SMS1 für MC, FHS Hagenberg
11. Übungsblatt für den 12. Jänner 2006

1. Ist $H(x) := x^3 \mod 3494122503799$ eine Einwegfunktion? Eine Hashfunktion?
   Geben Sie eine Kollision für H an. Ist H stark oder schwach kollisionsresistent?

2. Recherche: Wie funktioniert die MD4 Hash-Funktion? Erklären Sie die wesentlichen Elemente im Algorithmus (siehe [1, 9.4.2 (i)]). Insbesonders:

   (a) Welches Format haben Input und Output?
   (b) Wie wird der Input vorformatiert?
   (c) Wieviele Bits des vorformatierten Inputs werden in jeder Iteration zu den neuen "chaining values"verarbeitet?
   (d) Was ist der Zusammenhang zwischen den "chaining values von einer Iteration zur nächsten?

3. Das Authentifizierungsprotokoll von Fiat-Shamir mit Modul $n = 99899$ und $t = 2$: Sie wählen das Geheimnis $s = 1841$ und geben den öffentlichen Schlüssel v bekannt.

   Um sich bei Bob zu identifizieren, wählen Sie $r_1 = 25497$ und schicken den zugehörigen Zeugen an Bob. Der antwortet mit der Herausforderung (challenge) $e = 1$. Was antworten Sie?

   In der zweiten Runde wählen Sie $r_2 = 19054$ und erhalten die Herausforderung $e = 0$. Was sollen Sie antworten?

4. Es seien n, t wie in der vorigen Aufgabe. Alice hat den öffentlichen Schlüssel $v = 8488$ und möchte sich bei Ihnen identifizieren. In der ersten Runde schickt sie den Zeugen $x_1 = 65118$ und antwortet auf die Herausforderung $e = 1$ mit $y_1 = 38617$. In der zweiten Runde schickt sie den Zeugen $x_2 = 41568$ und antwortet auf die Herausforderung $e = 0$ mit $y_2 = 82961$. Was schließen Sie?

5. Wie können Sie beim Fiat-Shamir Protokoll vortäuschen, das Geheimnis s zu kennen, wenn Sie wissen, dass Bob immer die Herausforderung $e = 0$ stellt? Wie, wenn Bob immer $e = 1$ fordert?

Literatur

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.