Cryptography for Computer Scientists 2016/17 Nov 28, 2018

Exercises 9

Stefan Dziembowski MIM UW

Exercise 1: Facts about $Z^*_{N^2}$

Let N be an RSA modulus, i.e., $N = pq$ where $p \neq q$ are odd primes of equal length (in binary).

1. Prove that $N \perp \varphi(N)$.
2. Show that $\mathbb{Z}_N \times \mathbb{Z}^*_N$ is isomorphic to $\mathbb{Z}^*_{N^2}$ with isomorphism $f : \mathbb{Z}_N \times \mathbb{Z}^*_N \to \mathbb{Z}^*_{N^2}$ given by

$$f(a, b) = (1 + N)^a \cdot b^N \bmod N^2.$$

Exercise 2: Merkle Puzzles

For $t \in \mathbb{N}$ a $t-$*puzzle* is an algorithm $\mathsf{puzzle} : \{0,1\}^* \to \{0,1\}^*$ that satisfies the following properties:

- puzzle is an injective functions,
- computing puzzle takes constant time,
- for every $y = \mathsf{puzzle}(x)$ finding the value of x takes exactly expected time t, i.e., (a) an honest user can find x in expected time t, and (b) every adversary that finds x with probability 1 needs to work expected time t.

(Here the notion of *time* refers to some abstract computational model that does not matter here.)

1. For any t that is a power of 2 show how a t-puzzle can be implemented using block ciphers (modeling a block cipher as a black-box).
2. Using t-puzzles (and no other cryptographic primitives) show (for any $n \in \mathbb{N}$) a key exchange protocol that has the following properties:
   - the total work of honest users is $t + n$ and
   - *weak security:* every adversary that learns the agreed key K with probability 1 needs to work expected time tn.

Exercise 3: Hash function for discrete log

Let G be a group of in which discrete log is computationally hard. Let $q = |G|$ and suppose q is prime. Let g, h be two generators of G such that $\log_g h$ is unknown. Show that a function $H : Z_q \times Z_q \to G$ defined as

$$H(a, b) := g^a h^b$$

is a collision-resistant hash function.