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
Tuesday, December 12, 2006
Time: 0900-1300
Permitted aids: approved calculator

Problem 1 In this task, we shall consider the RSA public key $(667, 417)$.

a) Given that $667 = 23 \cdot 29$, find the corresponding RSA private key.

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

Problem 2

a) Show that 7 has order 70 modulo 71.

b) Use Shank's Baby-step Giant-step method to compute the discrete logarithm of 57 to the base 7 modulo 71.

c) Use Pollard's ρ method to factor 253 using 2 as a starting value.

Problem 3 Let $p = 29$. Then $g = 2$ has order 28 modulo 29. Let 11 be a secret key for the ElGamal cryptosystem.

a) Explain how the ElGamal cryptosystem works and compute the public key corresponding to the secret key 11. Decrypt the ciphertext $(3, 15)$.

b) Using the knowledge that $(24, 25)$ decrypts to 7 under this private key, decrypt the ciphertext $(24, 3)$.

Problem 4

a) Explain what a stream cipher is. What happens if the initialization vector is ever reused?

We build a stream cipher around a linear feedback shift register with linear feedback relation $x_n = x_{n-15} \oplus x_{n-18}$. We initialize the register from a 9-bit key $k_0k_1 \dots k_8$ and 8-bit iv $iv_0iv_1 \dots iv_7$ as

x_0	x_1	x_2	x_3	$\dots$	x_{15}	x_{16}	x_{17}
k_0	iv_0	k_1	iv_1	$\dots$	iv_7	k_8	p

where p is chosen such that the number of 1-bits in the register is odd. The filter function is

$$f(x_{n-17}, x_{n-16}, \dots, x_{n-2}, x_{n-1}, x_n) =$$
$$(x_{n-14} \wedge x_{n-12} \wedge x_{n-10}) \oplus (x_{n-8} \wedge x_{n-6} \wedge x_{n-4}) \oplus (x_{n-14} \wedge x_{n-12}) \oplus (x_{n-6} \wedge x_{n-4}) \oplus x_{n-8} \oplus 1.$$

(Here, $\wedge$ and $\oplus$ denote the usual *and* and *exclusive or* logical operations, where 1 is true and 0 is false.)

b) Generate 8 bits of output starting with $iv = 0101\,0101$ and $k = 111\,000\,111$.

c) Decide if the ciphertext (encrypted with a randomly chosen key, *not the one from the previous task*)

$$1100\,0111\,0100$$

is an encryption of 0000 or 1111.