WOLFGANG K. SEILER
Tel. 2515

A5, C201

12. Januar 2005

10. Übungsblatt Kryptologie

Aufgabe 1: (*4 Punkte*)
Im Maple *worksheet* blatt10.mws auf der *home page* der Vorlesung sind fünf 2048-Bit RSA-Moduln $N_1, \ldots, N_5$ mit den zugehörigen privaten Exponenten e_i zu finden. Bestimmen Sie möglichst viele der privaten Exponenten d_i ausgehend von der Hypothese, daß bei der Konstruktion der N_i Primzahlen mehrfach verwendet wurden!

Aufgabe 2: (*7 Punkte*)
Ihr RSA-Modul ist die, wie alle folgenden Zahlen, in blatt10.mws zu findende Zahl M; Ihr privater Exponent ist d und Ihr öffentlicher Exponent ist e. Einer Ihrer Kollegen hat den öffentlichen Exponenten e_0. Was sind sein privater Exponent?

Aufgabe 3: (*4 Punkte*)

a) Verschlüsseln Sie gemäß PKCS1-Standard den Text „Leider reduziert bei RSA fast jeder Trick, der Rechenzeit spart, gleichzeitig die Sicherheit des Verfahrens. Dies kann gelegentlich fatale Konsequenzen haben.“ mittels des öffentlichen Schlüssels (M, e_0) aus Aufgabe 2!

b) Unterschreiben Sie die Nachricht als Inhaber des (öffentlichen) Schlüssels (M, e) !

Aufgabe 4: (*5 Punkte*)

a) Berechnen Sie, ohne Computer oder Taschenrechner, die Zahlen

$$2^{64} \bmod (2^{16}+1) \quad \text{und} \quad 2^{64} \bmod (2^{16}+3)\,!$$

b) Berechnen Sie, ausgehend von *a),* den Wert von $2^{64} \bmod (2^{16}+1)(2^{16}+3)$! (Für das Endergebnis werden Sie wohl einen Taschenrechner oder Computer brauchen.)

Abgabe bis zum Dienstag, dem 18. Januar 2005, um 12.00 Uhr