Übungen zur Vorlesung Kryptographie

Blatt 9

Aufgabe 33: (Primitivwurzeln für Diffie-Hellman finden)
Wir betrachten einen Diffie-Hellman-Schlüsseltausch mit $G = Z_p^*$ mit p Primzahl. Im Allgemeinen ist es knifflig, eine echte Primitivwurzel mod p zu finden. Folgende Idee hilft: Finde eine Primzahl q einer gewünschten Länge n (sagen wir, 1024 bit), so dass auch $p = 2q + 1$ Primzahl ist. (Das geht in $O(n^2)$ statt in $O(n)$ Versuchen.)

(a) Bestimmen Sie alle Werte $i \in \{1, \ldots, p-1\}$, so dass es ein $a \in Z_p^*$ gibt mit $a^i \equiv 1 \bmod p$, und $a^j \not\equiv 1 \bmod p$ für alle $j \in \mathbb{N}$ mit $1 \leq j < i$.

(b) Bestimmen Sie für die beiden kleinsten dieser Werte i alle $a \in Z_p^*$ mit $a^i \equiv 1 \bmod p$.

(c) Wie kann Alice nun schnell eine Primitivwurzel mod$p$ finden? (Übrigens: Alternativ ist es auch sicher, alle Werte außer die aus (b) als Ersatz für die eigentlichen Primitivwurzeln bei Diffie-Hellman zu verwenden.)

Aufgabe 34: (ElGamal mod p)
(a) Der öffentliche Schlüssel von Alice ist $(p, g, g^a \bmod p) = (601, 7, 598)$. Verschlüsseln Sie die Nachricht $m = 2$ an Alice. Benutzen Sie dabei $r = 3$ als Zufallszahl.

(b) Der öffentliche Schlüssel von Alice sei wie in (a), der private Schlüssel sei $a = 4$. Entschlüsseln Sie die Nachricht $(g^r \bmod p, c) = (5, 3)$.

(c) Angenommen, Bob wählt zweimal denselben Exponenten r und berechnet damit aus den Klartexten $m = 23$ und m' jeweils die Schlüsseltexte $(574, 466)$ und $(574, 459)$, wobei $(601, 7, 21)$ der öffentliche Schlüssel von Alice ist. Berechnen Sie den Klartext m'.

Aufgabe 35: (Polynome über $\mathbb{F}_p$)
(a) Bestimmen Sie alle Nullstellen der Polynome $p(x) = x^3 + x$ und $q(x) = x^3 + x^2 + x$ jeweils einmal in $\mathbb{F}_5$ und einmal in $\mathbb{F}_7$.

(b) Bestimmen Sie $a_1, a_2, a_3 \in \mathbb{F}_5$, so dass in $\mathbb{F}_5$ gilt: $p(x) = (x - a_1) \cdot (x - a_2) \cdot (x - a_3) \bmod 5$.

(c) Finden Sie ein Polynom der Form $x^3 + ax^2 + bx + c$, das genau zwei Nullstellen in $\mathbb{F}_5$ hat; sowie ein Polynom der Form $x^4 + ax^3 + bx^2 + cx + d$, das genau vier Nullstellen in $\mathbb{F}_7$ hat.

Aufgabe 36: (Wann ist's keine Gruppe?)
(a) Es wäre nahliegend, die Gruppenoperation auf einer elliptischen Kurve E über $\mathbb{R}$ einfach zu definieren als $p \odot q = r$, wobei r der dritte Schnittpunkt der Gerade durch p und q mit E ist (bzw der zweite Schnittpunkt von E mit der Tangente in p an E, falls $p = q$). Erklären Sie, warum das im Allgemeinen keine Gruppe liefert.
(Als Lösung reicht hier ein aussagekräftiges Bild)

(b) Für welche Werte von b liefert $y^2 = x^3 - x + b$ keine elliptische Kurve über $\mathbb{R}$? Für welche Werte von b liefert $y^2 = x^3 + b$ keine elliptische Kurve über $\mathbb{R}$? Zeichnen Sie all diese Kurven (gerne mit einer geeigneten Software). Erläutern Sie, warum die jeweils keine Gruppe liefern.

Abgabe: Mittwoch 12.6.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Dienstag	Philipp Braukmann	pbraukmann@techfak.uni-bielefeld.de
Donnerstag	Oliver Tautz	otautz@techfak.uni-bielefeld.de