Dr. Dirk Frettlöh 26.6.2024

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.

Beschreiben Sie, wie Sie vorgingen (falls Sie einfach wild rumprobiert haben, dann schreiben Sie eben das.)

Aufgabe 42: (ElGamal auf elliptischen Kurven)
Bob möchte eine Nachricht an Alice schicken und dabei ElGamal-Verschlüsselung über der elliptischen Kurve E mit der Gleichung $y^2 = x^3 + 3x + 2$ über $\mathbb{F}_{11}$ nutzen. Der öffentliche Erzeuger von E sei $g = (3, 7)$. Alice geheimer Schlüssel ist $a = 3$.

(a) Was ist das g^a in Alice öffentlichem Schlüssel (E, g, g^a)?
(b) Bob wählt zufällig $r = 6$. Was ist der Einmalschlüssel $k = (g^a)^r$ für diese Verschlüsselung?
(c) Bob verschlüsselt die Nachricht $m = 10$. Dazu wählt er das Element $(10, 3) \in E$ und verschlüsselt es als $c = m \odot k$. Was ist c? Was genau schickt Bob an Alice?
(d) Was berechnet Alice alles, um die Nachricht zu entschlüsseln?

(Es ist vermutlich auch hier hilfreich, den Cayleygraphen zu haben und zu nutzen. Dazu und für andere Aufgaben auf diesem Blatt ist die Software von meiner Webseite sicher wieder hilfreich.)

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 40, 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!

Fortsetzung auf der zweiten Seite

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 Dienstag 2.7.2024 bis 23:59 Uhr per Email an den Tutor.

Jakob Niermann	Mi 16 Uhr in T2-233	janiermann+krypto@techfak.de
Enrico di Gaspero	~~Do 16 Uhr in U2-216~~	edigaspero+krypto@techfak.de
Lisa Henetmayr	Fr 10 Uhr in X-E0-205	lhenetmayr+krypto@techfak.de
Richard Freidhof	Fr 12 Uhr in T2-141	rfreidhof+krypto@techfak.de