MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
July 13, 2007

Cryptography, Final Written Exam (Klausur)

Problem 1

a) Calculate the Jacobi symbol $\left(\frac{17}{107}\right)$.

b) Prove that 17 is a primitive root modulo 107.

Problem 2

Suppose $(N, e) = (143, 17)$ is the public key of a mini RSA system. Calculate the decryption exponent d.

Problem 3

To encrypt messages $x_1, x_2 \in \mathbb{Z}_2^{2n}$, Bob uses independent One-Time-Pads $p_1, p_2 \in \mathbb{Z}_2^{2n}$ and sends $y_1 := x_1 \oplus p_1$ to Alice and $y_2 := x_2 \oplus p_2$ to Ann. To encrypt another message

$$x_3 = (x_3', x_3'') \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n = \mathbb{Z}_2^{2n}$$

for Amy, he does not use a new independent One-Time-Pad, but uses $p_3 := p_1 \oplus p_2$ instead. He sends $y_3 := x_3 \oplus p_3$ to Amy.
Suppose that the first half x_3' of x_3 coincides with the first half of x_1 and the second half x_3'' of x_3 coincides with the second half of x_2.
Which parts of the messages x_1, x_2 can Eve reconstruct from y_1, y_2, y_3 ?

Problem 4

a) Prove that the polynomial $f(X) = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ is irreducible.

b) What is the period length of the LFSR sequence defined by

$$b_{k+5} := b_{k+2} + b_k \quad \text{for } k \geq 0$$

with initial vector $(b_0, \ldots, b_4) := (0, 0, 0, 0, 1) \in \mathbb{F}_2^5$? What about other initial vectors $v \in \mathbb{F}_2^5 \smallsetminus \{\vec{0}\}$?

Problem 5

The ElGamal Public-Key Cryptosystem in $(\mathbb{Z}/p)^*$ is defined as follows:

Let p be a prime such that the DL problem in $(\mathbb{Z}/p)^*$ is intractible. The public key of Alice is (p, g, h), where g is a primitive root modulo p and $h = g^\nu \bmod p$ with a secret exponent $\nu \in \mathbb{Z}/(p-1)$, only known to Alice.

If Bob wants to send a message $x \in (\mathbb{Z}/p)^*$ to Alice, he encrypts it in the following way: He chooses a secret random number $\alpha \in \mathbb{Z}/(p-1)$ and calculates

$$y_1 := g^\alpha \bmod p, \qquad y_2 := xh^\alpha \bmod p.$$

The ciphertext is then $y = (y_1, y_2)$.

How can Alice decrypt the ciphertext?