Exercise 4.1: (4 points)

(a) Compute all generators of $\mathbb{Z}_{23}^*$. 

(b) Apply the JACOBI algorithm to $\binom{356672}{487741}$.

Exercise 4.2: (4 points)

Construct a public-key system based on the following NP-complete problem:

**SUBSET PRODUCT**

*Input:* $A = (A_1, \ldots, A_n) \in \mathbb{N}^n$, and $B \in \mathbb{N}$.

*Problem:* Is there a subset $I \subseteq \{1, \ldots, n\}$ with $\prod_{i \in I} A_i = B$?

**Hint:** Add to the plaintext, coded as 0-1-sequence, an appropriated padding in order to ensure a necessary condition on the number of ones in the sequence.

Exercise 4.3: (4 points)

Let $c = E^{RSA}_e(w)$ be the ciphertext belonging to the plaintext $w$ if an RSA system is used. Assume that the public-key $e \leq 10$. Furthermore, assume there is an oracle that gives for the unknown plaintext $w$ and input $r > 0$ the value $c_r = E^{RSA}_e(w + r)$.

**Prove:** The plaintext can be decrypted efficiently.

Exercise 4.4: (4 points)

Let $n = pq$ be an RSA modulus, $m$ be a plaintext, and $r$ be the order of $m$, i.e., $m^r \equiv 1 \pmod{n}$. Furthermore, let $r$ be even and $m^{r/2} \not\equiv -1 \pmod{n}$.

**Prove:** $\gcd(m^{r/2} - 1, n) \in \{p, q\}$.

---

**Deadline:** Wednesday, November 14, 2012, 15:00, in the lecture or in the letterbox in front of i1.