MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
June 21, 2005

Cryptography

Problem Sheet #10

Problem 37 Fermat's factorizing method works as follows: To factorize an odd composite integer $N > 5$, set $x_0 := \lceil \sqrt{N}\, \rceil$. For $x := x_0 + k$, $(k = 0, 1, 2, 3, \ldots)$, calculate the differences $x^2 - N$ until a square number appears:

$$x^2 - N = y^2.$$

Then $N = (x + y)(x - y)$.

a) Prove that this method always succeeds after a finite number of steps.

b) Suppose $N = pq$, p, q primes with $|p - q| \le \alpha\sqrt[4]{N}$, where α is a positive real constant. Estimate the number of steps (as a function of α) necessary to factorize N by the Fermat factorization algorithm.

c) Factorize $N := 1157917699$ using the Fermat factorization algorithm.

Problem 38 Let g, g' be primitive roots modulo a prime p. Prove

(i) $\log_g(g')\log_{g'}(g) = 1 \bmod (p-1)$,

(ii) $\log_{g'}(x) = \log_g(x)\log_{g'}(g) \bmod (p-1)$ for all $x \in (\mathbb{Z}/p)^*$.

Problem 39 A *Sophie Germain prime* is a prime of the form $p = 2q + 1$, where q is itself a prime. Show that an integer g is a primitive root modulo a Sophie Germain prime p if and only if $g^2 \not\equiv 1 \bmod p$ and $\left(\frac{g}{p}\right) = -1$.

Problem 40 a) Prove that 3 is a primitive root modulo $p = 2^{16} + 1$.

b) Alice and Bob agreed on a secret key K by the Diffie-Hellman method using the (unrealistically small) prime $p = 2^{16} + 1$ and primitive root $g = 3 \in (\mathbb{Z}/p)^*$. The data sent from Alice to Bob resp. vice-versa were $a = g^\alpha = 13242$ and $b = g^\beta = 48586$. The key $K = g^{\alpha\beta}$ was used to generate a byte sequence $z_1, z_2, z_3, \ldots$ as a one-time-pad in the following way: With

$$Z_i := K^i \bmod p = \sum_{j=0}^{16} b_{ij}2^j,\ b_{ij} \in \{0, 1\}, \quad \text{set} \quad z_i := \sum_{j=4}^{11} b_{ij}2^{j-4}.$$

This one-time-pad was XORed with an ASCII-plaintext. The resulting cipher text is

`F02B 1756 5C98 54C5 3923 109E 62E6 C89E 9F6E B9DE`

Calculate the values of α, β, K and decrypt the ciphertext.

Due: Thursday, June 30, 2005, 14:10 h