

### Session 3

#### Exercise 1 (Properties of secure hash function)

We recall the Merkle-Damgård construction in Figure 1.

1. For a cryptographic hash function, recall the definition of the preimage resistance, second preimage resistance, and of the collision resistance.
2. Let  $h$  be a hash function. Show that if  $h$  is collision-resistant then  $h$  is second-preimage resistant. In the same way, show that if  $h$  is second-preimage resistant, then  $h$  is preimage resistant.

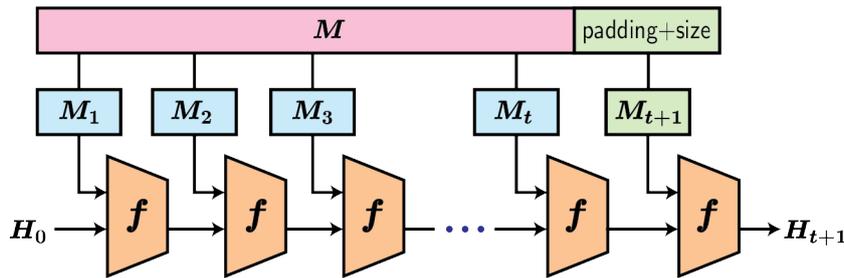


Figure 1: Merkle-Damgård construction.

#### Exercise 2 (CBC ciphertext stealing)

This exercise presents an elegant technique to avoid increasing the length of the CBC encryption of a message whose length  $L$  is not a multiple of the block size  $n$  of the block cipher, as long as  $L > n$ .

Let  $M = m_1 || \dots || m_\ell$  be a message of length  $L = (\ell - 1).n + r$ , where  $r = |m_\ell| < n$ . Recall that the CBC encryption of  $M$  with the block cipher  $\mathcal{E}$  and the key  $k$  is  $C = c_0 || \dots || c_\ell$ , where  $c_0$  is a random initial value and  $c_i = \mathcal{E}_k(m_i \oplus c_{i-1})$  for  $i > 0$ .

1. What is the bit length of  $C$ , assuming that  $m_\ell$  is first padded to an  $n$ -bit block?
2. Write the decryption equation for one block (that is, explain how to compute  $m_i$  in function of  $c_i$ ,  $k$ , and possibly additional quantities).

Let us now rewrite the penultimate ciphertext  $c_{\ell-1} = \mathcal{E}_k(m_{\ell-1} \oplus c_{\ell-2})$  as  $c'_\ell || P$  where  $c'_\ell$  is an  $r$ -bit long. We also introduce  $m'_\ell = m_\ell || 0^{n-r}$  (that is padding with  $n - r$  zeros). Finally, let  $c'_{\ell-1} = \mathcal{E}_k(m'_\ell \oplus (c'_\ell || p))$ .

3. What is the bit length of  $C' = c_0 || \dots || c_{\ell-2} || c'_{\ell-1} || c'_\ell$ ?
4. Explain how to recover  $m_\ell$  and  $P$  from the decryption of  $c'_{\ell-1}$ , and from there  $m_{\ell-1}$  from the one of  $c'_\ell$ .

#### Exercise 3 (Davies-Meyer fixed-points)

In this exercise, we will see one reason why *Merkle-Damgård strengthening* (adding the length of a message in its padding) is necessary in some practical hash function constructions.

We recall that a compression function  $f : \{0, 1\}^n \times \{0, 1\}^b \rightarrow \{0, 1\}^n$  can be built from a block cipher  $\mathcal{E} : \{0, 1\}^b \times \{0, 1\}^n \rightarrow \{0, 1\}^n$  using the “Davies-Meyer” construction as  $f(h, m) = \mathcal{E}(m, h) \oplus h$ .

1. Considering the feed-forward structure of Davies-Meyer, under what conditions would you obtain a fixed-point for such a compression function? (i.e., a pair  $(h, m)$  such that  $f(h, m) = h$ )
2. Show how to compute the (unique) fixed-point of  $f(\cdot, m)$  for a fixed  $m$ . Given  $h$ , is it easy to find  $m$  such that it is a fixed-point, if  $\mathcal{E}$  is an ideal block cipher (i.e., random permutations)?

3. A semi-freestart collision attack for a Merkle-Damgård hash function  $H$  is a triple  $(h, m, m')$  s.t.  $H_h(m) = H_h(m')$ , where  $H_h$  denotes the function  $H$  with its original IV replaced by  $h$ . Show how to use a fixed-point to efficiently mount such an attack for Davies-Meyer + Merkle-Damgård, when strengthening is not used.

**Note:** Fixed-points of the compression function can be useful to create the expandable messages used in second preimage attacks on Merkle-Damgård.

**Exercise 4 (DES)**

Let  $E$  be the encryption algorithm of the DES cryptosystem. Prove that we have:

$$E_K(P) = C \Leftrightarrow E_{\bar{K}}(\bar{P}) = \bar{C} ,$$

where  $P$  is a plaintext,  $K$  is a secret key,  $C$  a ciphertext, and  $\bar{X}$  denotes the binary complementary of  $X$ .

**Exercise 5 (LFSR)**

1. We consider the LFSR of length  $\ell = 3$  with  $(c_1, c_2, c_3) = (1, 0, 1)$ , initialized to  $(z_0, z_1, z_2) = (1, 0, 0)$ . Represent the LFSR state for  $1 \leq i \leq 7$ . Give the output of this LFSR and its period.
2. Why are outputs of LFSR periodic? What is the biggest period made by an LFSR of length  $\ell$ ?