Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse I

SS 2015

Blatt 2 / 7 Mai 2015

Aufgabe 1:
Given an RSA-pair (N, e) with corresponding CRT secret key (d_p, d_q), give an algorithm to factor N with running time $\widetilde{\mathcal{O}}(\min\{d_q, d_p\})$ and memory-complexity $\widetilde{\mathcal{O}}(1)$.

Aufgabe 2:
The Subset-Sum Problem. You are given a list of n positive integers $(M_1, \ldots, M_n)$ and another integer S. Find a subset of the elements in the list whose sum is S (we assume there is at least one such subset).
Devise a meet-in-middle type algorithm to solve the Subset-Sum Problem in time $\widetilde{\mathcal{O}}(2^{n/2})$ and space $\mathcal{O}(2^{n/2})$.

Aufgabe 3:
Given a group $\mathbb{G}$, an element $a \in \mathbb{G}$, and $b = \langle a \rangle$, the Discrete Logarithm Problem (DLP) asks to find x s.t. $b = a^x \mod \text{ord}(a)$.
Computational Diffie-Hellman Problem (CDH) ask to find a^{xy} when (a, a^x, a^y) are given. In the lecture, you were told about the ElGamal encryption scheme.
Show the following implications:

$$\textsc{ElGamal dec. oracle} \Leftrightarrow \text{CDH} \Leftarrow \text{DLP}.$$

.

Aufgabe 4:
Describe a chosen-ciphertext attack on Textbook ElGamal.