Cryptography (SS2006) Prof. Michael Backes

Exercise Sheet 10

Out: July 4, 2006 Saarland University

Problem 1: Square Roots modulo Composites

Compute the square roots of 58 modulo 77.

Problem 2: Factoring and Computing Square Roots

Prove Lemma 13.5(a) in the lecture notes which says that computing square roots modulo a composite number $N = pq$ is as hard as factoring N. We already know that given the factorization of N one can compute square roots. Thus the following remains to be shown: Given an algorithm that computes square roots of randomly chosen elements modulo N with not negligible probability, construct an algorithm that factors N with not negligible probability.

Problem 3: Commitment Schemes

Consider the following commitment scheme, which is copied literally from the book "Applied Cryptography" by Bruce Schneier, page 87 of the second edition:

> *This protocol uses one-way functions.*
>
> *(1) Alice generates two random-bit strings, R_1 and R_2.*
>
> $$R_1, R_2$$
>
> *(2) Alice creates a message consisting of her random strings and the bit she wishes to commit to (it can actually be several bits).*
>
> $$(R_1, R_2, b)$$
>
> *(3) Alice computes the one-way function of the message and sends the result, as well as one of the random strings, to Bob.*
>
> $$\mathsf{H}(R_1, R_2, b), R_1$$
>
> *This transmission from Alice is evidence of commitment. Alice's one-way function in step (3) prevents Bob from inverting the function and determining the bit.*
>
> *When it comes time for Alice to reveal her bit, the protocol continues:*
>
> *(4) Alice sends Bob the original message.*
>
> $$(R_1, R_2, b)$$
>
> *(5) Bob computes the one-way function on the message and compares it and R_1, with the value and random string he received in step (3). If they match, the bit is valid.*

Answer the following questions:

(a) A (secure) commitment scheme has the properties correctness, binding, and hiding. Does the above scheme fulfill these properties? Explain.

(b) If you answered part (a) negatively: Modify the above scheme such that it fulfills these properties.

Hint: If one takes H to be the exponentiation function, how would one embed the bit b securely in the exponent?

Problem 4: Commitment Schemes II

Consider the Discrete Logarithm Commitment Scheme presented in Section 13.4.1. In the construction the committer verifies (i) that p, q are primes and (ii) that g and h have order q. Assume he does not perform one of these tests, can you find an attack against the security of the commitment scheme, i.e., against the hiding or the binding property?