Introduction to Modern Cryptography
Exercise Sheet #4

University of Amsterdam, Master of Logic, 2014
Lecturer: Christian Schaffner
TA: Malvin Gattinger

Monday, 22 September 2014
(**Exercise 1 to be emailed by Wednesday, 24 September 2014, 14:00.**
other exercises to be handed in by Monday, 29 September 2014, 11:00)

Homework

1. Watch the five lectures by Dan Boneh (linked on the course homepage) about block ciphers. Prepare the following two types of questions and email them **before Wednesday, 24 September 2014, 14:00** to c.schaffner@uva.nl. `10 p.`

   (a) A content question (including the answer). This question is easy to answer for somebody who watched the lectures. For instance: What is the core idea behind the DES design? Answer: A Feistel Network.

   (b) An exercise about DES or AES you find interesting. Feel free to get inspired by the exercises in Chapter 5 of [KL], and/or by Dan Boneh's exercises of week 2. You should be able to solve the exercise yourself.

   Out of all questions I receive, I will compile a list of the most interesting ones. We will then discuss them in class on Thursday, 25 September 2014 at 9:00.

2. **One-time MAC:** Let us consider the following message authentication code: `15 p.`

   $\mathsf{Gen}(1^n)$**:** Let $p = \text{NextPrime}(2^n)$; pick $a \leftarrow \mathbb{Z}_p^*$, $b \leftarrow \mathbb{Z}_p$ (so $a \in \{1, 2, \ldots, p-1\}$, $b \in \{0, 1, 2, \ldots, p-1\}$.) Output p, a, b.

   $\mathsf{Mac}_{p,a,b}(m)$**:** Output $[(am + b) \mod p]$.

   $\mathsf{Vrfy}_{p,a,b}(m, t)$**:** Output 1 if $\mathsf{Mac}_{p,a,b}(m) = t$, output 0 otherwise.

   Note that this MAC handles messages $m \in \mathbb{Z}_p$ (only).

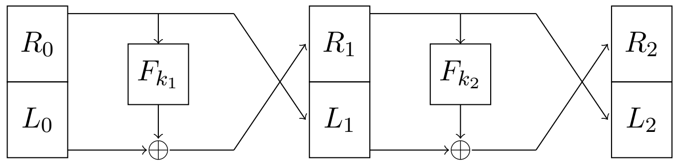
   Show that the above MAC is secure against any adversary making at most one query (see Definition 4.2 in [KL]). In particular, show that this MAC is secure even if the adversary is *not* restricted to run in polynomial time.

3. **Pre-image resistance of hash functions:** Exercise 4.10 of [KL]: Provide formal definitions for second pre-image resistance and pre-image resistance. Formally prove that any hash function that is collision resistant is second pre-image resistant, and that any hash function that is second pre-image resistant is pre-image resistant. `20 p.`

more on the back side

4. **Two-round Feistel network:** Exercise 6.18 of [KL]: Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. Using a Feistel network with two rounds, we contruct a permutation $F' : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ which maps input (L_0, R_0) to output (L_2, R_2), where $k_1, k_2 \in \{0,1\}^n$ are the first and second part of the key k of F'. It holds that 15 p.

$$L_i = R_{i-1} \text{ and } R_i = L_{i-1} \oplus F_{k_i}(R_{i-1}).$$

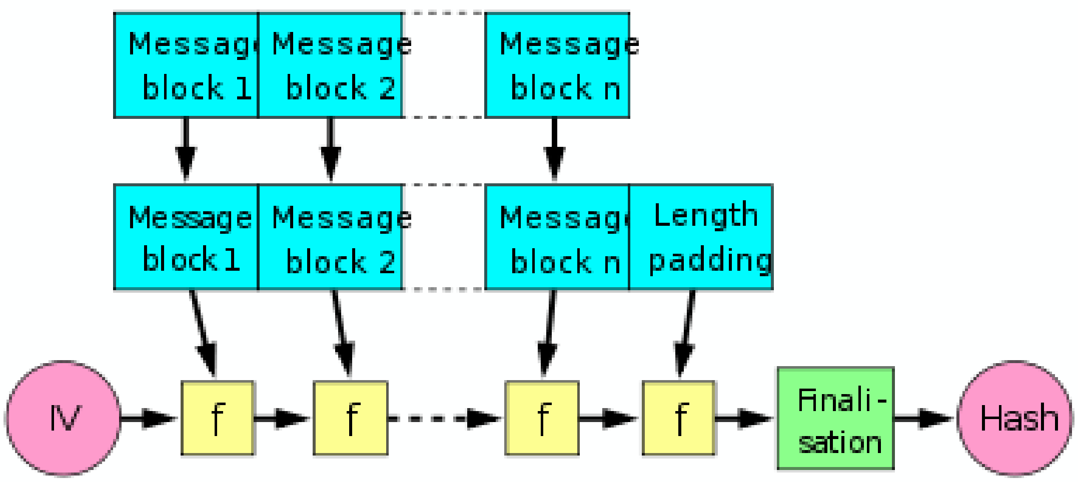


Show that the resulting permutation F' is *not pseudo-random.*

5. **Double-hash:** Exercise 4.12 in [KL]: Let (Gen, H) be a collision-resistant hash function. Show that $(\mathsf{Gen}, \hat{H})$ defined by $\hat{H}^s(x) := H^s(H^s(x))$ is necessarily collision resistant. 15 p.

6. **A dangerous idea:** Exercise 4.17 of [KL]: Before HMAC was invented, it was quite common to define a MAC by $\mathsf{Mac}_k(m) = H^s(k||m)$ where H is a collision-resistant hash function. Show that this is not a secure MAC when H is constructed via the Merkle-Damgård transform where the underlying fixed-length collision-resistant hash function (Gen, h) is known to the adversary. 15 p.

   Hint: Use $\mathsf{Mac}_k(m)$ to construct a valid tag on a particular longer message m'. Note that Merkle-Damgård appends the length of the message to the end of the (padded) input string, you'll need to figure out how to get around that.



The Merkle-Damgård construction
Image credit: `David Göthberg, wikimedia.org` .