MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
June 6, 2007

Cryptography
Problem Sheet #8

Problem 29

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. $x^{ed'} \equiv x \bmod N$ for all x.

Problem 30

Consider a mini RSA system with modulus $N = 59291$ and encryption exponent $e = 17$.

a) Determine the decryption exponent d defined by $ed \equiv 1 \bmod \varphi(N)$, and d' defined as in problem 29.

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

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

defined by

$$x := a \cdot 256 + b, \quad y := x^e \bmod N, \text{ with } y = \overline{a} \cdot 256 + \overline{b}.$$

The following 12-byte ciphertext was obtained in this way:

```
29CA 8D6E 79DB DF23 77AB 969B
```

Find the plaintext.

Problem 31

Let $N = pq$ ($p \neq q$ odd primes) be an RSA modulus and e an encryption exponent.

a) Prove that the encryption function $E : \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$, $x \mapsto E(x) = x^e \bmod N$, 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 $E(x) = x$.

b) Determine all fixpoints in the case $(N, e) = (8453, 17)$.

Problem 32

a) Suppose Alice and Ann set up RSA systems with the same modulus N but different public encryption exponents $e_1 = 5$, $e_2 = 17$. Bob sends the same message $x \in \mathbb{Z}_N$, encrypted as

$$y_1 := x^{e_1} \bmod N, \quad y_2 := x^{e_2} \bmod N$$

to Alice and Ann. Show how Eve can retrieve the message x from y_1 and y_2 without factorizing N.

b)* Find the plaintext in the following example (hexadecimal notation):

N = `FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 262E`
`C832 3112 D80A B28E AAFC 2BD0 15C0 934B E2F3`

y_1 = `12AA 25EF 5206 4482 3F53 45F9 B7B2 BB09 850A 297C`
`B9CE 879E DA8E 8658 7300 D25A 85BB 66F1 10B9`

y_2 = `03B4 C925 9E24 DB6C 09D8 1A53 F20B 2470 C845 D858`
`0915 5533 323A 0A77 709A ADF6 2FCA 84FE 7E8C`

Here the plaintext was an ASCII text $(a_1, a_2, \ldots, a_n)$, $a_i \in \mathbb{Z}_{256}$, represented by the integer

$$x = \sum_{i=1}^{n} a_i \cdot 256^{n-i}.$$

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

Due: Friday, June 15, 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.