HW2: Public Key Cryptography

This homework is due before Monday, April 8th at 1pm.
You can either hand your copy before the exam or submit it by email at:
`alain.passelegue@ens-lyon.fr;arthur.herledan_le_merdy@ens-lyon.fr`
Late submissions will receive a 2-point penalty for each day after the due date.

Exercise 1.
Let $H : \{0,1\}^{2n} \mapsto \{0,1\}^n$. We say that H is second-preimage resistant if for all efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$ succeeds in the following experiment is negligible. It is given $x \leftarrow U(\{0,1\}^{2n})$ and it has to find $x' \neq x$ such that $H(x') = H(x)$.

1. Recall the definition of collision resistance. Show that collision resistance implies second-preimage resistance.

2. Assume that there exists a second-preimage resistant $H : \{0,1\}^{2n} \mapsto \{0,1\}^n$. Show that there exists a second-preimage resistance H' that is not collision-resistant.

Exercise 2.
Let $N = pq$ with p and q primes of identical bit-size, and ϕ be the Euler function. We first want to study the algebraic structure of $(\mathbb{Z}/N^2\mathbb{Z})^\star$.

1. Show the following propositions:
   1. $\gcd(N, \phi(N)) = 1$.
   2. For any $a \in (\mathbb{Z}/N\mathbb{Z})$, $(1+N)^a = (1+aN) \bmod N^2$.
   3. $(1+N)$ has order N mod N^2.
   4. $(\mathbb{Z}/N^2\mathbb{Z})^\star$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^\star$ with the following function $f(a,b) = (1+N)^a \cdot b^N \bmod N^2$.

2. We say that an element x of $(\mathbb{Z}/N^2\mathbb{Z})^\star$ is a *residue* if it can be written as an N-th power (that is, $x = y^N \bmod N^2$ for some $y \in (\mathbb{Z}/N^2\mathbb{Z})^\star$). Show that the set of residues of $(\mathbb{Z}/N^2\mathbb{Z})^\star$ is isomorphic to
$$\{(a,b) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^\star \mid a = 0\}.$$

We define the Decisional Composite Residue problem (DCR) as follows: the goal of an adversary $\mathcal{A}$ is to distinguish with non-negligible advantage between $r^N \bmod N^2$ and $r \bmod N^2$, where r is sampled uniformly in $(\mathbb{Z}/N^2\mathbb{Z})^\star$.

3. Show that if an adversary knows the factorisation of N, then he can solve the DCR problem.

We now define the Paillier's Encryption scheme. The public key pk of the scheme is $N = pq$ with p and q prime, and the secret key sk is $\phi(N)$ and $\phi(N)^{-1} \bmod N$. For a message $m \in (\mathbb{Z}/N\mathbb{Z})$, the encryption algorithm picks $r \in (\mathbb{Z}/N\mathbb{Z})^\star$ at random and returns:
$$\mathrm{Enc}_{pk}(m) = (1+N)^m \cdot r^N \bmod N^2.$$

4. Give a decryption function.

5. Show that if the DCR problem is hard, then Paillier's encryption is IND-CPA secure.

6. Show that this scheme is additively homomorphic, i.e., that given the public key and the encryptions of two messages m_1 and m_2, one can compute a valid ciphertext for $m_1 + m_2$. That is, given $ct_1 = \mathrm{Enc}_{pk}(m_1)$ and $ct_2 = \mathrm{Enc}_{pk}(m_2)$, explain how to obtain ct_{1+2} such that $\mathrm{Dec}_{sk}(ct_{1+2}) = m_1 + m_2$. Is it an interesting property?

7. Show a similar property for the ElGamal encryption scheme.

   Hint: prove the same for the group law $*$ of $\mathbb{G}$. Then, explain also how we can obtain the same for the addition $+$ over $\mathbb{Z}_p$ assuming the plaintexts are small over $\mathbb{Z}_p$ (e.g., $\text{poly}(\lambda)$).

Exercise 3.
The notion of existential unforgeability under single-message attack for a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{V})$ states that no adversary can output a valid tuple (m', σ) with non-negligible probability by only querying once the signing oracle for m with $m \neq m'$.
The goal of this exercise is to go from euSMA-security to euCMA-security. The idea is, for each bit of the message, to generate two new public keys, sign them using the public key from the previous bit, and use one of them for the next bit (depending on the value of the current bit). This can be seen as building a binary tree.
Let F be a secure PRF. It will come in handy to make sure we use the same randomness to generate the keys (so that we do not have memory to store them, from one signature to the next one).
We assume the following about the PRF: its output is long enough to be given to Gen as randomness seed, and there is some one-to-one deterministic padding in the case where the input is too small.
Here is the construction, where $m_{|i}$ denotes the first i bits of m and $m_{|0}$ is the empty word ε:

$\mathsf{Gen}^\star(1^\lambda)$**:** Generate $(vk_\varepsilon, sk_\varepsilon) \leftarrow \mathsf{Gen}(1^\lambda)$ and two PRF keys k, k'. Return $vk = vk_\varepsilon$ and $sk = (sk_\varepsilon, k, k')$.

$\mathsf{Sign}^\star(sk, m)$**:** Let $n = |m|$. For $i = 0$ to n do the following: Compute $r_{m_{|i}|0} := F(k, m_{|i}|0)$, and $r_{m_{|i}|1} := F(k, m_{|i}|1)$. Then generate $vk_{m_{|i}|1}, sk_{m_{|i}|1} \leftarrow \mathsf{Gen}(1^\lambda; r_{m_{|i}|0})$ and $vk_{m_{|i}|0}, sk_{m_{|i}|0} \leftarrow \mathsf{Gen}(1^\lambda; r_{m_{|i}|1})$. Then, sign $\sigma_{m_{|i}} \leftarrow \mathsf{Sign}(sk_{m_{|i}}, (\mathsf{vk}_{m_{|i}|0}, \mathsf{vk}_{m_{|i}|1}); r'_{m_{|i}})$, where $r'_{m_{|i}} \leftarrow F(k', m_{|i})$.

Compute $\sigma_m \leftarrow \mathsf{Sign}(\mathsf{sk}_m, m; F(k', m))$.

Then, return $\Big(\{\sigma_{m_{|i}}, vk_{m_{|i}|0}, vk_{m_{|i}|1}\}_i, \sigma_m\Big)$.

1. Give a verification algorithm $\mathsf{V}^\star$. How many times does it call V, depending on the message size? How many public keys are manipulated (i.e. generated, used to sign or signed) during one call to $\mathsf{Sign}^\star$?

In order to prove the euCMA-security of this scheme, we introduce the following hybrid H_1: the game is the same as in the euCMA setup (we will call it H_0), except that $F(k, \cdot)$ is replaced by a truly random function, whose table is built adaptively.

2. Show that H_0 and H_1 are indistinguishable.

Then we introduce H_2, which is as H_1 except that this time $F(k', \cdot)$ is replaced by a truly uniform function, whose table is also built adaptively.

3. Show that H_1 and H_2 are indistinguishable.

4. Show that under the euSMA security of the base signature, no adversary has non-negligible advantage in the game H_2.

5. Conclude.