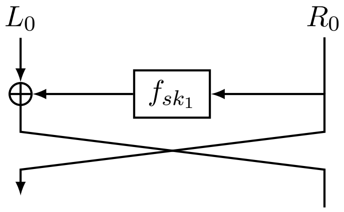
C. Olivier-Anclin

Session 3

Exercise 1 (ECB is not IND–CPA secure)
Prove that the ECB mode of operation does not yield an IND–CPA secure symmetric encryption scheme, no matter how good the underlying block cipher is.

Hint: Write the definitions of IND–CPA security and consider messages with two blocks.

Exercise 2 (DES)
Let E be the encryption algorithm of the DES cryptosystem. DES is a Feistel network of 16 round for which a round operate like described below after an initial permutation IP and before a final permutation IP^{-1}.



Where $f(R_{i-1}, K_i) = P\big(S(E(R_{i-1}) \oplus K_i)\big)$ with:

- E expands the 32-bit input R_{i-1} to 48 bits by using a permutation and duplicating some bits;
- $\oplus$ denotes bitwise XOR with the 48-bit round key K_i;
- S applies the eight S-box substitutions, reducing 48 bits to 32 bits;
- P is a fixed permutation on 32 bits.

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 3 (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.
3. Consider the Merkel Damgård construction below. Prove that if f is preimage resistant then so is H.

Exercise 4 (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 $f : \{0,1\}^n \times \{0,1\}^b \to \{0,1\}^n$ can be built from a block cipher $\mathsf{Enc} : \{0,1\}^b \times \{0,1\}^n \to \{0,1\}^n$ using the "Davies-Meyer" construction as $f(h,m) = \mathsf{Enc}(m,h) \oplus h$.

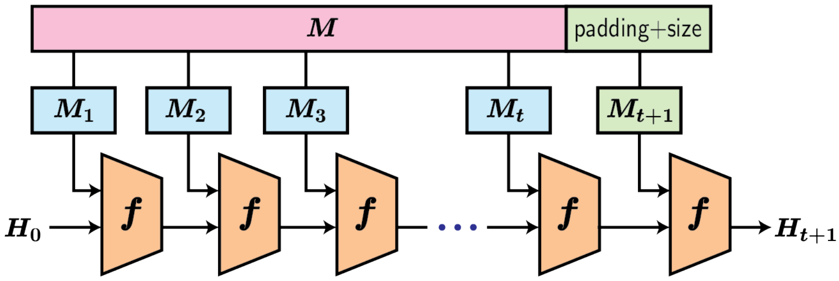


Figure 1: Merkle-Damgård construction.

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 $f(., m)$ for a fixed m. Given h, is it easy to find m such that it is a fixed-point, if Enc 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.

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