MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
June 13, 2007

Cryptography

Problem Sheet #9

Problem 33

For a sequence of integers $a_0, a_1, a_2, \dots, a_k, \dots$, where $a_i > 0$ for $i \geq 1$, define u_i, v_i recursively by

$$u_{-1} = 1,\ u_0 = a_0, \qquad u_i = a_i u_{i-1} + u_{i-2},$$
$$v_{-1} = 0,\ v_0 = 1, \qquad v_i = a_i v_{i-1} + v_{i-2}, \quad (i \geq 1).$$

a) Prove that $\gcd(u_i, v_i) = 1$ for all $i \geq 0$.

b) Show that u_i/v_i is the i-th convergent of the continued fraction

$$x = \text{cfrac}(a_0, a_1, a_2, \dots, a_k, \dots).$$

c)* The following numbers N, e (hexadecimal notation) constitute the public key of an RSA system.

```
 N = 7D96 3333 37CC 33A2 EA4D 4D53 49B3 8011 BEB9 9F52 1CE8 0329 839F
A8F3 855B 1723 F6D0 4F29 AB86 9C30 1567 7060 60F4 6083 7601 4355 3A82
2C30 859C D1D8 72C8 6C6E 00F3 A26A DE5B EFC9 FDF3 75CB 14E9 BD0C A69D
8427 EB63 03EA 4FD4 39B8 D555 1F54 3C4A 2E46 9BE4 6F7A D3FB E077 BBBD
9544 0A72 E4A9 3538 DB29 D35A E9CF 726B 532D

 e = 3146 C2C8 004B 89E2 9112 55C9 DD76 A068 6CFA 636A 6006 8965 98AF
44EB B6F3 1541 49FC 8C2A 71B2 4EFF 671F 3CC0 F8E4 E535 6D15 9A9F AB9E
F614 3A4D 9DD2 604B 5F69 5D23 2FFE 6594 5C52 A263 EF42 F64D 8A55 02E9
C6CF D6A5 7AC0 2174 67A8 BFF6 87EC 751F B3B7 19DF B184 96C5 A8E3 BB8A
EE90 A772 2D68 049E AA35 65D5 6729 15CE 0409
```

It is known that the decryption exponent satisfies $d < 2^{250}$. Use Wiener's continued fraction attack to calculate d and the prime decomposition of N.

Problem 34

Let p, q be two coprime Carmichael numbers, $N := p \cdot q$ and $e \geq 3$ an integer with $\gcd(e, (p-1)(q-1)) = 1$. Define d by the relation

$$ed \equiv 1 \bmod (p-1)(q-1).$$

a) Prove that

$$x^{ed} \equiv x \bmod N \quad \text{for all } x \in (\mathbb{Z}/N)^*,$$

i.e. N, e, d can be used for an RSA system.

---

p.t.o.

b) Explain why it is nevertheless not advisable to use Carmichael numbers instead of primes for setting up an RSA cipher system.

Problem 35

Let k be a positive integer and p a prime with $p > 2k$. Prove that $N := 2kp + 1$ is prime if and only if there exists an integer a such that

$$a^{N-1} \equiv 1 \bmod N \quad \text{and} \quad \gcd(a^{2k} - 1, N) = 1.$$

Problem 36

Let $N \geq 9$ be an odd composite integer and let $p_1, \ldots, p_r$ be the distinct prime divisors of N. We define the following subgroups of $(\mathbb{Z}/N)^*$:

$$\begin{aligned} A_N &:= \{x \in (\mathbb{Z}/N)^* : x^{N-1} = 1\}, \\ B_N &:= \{x \in (\mathbb{Z}/N)^* : x^{(N-1)/2} = 1\}, \\ C_N &:= \{x \in (\mathbb{Z}/N)^* : x^{(N-1)/2} = \left(\frac{x}{N}\right)\}. \end{aligned}$$

a) Show that

$$\begin{aligned} |A_N| &= \prod_{i=1}^{r} \gcd(N-1, p_i - 1), \\ |B_N| &= \prod_{i=1}^{r} \gcd((N-1)/2, p_i - 1). \end{aligned}$$

b) Prove

$$[B_N : B_N \cap C_N] \leq 2, \qquad [C_N : B_N \cap C_N] \leq 2$$

and deduce

$$|C_N| = \gamma_N \cdot |B_N| \quad \text{with } \gamma_N \in \{\tfrac{1}{2}, 1, 2\}.$$

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

Due: Friday, June 22, 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.