The RSA ecosystem

Exercise 1. *Attacks on textbook RSA*

Using the RSA trapdoor function directly as an encryption scheme or a signature scheme is insecure. We present a few more attacks in this exercise. We remind that 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 $m \in \mathbb{Z}/N\mathbb{Z}$. The inverse function, kwowing the trapdoor d, is $c \mapsto c^d \bmod N$.

1. We consider the original RSA encryption scheme.
   - **i.** We first design a chosen ciphertext attack. Describe an adversary that, given the public key (N,e) and a ciphertext c, is able to compute m such that $m^e \bmod N = c$. *Hint: What does "chosen ciphertext attack" mean?*
   - **ii.** We now show that using two keys with the same modulus N is insecure. Let us assume that Alice has the pair of keys $((N,e_1),(N,d_1))$ and Bob the pair $((N,e_2),(N,d_2))$. We further assume that $\text{GCD}(e_1,e_2) = 1$.
     An adversary intercepts two ciphertexts c_1 and c_2, both encryptions of a same message m but under Alice's and Bob's keys respectively. Prove that the adversary 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. *That is, the adversary chooses to sign a message m, and to this end is allowed to query the signature of one message $m' \neq m$.*

Exercise 2. *Padded RSA signature*

Let (N,e) and (N,d) be public and private 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 private key (N, d) is $H(m)^d \bmod N$ for some hash function H. The verification of a signature σ with the public 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.