Cryptography (SS2006) Prof. Michael Backes

Exercise Sheet 7

Out: June 13, 2006 Saarland University

Problem 1: OWFs

Several variations of the definition of OWFs (Definition 9.1 in the lecture notes) could be taken into account. For each of the following two variations, show if the variation is stronger than the existing Definition 9.1 of OWFs, weaker than Definition 9.1, equivalent to Definition 9.1, or incomparable to Definition 9.1.

(a) Instead of "$\mathsf{F}(x) = \mathsf{F}(x')$" in the probability of Definition 9.1, write "$x' = x$".

(b) Instead of "$\mathsf{F}(x) = \mathsf{F}(x'); x \leftarrow_{\mathcal{R}} \{0,1\}^n,\ y := \mathsf{F}(x)$", write "$y = \mathsf{F}(x'); y \leftarrow_{\mathcal{R}} \{0,1\}^n$".

Problem 2: More Insecurities of Naive RSA

Let (N_1, e), (N_2, e) and (N_3, e) denote three (independent) RSA public keys, and assume that we have $e = 3$ for all of them. Assume further that the adversary sees the encryption of an arbitrary message m under all these public keys, i.e., it sees $c_1 := m^3 \bmod N_1$, $c_2 := m^3 \bmod N_2$, and $c_3 := m^3 \bmod N_3$. Show that having this information and the public keys already allows for efficiently retrieving the message m with probability one.

Problem 3: On Factoring N and Computing $\varphi(N)$

Let $N = pq$ be a publicly known RSA modulus. Prove that, given N, computing $\varphi(N)$ is equivalent to factoring N, i.e., if an efficient algorithm exists that computes $\varphi(N)$ given N, then there also exists an efficient algorithm for factoring N given N, and vice versa.

Problem 4: Hardcore Predicates

Let p be a prime and let g be a generator of $\mathbb{Z}_p^*$. Show that the predicate

$$\pi(x) := \begin{cases} 0 & \text{if } x < \frac{p}{2} \\ 1 & \text{if } x \geq \frac{p}{2} \end{cases}$$

is a hardcore predicate of $\mathsf{F}^{\mathsf{DLog}}(x) := g^x \bmod p$. In other words, show that if an efficient algorithm exists that computes $\pi(x)$ on input $p, g, g^x \bmod p$, then there exists an efficient algorithm for computing discrete logarithms in $\mathbb{Z}_p^*$.
Hint: Look at the corresponding posts on the board in forum "Lecture".