Mid-term exam – March 14., 2025

No document is allowed. Except indicated otherwise, answers must be carefully justified to get maximum credit. The exercises are independent, but not all questions. You may admit a result from a previous question by clearly stating it. You may answer in English or French. The duration is 1 hour 15 minutes.

Exercise 1 (6 points). *Short questions*

1. What are the two constructions described in the lecture to build a hash function? *Give the name of each construction and define the object it is based on. You are not asked to explain how the construction works.*
2. Is AES a block cipher or a symmetric encryption scheme?
3. Describe the syntax of a MAC, and its role.
4. Is an attack against an encryption scheme which has advantage p and running time t a problem in practice for the following values of p and t: $p = \frac{1}{2}$ and $t = 2^{128}$; $p = (\frac{1}{2})^{120}$ and $t = 2^{32}$; $p = \frac{1}{2}$ and $t = 2^{32}$?

Exercise 2 (6 points). *Modes of operation*

Let $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. We consider two modes of operations. *It is highly recommended to draw pictures of the modes of operation to answer the questions.*

Let $m = m_1 \| \cdots \| m_\ell$ where $m_1, \ldots, m_\ell \in \{0,1\}^n$, and $c_0 \twoheadleftarrow \{0,1\}^n$ be a random IV.

1. Let $\mathsf{Enc}_k^1(m) = c_0 \| c_1 \| \cdots \| c_\ell$ where $c_i = E_k(m_i) \oplus c_{i-1}$ for $1 \leq i \leq \ell$.
   - **i.** Write the decryption algorithm $\mathsf{Dec}_k^1(c)$.
   - **ii.** Prove that this mode does not yield IND-CPA security, no matter how good E is. *Hint. Show that an adversary can check, given the encryption of $m = m_1 \| m_2$, whether $m_1 = m_2$, and turn this into an advantage in the IND-CPA game.*
2. Let $\mathsf{Enc}_k^2(m) = c_0 \| \cdots \| c_\ell$ where for $1 \leq i \leq \ell$, $c_i = r_i \oplus m_i$ with $r_i = E_k(r_{i-1})$ and $r_0 = c_0$.
   - **i.** Write the decryption algorithm $\mathsf{Dec}_k^2(c)$.

   We assume now that E_k is replaced by a random function $f : \{0,1\}^n \to \{0,1\}^n$.
   - **ii.** Justify, intuitively, that an adversary cannot obtain any information on the input message m from the ciphertext c alone.

Exercise 3 (10 points). *Feistel networks*

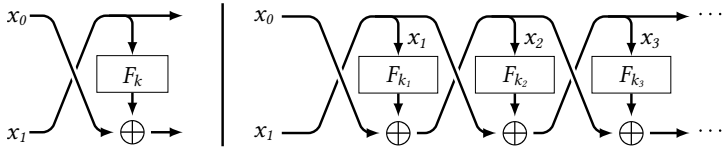

Figure 1: A Feistel round (left) and a Feistel network (right)[1]

A *Feistel round* turns a function $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ into a block cipher $E : \{0,1\}^\kappa \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ as follows: $E_k(x_0\|x_1) = x_1\|(F_k(x_1) \oplus x_0)$, where $x_0, x_1 \in \{0,1\}^n$, $\|$ denotes the concatenation and $\oplus$ the bitwise XOR.

1. **i.** Prove that E is a block cipher, that is E_k is a permutation for each k. *Hint. Describe the computation of* $E_k^{-1}(\cdot)$.

ii. Prove that E is *not* a secure block cipher: an adversary can distinguish E_k from a random permutation by making one query, with very good probability.

An r-round *Feistel network* turns $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ into a block cipher $E : \{0,1\}^{r\kappa} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ as follows: let $k = k_1\|\cdots\|k_r$ be the $r\kappa$-bit key, $x_0\|x_1$ the $2n$-bit message, and $x_{\ell+1} = F_{k_\ell}(x_\ell) \oplus x_{\ell-1}$ for $1 \le \ell \le r$; then $E_{k_1\|\cdots\|k_r}(x_0\|x_1) = x_r\|x_{r+1}$.

We prove that a 3-round Feistel network satisfies a PRF security. **We assume that each F_{k_ℓ} is replaced by a function $f_\ell : \{0,1\}^n \to \{0,1\}^n$ sampled uniformly at random in the set of functions from $\{0,1\}^n$ to itself. The probabilities are taken over these random choices.**

Let $\mathcal{A}$ be an adversary that makes q queries $m^1, \ldots, m^q$ where $m^i = x_0^i\|x_1^i$ for $1 \le i \le q$, and let $x_{\ell+1}^i = f_\ell(x_\ell^i) \oplus x_{\ell-1}^i$ for $\ell = 1$ to 3. We assume that the queries are pairwise distinct.

2. **i.** Justify that if the x_2^is are pairwise distinct, the x_3^is are independent and uniform. *Hint. One-time pad.*

ii. Let $1 \le i < j \le q$. Prove that $\Pr\left[x_2^i = x_2^j\right] \le 1/2^n$. *Hint. Consider two distinct cases* $x_1^i = x_1^j$ *and* $x_1^i \ne x_1^j$.

iii. Conclude that $\Pr\left[\exists i \ne j, x_2^i = x_2^j\right] \le q(q-1)/2^{n+1}$.

We admit similarly that $\Pr\left[\exists i \ne j, x_3^i = x_3^j\right] \le q(q-1)/2^{n+1}$, and that if the x_3^is are pairwise distinct, the x_4^is are independent and uniform.

3. Conclude that the adversary cannot distinguish $E_{k_1\|k_2\|k_3}$ from a random function with probability more than $q(q-1)/2^n$.

[1] Source: M. Rosulek, *The Joy of Cryptography*, https://joyofcryptography.com.