Kryptographie II – Übungsblatt 2

Aufgabe 1: Kettenbruchentwicklung rationaler und irrationaler Zahlen

(8 Punkte)

A. Berechne die Kettenbruchentwicklungen $x = \langle q_0, q_1, q_2, \dots \rangle$ der folgenden Zahlen

(i) $2007/1971$.

(ii) $\sqrt{7} + 2$.

B. Finde die Zahl, deren Kettenbruchentwicklung ist:

(i) $\langle 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \rangle$ (benutze dabei die Rekursionsrelationen);

(ii) $\langle 1, 2, 3, 1, 2, 3, 1, 2, 3, 1, \dots \rangle$.

Aufgabe 2: RSA mit kleinem privatem Exponent

(3+6 Punkte)

1. Seien $n = pq = 11413$ ein RSA-Modulus und $e = 5091$ ein öffentlicher Exponent.

Finde die Faktorisierung von n und den privaten Exponenten d mittels der Methode der Kettenbruchentwicklung.

2. Und jetzt noch mal mit etwas anderen Zahlen.

```
n = 5ffa391905f026a9e64e
   = ec553e37209938977ac1
   = 1d1ef969d3848a9e2f77
   = dd33fc12fb698b872ba1
   = bd3bf5ac6e02a1fd24e6
   = c26f95790f7a21e3f51a
   = 806919cd7254a7bb1ec3
   = a23d7c0f7e773ffce083
   = f09daaf34ef84b25df14
   = c8114ce4b4fbf7b20646
   = ea23aef46b51e62f395c
   = 966f20c906a1dea3a909
   = e9d4093503ebd833
```

e = 2025b7ef3c7484a7ed9d
= a144c3b92159fad4a7bd
= 4159fd16b83256d92814
= fb09ee8f13606ed4982a
= fa69e518511e9b0f0fc3
= d9220dca82a416a4ec98
= 91adf48b242a2e3e2dd5
= fc0f685aff1817c29a47
= ee83977a3253af1a0d6d
= cc3ae1806d0dc8f9c247
= e19bd5b8305ebad0c043
= b356c7d81d9e9f927e2f
= 833ccf862b521063

Nicht nur das Ergebnis, sondern auch Zwischenergebnisse und den Quellcode des Programms abgeben.

Abgabe: Freitag, 25.04.2008 bis 12:00 Uhr. Entweder im Kasten im Gebäude NA Ebene 02, oder per Mail an mansour.alsawadi@rub.de.