Dr. Dirk Frettlöh 27.6.2022

Übungen zur Vorlesung Kryptographie

Blatt 11

Aufgabe 41: (Buchstaben zu Punkten zu Buchstaben)
Wir benutzen die Koblitz-Kodierung aus der Vorlesung für die elliptische Kurve E mit der Gleichung $y^2 = x^3+5x+3$ über $\mathbb{F}_{17}$. Dabei ist wie üblich a=0, b=1, ... z=25. Also können wir jeden Buchstaben mit 6 Bit darstellen. Wir wählen hier also $d = 4$ und zerschneiden eine zu verschlüsselnde Botschaft (in Binärcodierung) in 2-Bit-Worte. Z.B. wäre p=15=$(00\ 11\ 11)_b$, also p wird zu 0,3,3. Auf 0, 3 und 3 wird nun einzeln die Koblitzkodierung angewandt.

(a) Was ist die Koblitz-Kodierung des Buchstaben "s"?
(b) Welches Wort ergibt das Ent-Kodieren der nach obigem Schema Koblitz-kodierten Nachricht

$$(1,3),(13,2),(4,6),\ (5,0),(2,2),(10,13),\ (2,-2),(1,14),(2,-2)?$$

Aufgabe 42: (Einfache Hashfunktion)
Wir codieren Buchstaben als $a = 00, b = 01, c = 02 \ldots, z = 25$. Wir benutzen eine Merkle-Damgård-Konstruktion mit Startwert $s = x_0 = 73$. Die m_i sind die einzelnen Buchstaben $m_1, m_2, \ldots, m_n$ des zu hashenden Texts, gefolgt von der Länge $m_{n+1} := n$ der Nachricht; also $m = (m_1, m_2, \ldots, m_n, m_{n+1} = n)$, als zweistellige Zahlen gelesen. Die Kompressionsfunktion $x_i = f(x_{i-1}, m_i)$ $(i = 1, \ldots, n+1)$ funktioniert folgendermaßen:

(1) $y = 19 \cdot (m_i + x_{i-1}) \bmod 100$
(2) Vertausche die Ziffern von y, nenne diese neue Zahl z (Obacht: aus $y = 7 = 07$ wird 70)
(3) $x_i = x_{i-1} + z \bmod 100$

Was ist der Hashwert $h(m)$ des Wortes $m =$"passwort"? Finden Sie ein (sinnfreies) Wort mit demselben Hashwert $h(m)$. Was ist der Hashwert von $m' =$"a"? Was ist der Hashwert von $m'' =$"password"? Was ist der Hashwert des leeren Strings ""?

Aufgabe 43: (Bessere Hashfunktion?)
Betrachten wir die Kompressionsfunktion $f : Z_{61} \times Z_{61} \to Z_{61},\ f(x,y) = 11^x \cdot 50^y \bmod 61$ und $g : Z_{67} \times Z_{67} \to Z_{67},\ g(x,y) = 7^x \cdot 12^y \mod 67$.

(a) Realisieren Sie die zugehörigen Hashfunktionen h zu f und h' zu g nach der Merkle-Damgård-Konstruktion (wie in Aufgabe 42, mit Startwert $s = x_0 = 43$ und mit Padding — also $m_{n+1} = n$ = Länge des Texts) und berechnen Sie jeweils die Hashwerte der Worte "alice", "bob", "carol" und "eve".
(b) Bestimmen sie die Wertebereiche von h und h' — also die Menge aller Werte, die h und h' jeweils annehmen können.
(c) Welche der beiden Funktionen ist die eindeutig ungeeignetere Hashfunktion? Erklären Sie, woran das liegt!

Aufgabe 44: (Wozu Padding?)
Eine naheliegende Variante der Merkle-Damgård-Konstruktion benutzt weder Startwert noch Padding. Ihre Aufgabe ist herauszufinden, warum das keine gute Idee ist. Sei der zu hashende Text $(m_0, m_1, \ldots, m_n)$. Betrachten Sie folgende Hashfunktion mit der Kompressionsfunktion g aus Aufgabe 43.

Setze $x_0 = m_0$. Für $i = 1, 2, \ldots, n$: Berechne $x_i = g(x_{i-1}, m_i)$. Ausgabe $h(m) = x_n$.

(a) Finden Sie zur Nachricht $m = (0, 11, 8, 2, 4)$ drei Kollisionen. Genauer: finden sie zu m drei weitere Urbilder m', m'', m''' der jeweiligen Länge 4, 3 und 2 mit $h(m) = h(m') = h(m'') = h(m''')$.

(b) Erläutern Sie allgemein, wie man hier zu einer Nachricht m der Länge $n+1$ leicht eine Nachricht m' der Länge n findet mit $h(m) = h(m')$. Erläutern Sie auch, wie Padding dies verhindert, und wie das Nutzen eines Startwerts das verhindert.

(Teil (a) kann brute-force erledigt werden. Wer aber Teil (b) kann, kann Teil (a) ohne viel Aufwand erledigen.)

Abgabe bis Montag 4.7.2022 bis 14 Uhr per Email an Ihren Tutor.
Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen: *techfakaccount*-bl$n$.pdf, also z.B. `dfrettloeh-bl11.pdf`, oder `dfrettloeh+mnebel-bl11.pdf`.

Jan-Philipp Brünger	jbruenger@techfak.de
Simon Hahm	shahm+krypto@techfak.de
Tim Lakämper	tlakaemper+krypto@techfak.de