

Cryptographic Protocols

SS 2017

Handout 1

Exercises marked () will be checked by tutors.*

We encourage submissions of solutions by small groups of up to four students.

Exercise 1 (4 points):

(*) Let $X = \{0, \dots, n-1\}$ be a set with n elements for some $n \in \mathbb{N}$. Assume, that we are able to choose bits $b \leftarrow \{0, 1\}$ uniformly at random. Construct an algorithm that chooses $x \leftarrow X$ uniformly at random and prove the correctness of your construction.

Exercise 2 (4 points):

(*) In this exercise we will consider the RSA signature scheme.

- Construct a ppt adversary, that wins the Sig – Forge game against the textbook RSA signature scheme without any signature queries with probability 1. Forgeries for $m \in \{-1, 0, 1\}$ are not allowed.
- Let $N = p \cdot q$ be the product of two distinct primes. Show that computing $\phi(N)$ is not easier than factoring N , i. e. show how to recover p and q if N and $\phi(N)$ are given.

Exercise 3:

Let $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be a one-way permutation, i. e. a length-preserving one-way function, which is bijective when restricted to $\{0, 1\}^n$ for some n . Consider the following signature scheme for the message space $\mathcal{M} = \{1, \dots, n\}$:

- Gen chooses the secret key uniformly at random $sk \leftarrow \{0, 1\}^n$ and the public key is computed as $pk := f^n(sk) = \underbrace{f \circ \dots \circ f}_{n \text{ times}}(sk)$.
- $\text{Sign}_{sk}(i)$ for $i \in \mathcal{M}$ outputs $\sigma := f^{n-i}(sk)$ (where $f^0(sk) := sk$).
- $\text{Vrfy}_{pk}(i, \sigma)$ for $i \in \mathcal{M}$ tests if $pk \stackrel{?}{=} f^i(\sigma)$.

- Show that the above scheme is not a one-time signature scheme. Given a signature on a message $i \in \mathcal{M}$, for what messages j can your adversary output a forgery?
- Prove that no ppt adversary given a signature on i can output a forgery on any messages $j > i$ except with negligible probability.
- Suggest how to modify the scheme so as to obtain a 1-time signature scheme. (Extend the private and the secret keys in such a way, that the security is based on the fact proven in (b)).

Exercise 4:

The following informal definitions of security for hash functions have been presented in the lecture:

- Second pre-image resistance: A hash function is second pre-image resistant, if given s and x it is infeasible for a probabilistic polynomial-time adversary to find $x' \neq x$ such that $H^s(x') = H^s(x)$.
- Pre-image resistance: A hash function is pre-image resistant if given s and $y = H^s(x)$ for a randomly chosen x , it is infeasible for a probabilistic polynomial-time adversary to find a value x' such that $H^s(x') = y$.

Provide formal definitions for second pre-image and pre-image resistance similarly to the security definitions introduced in the lecture.

Exercise 5 (4 points):

(*) Prove formally that any hash function that is collision resistant is also second pre-image resistant.

Is every collision-resistant function pre-image resistant? Prove your answer.