Norwegian University of Science and Technology
Department of Mathematical Sciences

Contakt during exam:
Kristian Gjøsteen 73 55 02 42/73 59 35 20

EXAM IN TMA4155 CRYPTOGRAPHY, INTRODUCTION

English
Saturday, December 2, 2006
Time: 0900-1300
Permitted aids: approved calculator

Problem 1 In this task, we shall consider the RSA public key $(589, 403)$.

a) Given that $589 = 19 \cdot 31$, find the corresponding RSA private key.

b) Explain the basic RSA signature scheme. Compute a signature for the message $m = 2$. Give a brief explanation of some of the security problems with this simple scheme.

Problem 2

a) Use the Chinese Remainder Theorem to find a solution to the following system:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

b) Use the Pohlig-Hellman algorithm to compute the discrete logarithm of 11 to the base 3 modulo 31.

c) Factor 253 using Pollard's $p - 1$ method.

Problem 3

a) Explain how the Diffie-Hellman key agreement protocol works and what its purpose and main properties are. Give an example with $p = 17$ and $g = 2$.

b) What is the man-in-the-middle attack on Diffie-Hellman? Give an example with $p = 17$, $g = 2$. Sketch one counter-measure against this attack.

Problem 4

a) Explain what a hash function is, and what preimage, second preimage and collision resistant means in this context.

As a building block for a hash function, we want to use a compression function $f : \{0,1\}^{18} \to \{0,1\}^9$. The compression function consists of three Feistel-like rounds of the form

$$L_i||R_i \longmapsto L_{i+1}||R_{i+1} = R_i||(F(R_i) \oplus L_i),$$

and $f(L_0||R_0) = R_3$. The function $F : \{0,1\}^9 \to \{0,1\}^9$ is defined by

$$F(x_0, x_1, \ldots, x_8) = S_0(x_0, x_1, x_2)||S_1(x_3, x_4, x_5)||S_2(x_6, x_7, x_8),$$

where S_i are substitution boxes defined by the following table:

	000	001	010	011	100	101	110	111
S_0	001	010	011	100	101	110	111	000
S_1	111	000	001	010	011	100	101	110
S_2	011	001	000	100	010	111	100	010

b) Evaluate $f(000\,111\,000\,101\,010\,111)$.

c) Find a collision in f.