Übung zur Vorlesung

Kryptographie und Komplexität

Prof. Dr. Christoph Kreitz
Universität Potsdam, Theoretische Informatik, WS 2014/15

Blatt 2 — Besprechungstermin: 11.12.2014

Für viele dieser Aufgaben benötigen Sie zumindest einen Taschenrechner.

Aufgabe 2.1 (Primzahlen und Faktorisierung)

1. Beweisen Sie mit dem Fermat-Test, daß 11111 keine Primzahl ist.
2. Verwenden Sie den Fermat Test um zu zeigen, daß $2^{(2^5)}+1$ zusammengesetzt ist.

   Verwenden Sie den Solovay-Strassen Test um zu zeigen, daß $2^{(2^5)}+1$ zusammengesetzt ist.

   Verwenden Sie den Miller-Rabin Test um zu zeigen, daß $2^{(2^5)}+1$ zusammengesetzt ist.

   Vergleichen Sie die Effizienz der drei Verfahren
3. Faktorisieren Sie $n = 13199$ mit der Fermat-Faktorisierungsmethode.
4. Faktorisieren Sie $n = 831802500$ vollständig mit Probedivision.
5. Faktorisieren Sie $n = 138277151$ mit der Pollard $p-1$ Methode.
6. Finden Sie mit quadratischen Sieben einen echten Teiler von $n = 11111$.

Aufgabe 2.2 (RSA- und Rabin Verschlüsselung)

1. Bestimmen Sie alle für das RSA-Modul n=437 möglichen Verschlüsselungsexponenten e.

   Versuchen Sie, eine allgemeine Formel für die Anzahl der möglichen Verschlüsselungsexponenten für ein gegebenes RSA-Modul n anzugeben
2. Wieviele Operationen erfordert die RSA Verschlüsselung mit den Verschlüsselungsexponenten $e_1 = 2047$, $e_2 = 65535$, $e_3 = 65537$ und $e_4 = 1073741825$.
3. Erzeugen Sie zwei 8-Bit Primzahlen p und q so, daß $n = p{\cdot}q$ eine 16-Bit Zahl ist und der öffentliche Schlüssel $e = 5$ verwendet werden kann. Berechnen Sie den privaten Schlüssel d zu e=5 und verschlüsseln Sie den 16bit-Block `0011010011011011` mit e.
4. Beschreiben Sie, wie eine Common-Modulus-Attacke durchgeführt werden kann:
   Gegeben seien die öffentlichen Schlüssel (n, e) und (n, e') mit $gcd(e, e') = 1$ sowie die Schlüsseltexte $y = x^e \bmod n$ und $y' = x^{e'} \bmod n$. Wie kann daraus der Klartext x berechnet werden?

   Verwenden Sie die Common-Modulus-Attacke um die Schlüsseltexte $y = 293$ bzw. $y' = 421$ bei bekannten öffentlichen Schlüssel $(n, e) = (493, 3)$ und $(n, e') = (493, 5)$ zu dechiffrieren
5. Sei $n = 713$ ein öffentlicher Rabin-Schlüssel und $y = 289$ ein Schlüsseltext, der durch Rabin-Verschlüsselung entstanden ist. Bestimmen Sie alle möglichen Klartexte, die zu diesem Schlüsseltext führen.