Übungen zur Vorlesung Kryptographie

Blatt 11

Aufgabe 41: (SHA-256 Kollisionen)
Finden Sie ein Onlinewerkzeug zum Erzeugen von SHA-256-Hashwerten (Eingabe Text, Ausgabe Hexadezimalzahl). Nutzen Sie das, um eine Kollision in der letzten Ziffer zu finden. Also: Finden Sie Eingaben m, m', so dass die letzten Hexadezimalziffern von $h(m)$ und $h(m')$ gleich sind, wobei h für SHA-256 steht.

Rechnen Sie Aufgaben 42-44 von Hand, nicht mit dem Rechner. Sie dürfen natürlich Ihre Ergebnisse mit dem Rechner überprüfen (sagemath, wolframalpha...)

Aufgabe 42: (Polynome über $\mathbb{F}_2$ - Level 1 bis 3)
Wir betrachten Polynome in $\mathbb{F}_2[x]$, also Polynome von der Form $a_n x^n + \cdots + a_1 x + a_0$ mit $a_i \in \mathbb{F}_2$ für $0 \leq i \leq n$.

(a) Berechnen Sie in $\mathbb{F}_2[x]$ die Ergebnisse von $(x^8+x^7+x^5+x^4+x^2+1)+(x^8+x^6+x^4+x^3+x^2+x+1)$ und $(x^4 + x^2 + 1) \cdot (x^3 + x + 1)$.
(b) Sei $p = x^5 + x^4 + x + 1$. Berechnen Sie $p \bmod x^4 + x^2$, $p \bmod x^4 + x$, und $p \bmod x^4 + 1$ in $\mathbb{F}_2[x]$.
(c) Berechnen Sie den ggT von $x^3 + 1$ und $x^4 + x^2 + x + 1$ in $\mathbb{F}_2[x]$.

(Tipp: Benutzen Sie bei (c) und bei A 43 den euklidischen Algorithmus, angepasst an Polynome über $\mathbb{F}_2$, vgl. Beispiel 8.1 im Skript S. 45.)

Aufgabe 43: (Polynome über $\mathbb{F}_2$ - Level 4 bis 5)
(a) Finden Sie Polynome p', q', so dass $p' \cdot (x^3 + 1) + q' \cdot (x^4 + x^2 + x + 1) = x + 1$ in $\mathbb{F}_2[x]$.
(b) Finden Sie ein Polynom q in $\mathbb{F}_2[x]$, so dass $q \cdot (x^3 + x^2 + x + 1) \equiv 1 \bmod x^4 + x + 1$.

Aufgabe 44: (Aufwärmübung Lineare Algebra über $\mathbb{F}_2$)
Gegeben sind die Matrizen $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in (\mathbb{F}_2)^{2\times 2}$ und $B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in (\mathbb{F}_2)^{3\times 3}$. Wir rechnen alles in $\mathbb{F}_2$ (also modulo 2).

(a) Berechnen Sie die inverse Matrix zu A.
(b) Finden Sie eine Matrix $X \in (\mathbb{F}_2)^{2\times 2}$, so dass $A \cdot X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
(c) Berechnen Sie die inverse Matrix zu B.

(Wie man über $\mathbb{R}$ eine inverse Matrix berechnet steht z.B. hier:

`https://www.math.uni-bielefeld.de/~frettloe/teach/alte-vorles/ueb/auff-skript-1-20.pdf`

auf Seite 47. Das geht in $\mathbb{F}_2$ genauso, nur das Rechnen wird einfacher.)

Abgabe bis Dienstag 20.6.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de