Final exam

The duration of the exam is 3 hours. The grading scale (on 40 points) is indicative and subject to change. No document nor any digital device is allowed. The exercises are largely independent, although the last three ones are all about a same signature scheme. 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. ***You can answer in French or English.***

Notations and probability reminder.

- The concatenation of two strings u and v is denoted by $u\|v$.
- For a set S, $x \twoheadleftarrow S$ means that x is chosen *uniformly at random* from S, *independently from any other random choice*.
- For two events E and F, $\Pr[E \vee F] \le \Pr[E] + \Pr[F]$ (*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 $q \le \sqrt{N}$. Then $\Pr\left[\exists i \neq j, y_i = y_j\right] \ge \frac{q(q-1)}{4N}$ and $\Pr\left[\exists i, j, y_i = z_j\right] \ge \frac{q^2}{2N}$ (*birthday bounds*).

Exercise 1. (7 pts)

1. Classify the following primitives into two categories, *deterministic* and *randomized*: block cipher, symmetric encryption scheme, hash function, Message Authentication Code (MAC), key exchange, public-key encryption scheme, digital signature.
2. Let G be a cyclic group of generator g. Define the *discrete logarithm (in base g)* of an element $h \in G$.
3. Let $N = p \times q$ for two distinct primes p and q. How many elements of $\mathbb{Z}/N\mathbb{Z}$ are *invertible modulo N*? *The answer must be expressed in terms of p and q.*
4. **i.** What is the role of a MAC?
   ii. How is called the primitive that combines the functionalities of an encryption scheme and a MAC?
5. Let $G = (\mathbb{Z}/29\mathbb{Z}^\times, \times)$ be the multiplicative group of invertible elements of $\mathbb{Z}/29\mathbb{Z}$. In this group, $g = 2$ is a generator. You perform a Diffie-Hellman key exchange with Alice: she has randomly drawn a secret value a and publishes $h_A = g^a$. You randomly draw a secret value b.
   i. What value do you need to publish to finish the key exchange?
   ii. What is the secret you and Alice finally share?
   iii. If $h_A = 7$ and $b = 4$, what is the value of the shared secret?

Exercise 2. (10 pts) *CFB mode of operation*

Let $E_k : \{0,1\}^n \to \{0,1\}^n$ be a block cipher with block length n. The *cipher feedback* (CFB) mode of operation is defined as follows: The encryption of a message $m = m_1\|\cdots\|m_t$ of length $t \times n$ is $c = c_0\|\cdots\|c_t$ (of length $(t+1) \times n$) where $c_0 = IV$ is an initialization vector and $c_i = m_i \oplus E_k(c_{i-1})$ for $i = 1$ to t.

1. **i.** Represent graphically the encryption of a message $m = m_1\|m_2\|m_3$ using the CFB mode of operation.
   ii. Give the decryption algorithm, *both schematically and in pseudo-code*.
2. **i.** To make a good mode of operation, should the initialization vector be fixed or random? Justify.
   ii. How can we encrypt a message whose length is not a multiple of n? Propose an explicit solution for the encryption and the decryption.
3. Let $m = m_1\|\cdots\|m_t$ be a message and $c_0\|\cdots\|c_t$ be a corresponding ciphertext. *Assume that E_k is a random permutation.*
   i. Prove that if there exists $i \neq j$ such that $c_i = c_j$, then $m_{i+1} \oplus m_{j+1} = c_{i+1} \oplus c_{j+1}$.
   ii. Justify that the ciphertext blocks $c_0, \ldots, c_t$ are uniform in $\{0,1\}^n$.
   iii. Give a value for t such that with probability $\ge \frac{1}{4}$, there exists $i \neq j$ such that $c_i = c_j$.
4. In the $\mathsf{IND-CPA}$ experiment for an encryption scheme, the adversary has oracle access to the encryption scheme and produces two equal-length messages m_0 and m_1. The challenger computes $c \leftarrow \mathsf{Enc}_k(m_b)$ where $b \twoheadleftarrow \{0,1\}$. Given c, the adversary outputs b'. Its advantage is $|\Pr[b' = 1|b = 1] - \Pr[b' = 1|b = 0]|$.

Describe an adversary for the $\mathsf{IND-CPA}$ experiment, when the encryption scheme is based on the CFB mode of operation, that has an advantage $\geq \frac{1}{4}$. *Be precise on the description of the messages m_0 and m_1 used in the attack, in particular their common length.*

Problem: Lamport signatures

A function $f : X \to Y$ is said *one-way* if there exists an efficient algorithm to compute it, but f is *hard to invert*. This notion is formalized in Exercise 5. A *Lamport signature*, or *one-time signature*, is a digital signature scheme built using a *one-way function*.

Definition Let $f : X \to Y$ be a fixed one-way function. Let $\mathcal{M} = \{0,1\}^k$ be the message space.

- The **secret and public keys** are

$$sk = \begin{pmatrix} x_1^{(0)} & x_2^{(0)} & \cdots & x_k^{(0)} \\ x_1^{(1)} & x_2^{(1)} & \cdots & x_k^{(1)} \end{pmatrix} \quad \text{and} \quad pk = \begin{pmatrix} y_1^{(0)} & y_2^{(0)} & \cdots & y_k^{(0)} \\ y_1^{(1)} & y_2^{(1)} & \cdots & y_k^{(1)} \end{pmatrix}$$

  where for $1 \leq i \leq k$ and $j \in \{0,1\}$, $x_i^{(j)} \twoheadleftarrow X$ is uniform in X and $y_i^{(j)} = f(x_i^{(j)})$.
- The **signature** $\mathsf{Sign}_{sk}(m)$ of a message $m = m_1 \| \ldots \| m_k \in \mathcal{M}$ (where each $m_i \in \{0,1\}$) is $\sigma = (x_1^{(m_1)}, x_2^{(m_2)}, \ldots, x_k^{(m_k)})$.

Exercise 3. (6 pts)

1. Let $X = \{1,\ldots,6\}$ and $f : X \to X$ defined by $f(x) = 3^x \bmod 7$. Let $sk = \left(\begin{smallmatrix} 2 & 3 & 5 \\ 3 & 4 & 1 \end{smallmatrix}\right)$, hence $k = 3$.
  i. Compute the corresponding public key pk.
  ii. Compute the signature of the message 011.
  iii. Is $(3,4,1)$ a valid signature for the message 101?

2. **i.** Describe the verification algorithm. *The algorithm must be completely specified, including its inputs.*
  ii. Under which condition is the verification algorithm *sound*, that is no invalid signature can be accepted?

3. Provide a two-chosen-message key recovery attack on the Lamport signature scheme. *That is, an adversary that can make two signature queries of its choice can compute the private key.*

Exercise 4. (4 pts) *Extending the message space*

In the original signature scheme, the space of messages is fixed to $\{0,1\}^k$. We want to use the signature scheme with message of length *at most k*. For, the signature of a message m of length $\ell \leq k$ is $(x_1^{(m_1)}, \ldots, x_\ell^{(m_\ell)})$.

1. Give a one-chosen-message existential forgery attack on this variant. *That is, after one chosen query m, an adversary produces a valid pair (m', σ') with $m \neq m'$.*

2. Propose a variant of the signature scheme that allows to sign any message of length $\leq k$, with a public key of size $2(k + \lceil \log k \rceil)$. Argue that it prevents the previous attack. *Hint: Authenticate both the message and its length.*

Exercise 5. (13 pts) *Proof of security*

To formalize the notion of *one-way* function $f : X \to Y$, we define the *one-way experiment*:

1. a challenger samples $x \twoheadleftarrow X$ and computes $y = f(x)$;
2. the adversary $\mathcal{A}$ is given y and oracle access to f, and outputs x'.

The advantage of $\mathcal{A}$ is $\mathsf{Adv}_f^{\mathsf{OW}}(\mathcal{A}) = \Pr[f(x') = y]$.

1. **i.** To which notion of security for hash functions corresponds the notion of one-way function?
  ii. Define an *advantage function* $\mathsf{Adv}_f^{\mathsf{OW}}(t)$ for the one-way experiment.

We formalize a security definition for *one-time signatures*, using the *one-time signature experiment* for a signature scheme $(\mathsf{Sign}, \mathsf{Vrfy})$:

1 a challenger generates a pair of keys (sk, pk);
2 the adversary $\mathcal{A}$ is given pk and sends a single query $m \in \{0,1\}^k$ to the challenger
3 the challenger sends back $\sigma \leftarrow \mathsf{Sign}_{sk}(m)$;
4 the adversary outputs a pair (m', σ') with $m' \neq m$.

2. **i.** What is the difference with the existential unforgeability experiment?
  ii. Define the advantage $\mathsf{Adv}_{\mathsf{Sign}}^{\mathsf{OT}}(\mathcal{A})$ for $\mathcal{A}$ in this experiment, by analogy with the advantage for the existential unforgeability experiment. *The advantage must be an real number between 0 and 1.*

iii. Define an advantage function $\mathsf{Adv}^{\mathsf{OT}}_{\mathsf{Sign}}(t)$ for one-time signatures. Why is there no "q" in the definition? We now prove that given an adversary $\mathcal{A}$ for the one-time signature scheme, we can build another adversary $\mathcal{A}'$ for the one-way experiment. All we know about $\mathcal{A}$ is that it is given a public key pk, asks a query m and gets back $\sigma = \mathsf{Sign}_{sk}(m)$, and finally outputs a pair (m', σ') where $m' \neq m$. The adversary $\mathcal{A}'$ will *simulate* $\mathcal{A}$, answering its single query. Its formal description is below.

```
ALGORITHM $\mathcal{A}'$:
  Input: $y \in Y$
  Output: $x \in X$ such that $f(x) = y$, or FAILURE
  $(sk, pk) \leftarrow \left( \begin{pmatrix} x_1^{(0)} & \cdots & x_k^{(0)} \\ x_1^{(1)} & \cdots & x_k^{(1)} \end{pmatrix}, \begin{pmatrix} y_1^{(0)} & \cdots & y_k^{(0)} \\ y_1^{(1)} & \cdots & y_k^{(1)} \end{pmatrix} \right)$    # key generation as in the Lamport signature scheme
  $i^* \twoheadleftarrow \{1, \ldots, k\}$, $b^* \twoheadleftarrow \{0, 1\}$ and $y_{i^*}^{(b^*)} \leftarrow y$    # replace one randomly chosen entry of the public-key by $y$
  $(m', \sigma') \leftarrow \mathcal{A}(pk)$    # run $\mathcal{A}$, answering its signature request on $m$ with $\sigma = (x_1^{(m_1)}, \ldots, x_k^{(m_k)})$
  If $m'_{i^*} = b^* \neq m_{i^*}$: return $\sigma'_{i^*}$
  Else: return FAILURE
```

3. **i.** Prove that if $\mathsf{Vrfy}_{pk}(m', \sigma') = 1$ and $b^* = m'_{i^*}$, $\mathcal{A}'$ does output a value x such that $f(x) = y$.

ii. Prove that if $b^* \neq m_{i^*}$, the probability that $\mathsf{Vrfy}_{pk}(m', \sigma') = 1$ is exactly $\mathsf{Adv}^{\mathsf{OT}}_{\mathsf{Sign}}(\mathcal{A})$.

iii. Prove that the probability that $m'_{i^*} = b^* \neq m_{i^*}$ is $\frac{1}{2k}$. *Hint: $\mathcal{A}$ does not know the value of i^* and b^*.*

iv. Conclude that $\mathsf{Adv}^{\mathsf{OW}}_{f}(\mathcal{A}') = \frac{1}{2k} \mathsf{Adv}^{\mathsf{OT}}_{\mathsf{Sign}}(\mathcal{A})$.

4. **i.** Deduce an *inequality* between $\mathsf{Adv}^{\mathsf{OW}}_{f}(t)$ and $\mathsf{Adv}^{\mathsf{OT}}_{\mathsf{Sign}}(t)$. Why isn't this an equality?

ii. Explain, in plain English/French, why the previous question proves the following informal statement: *If f is a one-way function, then the Lamport signature is a secure one-time signature scheme.*