Wolfgang K. Seiler
Tel. 2515

A5, C201

15. Dezember 2004

8. Übungsblatt Kryptologie

Aufgabe 1: (*4 Punkte*)

a) Wenden Sie auf die Zahl 15 sowohl den Fermat-Test an als auch dessen Modifikation nach Artjuhov, beides jeweils für die Basis vier!

b) Zählen Sie, für wie viele Basen a zwischen eins und 1728 die Zahl $p = 1729$ denn Fermat-Test besteht!

c) Für wie viele besteht sie auch die Modifikation?

Aufgabe 2: (*4 Punkte*)

a) Zeigen Sie: Ist $n = pq$ Produkt zweier ungerader Primzahlen, so gibt es genau vier Zahlen a zwischen 0 und $n - 1$ mit $a^2 = 1$!

b) Was gilt, wenn $n = 2p$ das Doppelte einer ungeraden Primzahl ist?

Aufgabe 3: (*4 Punkte*)

Die Zahl $p = (6t + 1)(12t + 1)(18t + 1)$ sei eine Carmichael-Zahl.

a) Zeigen Sie: Es gibt $1296t^3$ Zahlen a zwischen 1 und $p - 1$, für die p den Fermat-Test besteht.

b) Wie verhält sich die Wahrscheinlichkeit dafür, daß p für eine zufällige Basis a den Fermat-Test besteht, wenn t gegen unendlich geht?

Aufgabe 4: (*4 Punkte*)

Finden Sie via Eratosthenes und (modifiziertem) Fermat-Test die kleinste zehnstellige Zahl, die nicht als zusammengesetzt erkannt werden kann!

Aufgabe 5: (*4 Punkte*)

Faktorisieren Sie mit dem Fermatschen Verfahren die Zahl 1545013 !

Abgabe bis zum Dienstag, dem 21. Dezember 2004, um 12.00 Uhr