WOLFGANG K. SEILER
Tel. 2515

A5, C201

19. Januar 2005

11. Übungsblatt Kryptologie

Aufgabe 1: (*9 Punkte*)

a) Ermitteln Sie die bestmögliche Approximation der EULERschen Zahl e durch einen Bruch mit einstelligem Nenner!

b) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{3}$ und zeigen Sie, daß diese periodisch wird!

c) Welche reelle Zahl x hat die folgende Kettenbruchentwicklung:

$$6+\cfrac{1}{6+\cfrac{1}{6+\cfrac{1}{6+\cfrac{1}{6+\cfrac{1}{6+\cfrac{1}{6+\cdots}}}}}}$$

Aufgabe 2: (*6 Punkte*)

Im Maple *worksheet* `blatt11.mws` finden Sie einen RSA-Modul N und öffentlichem Exponenten e. Sie vermuten, daß der private Exponent d dazu relativ klein ist.

a) Bestimmen Sie den privaten Exponenten d!

b) Faktorisieren Sie N!

Aufgabe 3: (*5 Punkte*)

a) Bestimmen Sie für jede natürliche Zahl $a \leq 16$ Kern und Bild der Abbildung

$$\varphi_a\colon \{0,1,\ldots,15\} \to \{1,\ldots,16\}\,; \quad x \mapsto a^x \bmod 17\,!$$

b) Bestimmen Sie für alle a die Menge $\mathcal{L}_a = \{x \mid \varphi_a(x) = 9\}$!

Abgabe bis zum Dienstag, dem 25. Januar 2005, um 12.00 Uhr