TD 9 – The RSA ecosystem

Exercise 1. *Attacks on textbook RSA*

We present a few attacks on the original RSA encryption and signature schemes, that directly use the RSA trapdoor function. The RSA trapdoor function uses a public key (N, e) and a private key (N, d), where $N = p \times q$ for two distinct primes p and q, and $ed \bmod \varphi(N) = 1$ where $\varphi(N) = (p-1)(q-1)$. The trapdoor function is $m \mapsto m^e \bmod N$ where $m \in \mathbb{Z}/N\mathbb{Z}$ and its inverse is $c \mapsto c^d \bmod N$.

1. We consider the original RSA encryption scheme.
   - **i.** Describe an adversary $\mathcal{A}$ that, given the public key (N, e) and a ciphertext c, is able to compute m such that $m^e \bmod N = c$ using a *chosen ciphertext attack*. *Hint: What queries are allowed for $\mathcal{A}$?*
   - **ii.** Assume that Alice uses the keys (N, e_A) and (N, d_A), and Bob the keys (N, e_B) and (N, d_B), *where the modulus N is the same in both pairs*, and $\text{GCD}(e_A, e_B) = 1$. An adversary intercepts two ciphertexts c_A and c_B, both encryptions of a same message m but under Alice's and Bob's keys respectively. Prove that it can compute m. *Specify the algorithm used by the adversary.*
2. We now consider the original RSA signature scheme.
   - **i.** Recall the attack in which an adversary is given two valid pairs (m_1, σ_1) and (m_2, σ_2) and forges a new valid pair (m, σ) with $m \notin \{m_1, m_2\}$.
   - **ii.** Propose as a variant of the attack a universal forgery using one chosen-message query: *The adversary wants to sign a message m, and is allowed to query the signature of another message $m' \neq m$.*

Exercise 2. *Padded RSA signature*

Let (N, e) and (N, d) be verification and signing RSA keys, where N is n-bit long. We consider a padded RSA signature scheme, for messages of length $\ell < n$. To sign $m \in \{0,1\}^\ell$, we take a uniform $r \twoheadleftarrow \{0,1\}^{n-\ell}$ such that $r\|m \in \mathbb{Z}/N\mathbb{Z}$ and compute $\sigma = (r\|m)^d \bmod N$.

1. Why could $r\|m \notin \mathbb{Z}/N\mathbb{Z}$ happen? What is the probability that this happens? How to deal with this?
2. Describe the verification algorithm for this protocol.
3. Show that this signature scheme is not secure. *Hint: One of the attacks against the original RSA signature scheme still applies.*

Exercise 3. *Attacks on RSA-FDH*

In RSA-FDH, the signature of a message $m \in \{0,1\}^*$ with a key (N, d) is $H(m)^d \bmod N$ for some hash function H. The verification of a signature σ with the key (N, e) checks whether $H(m) = \sigma^e \bmod N$. This scheme is proven secure if H is a random oracle. We sketch attacks when H is not resistant enough.

1. Assume that H is not first preimage resistant. Adapt the attack of the original RSA signature scheme to this case.
2. Assume that H is not second preimage resistant. Prove that an adversary with a signature oracle can perform a universal forgery.
3. Assume that H is not collision resistant. Prove that an adversary with a signature oracle can perform an existential forgery.