The art of cryptography: security, reductions, and group cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

12. Assignment

(Due: Sunday, 8 July 2012, 23^{59})

Exercise 12.1 (The Rabin cryptosystem)**.** We study a close relative of the RSA cryptosystem with a nice security reduction.

Algorithms 1: Rabin cryptosystem

gen
Input: security parameter n in unary
Output: public key: n-bit Blum integer $N = pq$; secret key: (p, q)

enc
Input: public key N and message $m \in \mathbb{Z}_N^\times$
Output: ciphertext $c = (m^2, \mathsf{par}, \mathsf{jac}) \in \mathbb{Z}_N^\times \times \mathbb{Z}_2 \times \{\pm 1\}$, where the two bits par and jac indicate the least-significant bit of m and the Jacobi symbol of m modulo N, respectively.

dec
Input: secret key (p, q) and ciphertext $c \in \mathbb{Z}_N^\times \times \mathbb{Z}_2 \times \{\pm 1\}$
Output: message $m \in \mathbb{Z}_N^\times$ or "failure"

(i) (4 points) Show that encryption and decryption can be done efficiently by specifying the respective steps and their costs. [Hint: You may assume a subroutine that computes the square root mod p for a prime p in time $O(\log^2 p)$.]

(ii) (2 points) Does the Rabin cryptosystem have malleable encryptions? Does it have indistinguishable encryptions?

(iii) (2 points) Let $\mathcal{A}$ be an adversary that decrypts ciphertexts of the Rabin cryptosystem with non-negligible probability $p_{\mathcal{A}}$. Turn this into an algorithm that computes square roots modulo N.

(iv) (4 points) Show how to turn an algorithm for computing square roots mod N into an algorithm to factor N. [Hint: Recall from last semester how a congruence of squares $x^2 = y^2 \mod N$ yields factors of N. The root extractor returns one of the four square roots, with an unknown and arbitrary distribution on them. Can this always be one that is useless for factoring?]

(v) (2 points) Use (iii) and (iv) to formulate a theorem that reduces the security of the RABIN cryptosystem to a well-known problem. Specify the attack goal and attacker resource for which this works.