Selected Topics in Cryptography
Homework #2.
Deadline: November 21, midnight

Basic rules for submitting your homework:

- *the file has to be named: "firstname-lastname-HW2.pdf"*
- *put your name on the top of each page*
- *number the pages*
- *clearly mark which problem is being solved and list the solutions in the order of the problems from the assignment*
- *write the solutions carefully providing sufficient details; when in doubt, write more*
- *HW is to be turned in via* moodle *in the* pdf *format*
- *late homeworks only accepted in justified situations*

The total number of points in this HW is greater than 50 points. You cannot receive more than 50 points, so you may choose to just solve problems worth 50 pts. However, if you choose to do that, and some of your solutions turn out wrong or imperfect, you will loose points and will not receive the full 50 pts. On the other hand, if you choose to solve problems worth more than 50 points, even with some mistakes in some of the problems you may get enough done to earn the maximum of 50 points.

This homework is 'boring' - almost all the assigned problems are from textbooks, and you need to apply the material from the textbooks. However, cryptography is a practical subject and so acquiring skills is also important. The first two problems come from Chapter 8 of the more elementary textbook and from Chapter 10 of the textbook on number theory (from which we took the Knapsack Problem). The fifth and sixth problems are from Stinson's book.

1. (10 pts) Exercises 8.7.4, 8.7.8, 8.7.9, 8.7.10, and 8.7.20
2. (10 pts) Page 212, exercises 1, 3 (a), 5, 6, 7.
3. (10pts) Let $[a_1, a_2, a_3, \ldots, a_n]$ be a weight vector of different weights, and assume that you are solving an altered knapsack problem where you can choose not to use a weight a_i or use it once or use it twice (unlike the usual knapsack where you only have the options of using a weight once or not at all). Find a definition analogous to that of a super increasing sequence that, when applied to $[a_1, a_2, a_3, \ldots, a_n]$, would guarantee a fast solution for the altered knapsack problem for the sequence $[a_1, a_2, a_3, \ldots, a_n]$. Describe the solution algorithm and show your method on a reasonably sized example that requires using at least one of the weights twice.
4. (10pts) We say that a sequence $\{a_i\}$ increases with coefficient α if

$$\sum_{i=1}^{n} a_i \leq \alpha a_{n+1},$$

for all $n \geq 1$.

a) Is $\alpha = 1$ the smallest coefficient for which the knapsack problem becomes easy to solve?

b) If $\{a_i\}$ is an increasing sequence with coefficient $\alpha > 0$, find the smallest β such that

$$\liminf_{n\to\infty} \frac{a_n}{\beta^n} \geq 1$$

5. (15pts) Page 246, exercises 6.5, 6.7, 6.8, 6.9, 6.10.
6. (5pts) Page 247, exercise 6.13.

6. (2pts) Determine the Jacobi symbol $(\frac{22233}{18566})$.

7. (5pts) Search the web to determine which are the currently recommended values for the numbers used in the RSA, the Rabin, and the El Gamal Cryptosystems. Write a short summary, explain whether you believe the values you have found are those actually used today, and of course cite the source of your information in each case.