Mid-term Exam

The duration of the exam is 1 hour 15 minutes. The grading scale is indicative and subject to change. No document nor any digital device is allowed. The exercises are independent. Not all questions in an exercise are independent, but you may admit a result from a previous question by clearly stating it. For maximum mark, answers must be justified and correctly written out. A probability reminder is given at the end. ***You can answer in French or English.***

Exercise 1. (7 pts) *Basic notions*

Answer each question in at most a dozen of lines (depends on your handwriting, the language used, etc.). More concise answers are perfectly acceptable!

1. Let Enc be a randomized encryption scheme. In particular, for each key k and message m, several ciphertexts can be produced as $c \leftarrow \mathsf{Enc}_k(m)$. Let us assume that for each fixed k and m, the number of possible ciphertexts is 2^t.

- **i.** Recall why, intuitively, a *secure* encryption scheme has to be randomized.
- **ii.** What do you think are acceptable values for t: $t = 1$? $t = 8$? $t = 64$? $t = 128$?
- **iii.** Assume the ciphertexts associated to messages of size n all have the same size $\ell(n)$, where ℓ is an increasing function. Prove a lower bound on $\ell(n)$ in terms of n and t.

2. Explain, in plain English/French, what is the IND-CPA experiment for symmetric encryption schemes, and the IND-CPA advantage.

3. Give the two constructions of hash function that we presented in class. For each of them, specify the building block of the construction and give an example of a hash function built using that construction.

Exercise 2. (4 pts) *Compression functions*

Let $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ a block cipher with key size and block size n. We define two compression functions $f_1, f_2 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ by $f_1(h,m) = E_h(m) \oplus h$ and $f_2(h,m) = E_m(h) \oplus h$ (that is, f_2 is obtained using the Davies-Meyer construction).

1. Describe a first preimage attack against f_1, that is an algorithm that given t *and* h, computes a message m such that $f_1(h,m) = t$. Analyze its complexity.

2. Explain why the previous attack does not apply to f_2. *Which supposedly hard problem on the block cipher does it require to solve?*

Exercise 3. (9 pts) *Even-Mansour construction*

Let $\pi : \{0,1\}^n \to \{0,1\}^n$ be a public (random) permutation. Let $E : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ be the block cipher defined by $E_k(m) = \pi(m \oplus k_1) \oplus k_2$ where $k = k_1 \| k_2 \in \{0,1\}^{2n}$ is the key, split into two n-bit blocks.

1. Define the decription algorithm for E.

2. Let m_1, m_2 such that $m_1 \oplus m_2 = k_1$. Prove that $E_k(m_1) \oplus \pi(m_1) = E_k(m_2) \oplus \pi(m_2)$.

3. We define the following attack: The adversary samples q messages $m_1, \ldots, m_q$ and queries $E_k(m_i)$ for all i, and compute $\pi(m_i)$ for all i; For each *collision* $E_k(m_i) \oplus \pi(m_i) = E_k(m_j) \oplus \pi(m_j)$, the adversary computes a tentative key k' and checks whether it is correct.

- **i.** What is the probability that there exists $i \neq j$ such that $m_i = m_j \oplus k_1$?
- **ii.** Let m_i and m_j provoking a collision: how can the adversary compute a tentative (full) key k'?
- **iii.** How can the adversary check that the tentative key is (probably) the correct one?

4. We now turn this *key-recovery attack* into a significant advantage in the PRP experiment. Recall that the adversary has access to an oracle and must distinguish between the cases where $\twoheadleftarrow \mathrm{Perm}_n$ is a random permutation and $= E_k$ where $k \twoheadleftarrow \{0,1\}^{2n}$.

- **i.** Turn the key-recovery attack into an adversary that makes q queries to the oracle, and tries to distinguish between the cases. *You must describe the queries the adversary makes, the additional computations and the answer given depending on the results.*
- **ii.** Assume that $\twoheadleftarrow \mathrm{Perm}_n$. Explain what must happen for the adversary to be fooled (that is for the adversary to answer that $= E_k$), and justify that this happens with very low probability.
- **iii.** Provide a value for q such that the adversary has a constant nonzero advantage in the PRP experiment.

Probability reminder.

- For two events E and F, $\Pr[E \vee F] \leq \Pr[E] + \Pr[F]$ (*union bound*) and $\Pr[E|F]\Pr[F] = \Pr[F|E]\Pr[E]$ (*Bayes' formula*).
- Let $F_1, \ldots, F_n$ such that $\bigcup_i F_i = \Omega$ is the universe and $F_i \cap F_j = \emptyset$ if $i \neq j$. Then, for any event E, $\Pr[E] = \sum_{i=1}^{n} \Pr[E|F_i]\Pr[F_i]$ (*law of total probability*).
- Let $y_1, \ldots, y_q$ and $z_1, \ldots, z_q$ be uniform samples from a size-N set, with $q \leq \sqrt{N}$. Then $\Pr\left[\exists i \neq j, y_i = y_j\right] \geq \frac{q(q-1)}{4N}$ and $\Pr\left[\exists i, j, y_i = z_j\right] \geq \frac{q^2}{2N}$ (*birthday bounds*).