the padding function $\mathsf{pad}(m) := m||10^p||\lfloor|m|\rceil$, set $\mathsf{Mac}_k(m) := H(k||m) := F^*_k(\mathsf{pad}(m))$ for $k \in \{0,1\}^n$.

Show that $\mathsf{Mac}_k(m)$ is not secure.

Hint: Recall that the outer encryption used by NMAC and HMAC is to restrict the adversary to prefix-free queries.

Exercise 3.5

Let F be some secure block cipher with key and block length n (think of AES-128).

Consider the following deterministic MAC:

- Gen: as usual, in input 1^n, output $k \overset{u}{\in} \{0,1\}^n$.
- Mac: given $m \in \{0,1\}^+$ and k,

  first pad m to a multiple of n by appending a minimial number of 0,

  then break the padded message into n-bit blocks $m^{(i)}$.

  Starting with $k^{(0)} := 0^n$, compute $k^{(i)} = F_{k^{(i-1)}}(m^{(i)})$ for i from 1 to d where $d = \frac{|m|}{n}$.

  Finally, output $t := F_{k^{(n)}}(k)$.

  (Draw a picture! Note that the key is appended in this case.)
- Vrf: given m, t, and k, check that $\mathsf{Mac}_k(m) = t$.

Is this MAC secure?