Wolfgang K. Seiler
Tel. 2515

A5, C201

2. Oktober 2007

4. Übungsblatt Kryptologie

Aufgabe 1: (*5 Punkte*)
Als Martin Gardner 1977 das RSA-Verfahren im *Scientific American* vorstellte, gaben ihm Rivest, Shamir und Adelman die Beispielchiffre

$$c = 968696137546220614771409222543558829057599911245743198746951209308162982251457083569314766228839896280133919905518299451578151 54\,.$$

Sie war verschlüsselt mit dem öffentlichen Schlüssel bestehend aus dem Modul

$$N = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$$

und dem Exponenten $e = 9007.1994$ wurde der Faktor

$$p = 4905295108476509491478496199038981334177646384933878439908205 77$$

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

Aufgabe 2: (*5 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 3: (*4 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

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

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

Aufgabe 4: (*6 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!

Abgabe bis zum Dienstag, dem 9. Oktober 2007, um 12.00 Uhr