Exercise Sheet 9

Cryptography and Security 2025

Exercise 1 MAC From Hash Functions

In this exercise, we will study the security of some MAC constructions based on hash functions. Through this exercise, we will consider a hash function H based on an iterated hash function H_0 with ℓ-bit block messages and the Merkle-Damgård strengthening pad. That is, $m\|\mathsf{pad}(m)$ has a length multiple of ℓ and $H(m) = H_0(m\|\mathsf{pad}(m))$. (See fig.1.)

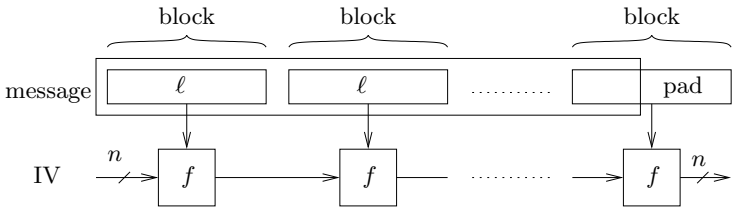

Figure 1: The Merkle-Damgård scheme

1. Recall the standard padding scheme $\mathsf{pad}(m)$ (or an equivalent one).
2. Recall three different security properties of a cryptographic hash function.
3. What is a MAC forgery? Detail the various security models with respect to the Oracles to which the adversary has access.
4. **The Prefix Method**. We consider the MAC algorithm defined given a ℓ-bit secret key K and a message m as
$$\mathsf{MAC}_K(m) = H_0(K\|m\|\mathsf{pad}(m))$$
where $\|$ denotes the concatenation operation.
Show that given the MAC of a known message m the adversary is able to output a forgery on a message $m' \neq m$.
5. **The Suffix Method**. Let us consider another variant defined given a secret key K and a message m as
$$\mathsf{MAC}_K(m) = H_0(m\|\mathsf{pad}(m)\|K)$$
Show that if H is *not* collision-resistant and the adversary has access to an Oracle to which he can submit a *chosen* message m and get $\mathsf{MAC}_K(m)$ then he is able to forge the MAC of a message $m' \neq m$.

Exercise 2 Collisions with a Subset

In a classroom, we have x female students and y male students. We assume that their birthday is uniformly distributed in a calendar of N possible dates, e.g., $N = 365$.

1. Let p_{xx} denote the *exact* probability, that there are at least two different female students with the same birthday. Express p_{xx} in terms of N and x.

2. Let $p_{xy|\neg xx}$ denote the *exact* probability, that there is at least one female-male pair of students who share the same birthday conditioned to that female students have pairwise different birthdays. Express $p_{xy|\neg xx}$ in terms of N, x, and y.

3. Show that $p_{xy|\neg xx} \approx 1 - e^{-\frac{xy}{N}}$.

4. Based on the previous computations, what is the *exact* probability $p_{x\star}$ that at least one female student shares the same birthday with another student (either female or male)?

5. Show that $p_{x\star} \approx 1 - e^{-\frac{x(x+2y)}{2N}}$.

   Hint: $p_{xx} \approx 1 - e^{-\frac{x^2}{2N}}$.

6. In a community of n_u users each having a password, we assume that there is a public directory for the hash of the passwords. We consider an attacker who tries to find password matches with the existing database of n_u password hashes. He is allowed to try n_t many random passwords and hash them. We say that he succeeds if he gets any match. That is to say, he succeeds if either he finds at least one password with a hash in the directory, or if he finds two users having the same password hash in the directory. What is his success probability?

Exercise 3 CBCMAC

Let k, b, and n be some integers and let $\mathsf{MAC} : \{0,1\}^k \times \left(\{0,1\}^b\right)^* \longrightarrow \{0,1\}^n$ be a message authentication code.

1. What is a MAC forgery attack against a message authentication code?
   Discuss on security models.

2. Ideally, considering $k > n$ what complexity (in terms of b, k, and n) should have the best MAC forgery attack against MAC?

We let

$$\mathsf{CBCMAC}\,(K, x_1, \ldots, x_m) = C(K, x_m \oplus \mathsf{CBCMAC}(K, x_1, \ldots, x_{m-1}))$$

and

$$\mathsf{CBCMAC}(K, \emptyset) = 0^b$$

where $C : \{0,1\}^k \times \{0,1\}^b \longrightarrow \{0,1\}^b$ is a block cipher, $\emptyset$ is an empty input, and 0^b is a bit-string of b bits all equal to 0.

3. Give the only possible value for n (in terms of b or k).

4. Explain how to make a MAC forgery attack against CBCMAC with a probability of success of 1 by using 3 chosen messages (or less).