MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
June 27, 2007

Cryptography

Problem Sheet #11

Problem 41

a) Let $m \geq 3$ be an odd integer and $a \in \mathbb{Z}$. Show that by using the first and/or second supplement to the quadratic reciprocity law, the calculation of the Jacobi symbol $\left(\frac{a}{m}\right)$ can be reduced to the calculation of $\left(\frac{a'}{m}\right)$ with $0 \leq a' < m/3$.

b) Calculate the following Jacobi symbols:

$$\left(\frac{37}{97}\right), \qquad \left(\frac{93}{115}\right), \qquad \left(\frac{203}{329}\right).$$

Problem 42

Let $\mathbb{F}_q$ be the finite field with q elements and let $g, h \in \mathbb{F}_q^*$ be two primitive roots, i.e. generators of the multiplicative group $\mathbb{F}_q^*$.

a) Show that

$$\log_h(x) = \log_h(g) \log_g(x) \quad \text{for all } x \in \mathbb{F}_q^*$$

and $\log_h(g) = \log_g(h)^{-1}$, where the inverse is taken in $\mathbb{Z}/(q-1)$.

b) Suppose q odd. Show that $\log_g(-1) = \log_h(-1)$ and determine its value.

Problem 43

Let $\mathbb{F}_q$ be the finite field with q elements and $g \in \mathbb{F}_q^*$ a primitive root. Prove

a) If $3 \mid q-1$, then an element $x \in \mathbb{F}_q^*$ posseses a cube root in $\mathbb{F}_q$ if and only if $\log_g(x)$ is divisible by 3. A cube root of x is then $y := g^{\log_g(x)/3}$. Are there other solutions of the equation $y^3 = x$ in $\mathbb{F}_q$?

b) If $3 \nmid q-1$, then every $x \in \mathbb{F}_q$ posesses a uniquely determined cube root in $\mathbb{F}_q$. Devise an efficient algorithm to calculate the cube root in this case.

---

p.t.o.

Problem 44

Alice and Bob agreed on a secret key K by the Diffie-Hellman method using the (unrealistically small) prime $p = 55147$ and primitive root $g = 11 \in (\mathbb{Z}/p)^*$. The data sent from Alice to Bob resp. vice-versa were $a = g^\alpha = 15938$ and $b = g^\beta = 5831$. The key $K = g^{\alpha\beta}$ was used to generate a byte sequence $z_1, z_2, z_3, \ldots$ as a pseudo one-time-pad in the following way: With

$$Z_i := K^i \bmod p = \sum_{j=0}^{15} b_{ij} 2^j,\ b_{ij} \in \{0,1\}, \quad \text{set} \quad z_i := \sum_{j=4}^{11} b_{ij} 2^{j-4}.$$

This one-time-pad was XORed with an ASCII-plaintext. The resulting ciphertext was

```
0E0A 2246 776D 41F5 C05B E524 C166 78BF 1ECA 7804
```

Calculate K and decrypt the ciphertext.

Due: Friday, July 6, 2007, 14:10 h
Solutions should be returned in the Cryptography letter box in the first floor of the Institute in front of the library.

Final written exam (Klausur) on Friday, July 13, 2007, 14–16h:
All students wishing to take part in this exam must register until July 11, see

```
http://www.mathematik.uni-muenchen.de/~hoefer/regexam.html
```