MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
June 20, 2007

Cryptography
Problem Sheet #10

Problem 37

Fermat's factorizing method works as follows: To factorize an odd composite integer $N \geq 9$, 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 (albeit sometimes large) number of steps.

b) Suppose $N = uv$, with positive integers u, v, satisfying $|u - v| \leq \alpha \sqrt[4]{N}$, where α is a (small) real constant. Estimate the number of steps (as a function of α) necessary to factorize N by the Fermat factorization algorithm.

c) Factorize the integers 3589, 46883 and 2191059743 using the Fermat factorization algorithm.

Problem 38

To set up an RSA system with a modulus $2^{2m} < N < 2^{2m+1}$, (e.g. $m = 512$), it is recommended to choose the primes p, q in the range

$$2^m < p < 2^m + 2^{m-2}, \quad 2^m + 2^{m-1} < q < 2^{m+1}.$$

a) Why is Fermat's algorithm not suited to factorize $N = pq$.

b)* In the following example of an RSA modulus N the above recommendation was not followed.

```
N = 1 2688 EA75 B318 8777 FF81 F05A 7DA8 4D5F DE7D 7384 860D CC3F 9793
 8F32 7ECB E1F2 E00D ED43 CBD6 2C05 9CE3 BCE7 EC2B 3D4B 2CB5 CD94 9F57
 0F67 D5F7 3BBF 666D F86B
```

The encryption exponent was $e = 2^{16} + 1$. Decrypt the ciphertext

```
y = 1 22DB CC91 6227 B03D E005 8197 50C6 702B 31E4 F1EB 9A6B CF26 CEF8
 238E 8761 B8EE BCE1 A6A6 CFF6 5C41 D771 5572 12B6 1D60 619D A707 33BA
 BD8E 8882 5CF2 DBF4 2277
```

which was obtained from an ASCII plaintext, converted to an integer x as in problem 32b).

---

p.t.o.

Problem 39

a) Prove that an odd integer $N > 1$ is prime if and only if the following two conditions are satisfied:

(1) $a^{(N-1)/2} \equiv \pm 1 \bmod N$ for all integers a with $\gcd(a, N) = 1$.

(2) $a^{(N-1)/2} \equiv -1 \bmod N$ for at least one integer a.

b) Show that in a), condition (2) is essential, by giving an example of an odd composite integer $N > 1$ satisfying (1).

c) Use a) to construct a probabilistic primality test. In your test, what is the probability of errors of the following types:

i) Error of the 1^{st} kind: A composite number is declared prime.

ii) Error of the 2^{nd} kind: A prime number is declared composite.

Problem 40

Let p be a prime of the form $p = 2q + 1$, where q is itself a prime (then q is called a *Sophie Germain* prime).

a) Prove that g is a primitive root modulo p if and only if $g^2 \not\equiv 1 \bmod p$ and $\left(\frac{g}{p}\right) = -1$.

b) If additionally $q \equiv 1 \bmod 4$, then 2 is a primitive root modulo p.

Problems marked by an asterisk * are not obligatory, but solutions get extra points.

Due: Friday, June 29, 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.