Exercise 2.1  
(4 points)

Discuss the security of the following protocol. A wants to send a message $m$ to B. For this, A and B generate $n$ strings of length $|m|$. Then, they send the following messages:

\[
\begin{array}{c}
A & m, a_1, \ldots, a_n \\
A & m \oplus a_1 \\
A & m \oplus a_1 \oplus b_1 \\
A & m \oplus a_2 \oplus b_1 \\
A & m \oplus a_2 \oplus b_2 \\
A & \vdots \\
A & m \oplus a_n \oplus b_{n-1} \\
A & m \oplus a_n \oplus b_n \\
A & m \oplus b_n \\
B & b_1, \ldots, b_n \\
\end{array}
\]

The protocol is an extension of the protocol without secure key-exchange presented in the lecture. Is this protocol for $n \geq 2$ secure?

Exercise 2.2  
(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 2.3**  
(4 points)

Let \( p_1, \ldots, p_n \) be distinct prime numbers, \( P = \prod_{i=1}^n p_i \), and \( A = (a_1, \ldots, a_n) \), where \( a_i = P/p_i \).

**Prove:** The knapsack problem with input \((A, \alpha)\) can be solved efficiently for all \( \alpha \in \mathbb{N} \).

**Exercise 2.4**  
(4 points)

A number \( \alpha \in \mathbb{N} \) is called *representable* by a knapsack vector \( A \) if the knapsack problem with input \((A, \alpha)\) is solvable.

**Prove:**

(a) Each knapsack vector \( B \) of length \( n \) has at least as many representable numbers as the knapsack vector \( A_n = (1, 2, 3, 4, \ldots, n) \), for all \( n \in \mathbb{N} \).

(b) Each knapsack vector \( B \) of length \( n \) has at most as many representable numbers as the knapsack vector \( A'_n = (1, 2, 4, 8, \ldots, 2^{n-1}) \), for all \( n \in \mathbb{N} \).

**Note:** In a knapsack vector \( A = (a_1, \ldots, a_n) \) all numbers \( a_i \) are distinct.

---

**Deadline:** Thursday, November 02, 2017, 10:15 a.m.,
in the lecture or in the box in front of the i1.