

7. Oktober 2010

## 4. Übungsblatt Kryptologie

### Aufgabe 1: (3 Punkte)

- a) Finden Sie die Umkehrabbildung zu  $\varphi: \begin{cases} \mathbb{F}_p \rightarrow \mathbb{F}_p \\ x \mapsto x^e \end{cases}$  für die Primzahl  $p = 123456791$  und den Exponenten  $e = 3$ !
- b) Zeigen Sie, daß es für  $e = 2$  keine Umkehrabbildung gibt!
- c) Bestimmen Sie alle  $e \leq 10$ , für die  $\varphi$  keine Umkehrabbildung hat!

### Aufgabe 2: (5 Punkte)

- a) Zeigen Sie:  $N = 2^{2^n} - 1$  ist genau dann eine Primzahl, wenn  $n = 1$  ist.
- b) Zeigen Sie:  $2^n - 1$  ist genau dann durch drei teilbar, wenn  $n$  gerade ist.
- c) Die Zahl  $N = \frac{1}{3}(2^{122} - 1)$  ist Produkt zweier Primzahlen. Finden Sie diese **ohne** Computerhilfe!
- d) Finden Sie den kleinsten öffentlichen Exponenten  $e$ , den man in einem RSA-System mit Modul  $N$  benutzen kann!
- e) Bestimmen Sie den privaten Exponenten dazu! (*Spätestens hierzu sollten sie definitiv einen Computer benutzen!*)

### Aufgabe 3: (3 Punkte)

Als MARTIN GARDNER 1977 das RSA-Verfahren im *Scientific American* vorstellte, gaben ihm RIVEST, SHAMIR und ADELMAN die Beispielchiffre

$$c = 9686961375462206147714092225435588290575999112457431987469512093 \\ 0816298225145708356931476622883989628013391990551829945157815154 .$$

Sie war verschlüsselt mit dem öffentlichen Schlüssel bestehend aus dem Modul

$$N = 1143816257578888676692357799761466120102182967212423625625618429 \\ 35706935245733897830597123563958705058989075147599290026879543541$$

und dem Exponenten  $e = 9007$ . 1994 wurde der Faktor

$$p = 490529510847650949147849619903898133417764638493387843990820577$$

von  $N$  gefunden. Entschlüsseln Sie die Nachricht! (Der Text ist verschlüsselt nach dem Schema  $A = 01$ ,  $B = 02, \dots, Z = 26$ , Leerzeichen =  $00$ ; die Zahlen  $c, N$  und  $p$  sind auch auf der home page der Vorlesung zu finden.)

### Aufgabe 4: (3 Punkte)

Untersuchen Sie den *Lawineneffekt* bei RSA-Nachrichten, indem Sie bei der Nachricht  $m = 123456787654321$  zum RSA-Modul  $N = 123456978897139$  und Exponent  $e = 1025$  jeweils eine der 15 Ziffern der Nachricht um eins erhöhen und zählen, wie viele Ziffern der Verschlüsselung dadurch verändert werden!

**Aufgabe 5:** (2 Punkte)

Leider haben Sie nur eine alte RSA-Implementierung, die nicht mit den heute wünschenswerten Modullängen zurechtkommt. Um trotzdem ein sicheres System zu bekommen, entwickeln Sie in Anlehnung an Triple-DES das folgende Triple-RSA-System: Sie wählen sich einen Modul  $N$  und zwei öffentliche Exponenten  $e_1, e_2$ ; ein Block  $b$  wird dann verschlüsselt als

$$\text{RSA}_{N,e_1} \left( \text{RSA}_{N,e_2} \left( \text{RSA}_{N,e_1}(b) \right) \right).$$

- a) Warum wird in der Mitte nicht, analog zu Triple-DES,  $\text{RSA}_{N,e_2}^{-1}$  verwendet?
- b) Ist die Sicherheit von Triple-RSA vergleichbar mit der von einfachem RSA mit doppelter Blocklänge?

**Aufgabe 6:** (4 Punkte)

Eine kurze Nachricht  $m$  wurde mit Modul

$$N = 85397342226735670654635508790584112503020721253533098926191$$

und Exponent  $e = 257$  verschlüsselt als

$$c = 70164475041013773588271207010038601194416445764382942513640.$$

Rekonstruieren Sie die Nachricht unter der Annahme, daß sie das Produkt zweier höchstens vierstelliger Zahlen ist!