Due Date: 19 Nov 2023 CS6160: Cryptology

Assignment 2

1. Let p, q be primes such that q divides $p-1$, and let $g \in \mathbb{Z}_p^*$ be such that $g^q = 1$. Suppose that there is an algorithm A, that, given the value of g^α, can compute $g^{\frac{1}{\alpha}}$, for every input α (here $\frac{1}{\alpha}$ is computed modulo q). Describe an algorithm using A as a subroutine, that given the values of g^α, g^β finds the value of $g^{\alpha\beta}$.

2. Consider three users who have RSA public keys $(N_1, 3), (N_2, 3), (N_3, 3)$, i.e they all use $e = 3$, with $N_1 < N_2 < N_3$. A message $m \in \{0,1\}^n$ is encrypted and sent to each of the users, as follows: A random $r \in \mathbb{Z}_{N_1}^*$ is chosen and the ciphertext is the tuple

$$\left(r^3 \bmod N_1, r^3 \bmod N_2, r^3 \bmod N_3, H(r) \oplus m\right),$$

where H is a hash function from $\mathbb{Z}_{N_1}^*$ to $\{0,1\}^n$. Show that an adversary who sees the ciphertext can recover m.

3. Let f be a one-way permutation on $\{0,1\}^n$. Consider the following signature scheme for the message space $M = \{1, \ldots, n\}$: the private key is a random value $x \in \{0,1\}^n$, and the public value is $f^{(n)}(x)$, where $f^{(j)}(x)$ denotes the value obtained by applying f iteratively j times, $f^{(0)}(x) = x$.

   For $i \in M$, $Sign(i) = f^{(n-i)}(x)$.

   (a) How can the receiver verify the signature?

   (b) Show that this scheme is not one-time secure.

4. Consider the following containment-free variant of Lamport signatures: the private key consists of $2t$ values $x_1, \ldots, x_{2t}$ and the public key consists of the corresponding hashes $y_1, \ldots, y_{2t}$, where $y_i = H(x_i)$. A message $m \in \{0,1\}^n$ is mapped injectively to a subset $S_m \subseteq \{1, 2, \ldots, 2t\}$ of size k. $Sign(m) = \{x_i\}_{i \in S_m}$.

   (a) For what value(s) of k is the scheme one-time secure?

   (b) How big can n be in terms of t?