Walter Unger
Sascha Geulen

WS 2012/2013
October 24, 2012

Exercise
Algorithmic Cryptography

Sheet 2

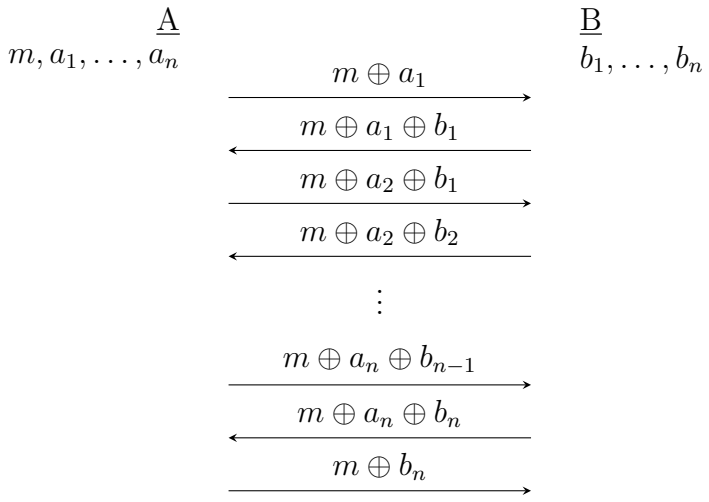
Exercise 2.1: **(4 points)**

(a) Compute $\gcd(54, 42)$.

(b) Compute the multiplicative inverse of 42 mod 55 using the extended Euclidean algorithm.

Exercise 2.2: **(4 points)**

Discuss the security of the following protocol. It is an extension of the protocol without secure key-exchange that uses One-Time-Pad and was presented in the lecture. Is this protocol secure?



Exercise 2.3: **(4 points)**

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

Prove:

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

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

Exercise 2.4: **(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, α) can be solved efficiently for all $\alpha \in \mathbb{N}$.

Deadline: Wednesday, October 31, 2012, 15:00,
in the lecture or in the letterbox in front of i1.