MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
June 14, 2005

Cryptography

Problem Sheet #9

Problem 33 Let $N = pq$ be an RSA modulus ($p \neq q$ odd primes) and $e \geq 3$ an encryption exponent for N, i.e. $\gcd(e, \varphi(N)) = 1$. Let $\lambda(N) := \operatorname{lcm}(p-1, q-1)$ (lcm = least common multiple). Define d' by the congruence

$$ed' \equiv 1 \bmod \lambda(N).$$

Show that d' can be used as a decryption exponent, i.e. $x^{ed'} \equiv x$ for all $x \in \mathbb{Z}/N$.

Problem 34 Let $p \neq q$ be two odd Carmichael numbers, $N := pq$ and e, d two integers with

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

Show that

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

Does this congruence hold even for all $x \in \mathbb{Z}/N$?

Problem 35 Let $N = pq$ ($p \neq q$ odd primes) be an RSA modulus and e an encryption exponent. Prove that the encryption function

$$E : \mathbb{Z}/N \longrightarrow \mathbb{Z}/N, \quad x \mapsto E(x) = x^e \bmod N$$

has precisely

$$m := (1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1))$$

fixpoints, i.e. elements $x \in \mathbb{Z}/N$ with $E(x) = x$.

Problem 36 Consider the mini RSA system with modulus $N = 61937$ and encryption exponent $e = 7$.

a) Determine the the decryption exponent d defined by $ed \equiv 1 \bmod \varphi(N)$ and d' defined as in problem 33.

b) This RSA system has been used as a bigram ASCII substitution

$$\mathbb{Z}_{256}^2 \ni (a, b) \mapsto (\overline{a}, \overline{b}) \in \mathbb{Z}_{256}^2$$

defined by $x := a \cdot 256 + b$, $y := x^e \bmod N$, $y = \overline{a} \cdot 256 + \overline{b}$.
The following 10-byte cipher text was obtained in this way

```
8CD0 5457 692A 52E0 2A9D
```

Find the plaintext.

Due: Thursday, June 23, 2005, 14:10 h