Dr. Dirk Frettlöh 16.6.2021

Übungen zur Vorlesung Kryptographie

Blatt 10

Aufgabe 37: (Buchstaben zu Punkten zu Buchstaben)
Wir benutzen die Koblitz-Kodierung aus der Vorlesung für die elliptische Kurve E mit der Gleichung $y^2 = x^3 + x + 3$ 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.

(a) Berechnen Sie die Koblitz-Kodierung des Buchstaben "j". Zeigen Sie Ihre Berechnung.

(b) Welches Wort ergibt das Ent-Kodieren der nach obigem Schema Koblitz-kodierten Nachricht

$(6,2),(2,8),(12,3)\quad (6,15),(6,2),(2,9)\quad (6,15),(2,8),(6,2)\quad (2,9),(8,8),(2,8)\quad (2,9),(12,14),(6,2)\quad (2,8),(6,15),(8,8)$?

Aufgabe 38: (Elliptische Kurven mit Primzahlordnung)
Es ist sehr praktisch, wenn die Ordnung einer elliptischen Kurve eine Primzahl p ist (warum nochmal?). Für große p ist es aber nicht einfach, so eine zu finden. Diese Aufgabe soll das ein wenig illustrieren.

(a) Zählen Sie alle elliptischen Kurven über $\mathbb{F}_7$ (also alle Paare (a, b), so dass die Gleichung $y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbb{F}_7$ definiert). Zählen Sie diejenigen darunter, so dass die Anzahl der Elemente eine Primzahl ist. Bestimmen Sie den Anteil dieser elliptischen Kurven mit Primzahlordnung an all diesen elliptischen Kurven.

(b) Tun Sie dasselbe für $\mathbb{F}_{647}$.

(Für noch größere p wird der Anteil immer kleiner, aber das konkret zu berechnen wird sehr langwierig.)

Aufgabe 39: (Ordnung von E ist ungefähr p)
Sei E eine elliptische Kurve über $\mathbb{F}_p$ (wie in Def. 6.1).

(a) Zeigen Sie, dass E spiegelsymmetrisch bezüglich der x-Achse ist. (Also: ist $(x, y) \in E$, dann auch $(x, -y) \in E$. Das $\mathcal{O}$ kann hier ignoriert werden.)

(b) Zeigen Sie: für die Ordnung $|E|$ von E gilt: $|E| \leq 2p + 1$.

Weiter auf Seite 2

Aufgabe 40: (Chosen-Ciphertext-Angriff auf ElGamal-Verschlüsselung)
Falls Bob Alice überreden kann, ihm eine von ihm als $(g^{r'}, c')$ mit Alices öffentlichem Schlüssel g^a verschlüsselte Nachricht m' zu entschlüsseln, kann er eine beliebige andere, früher an Alice gerichtete Nachricht m entschlüsseln (die mit demselben öffentlichen Schlüssel g^a von Alice verschlüsselt wurde). Z.B. könnte Bob Alice überreden, dass m' garantiert harmlos ist.

Alice benutzt ElGamal in Z^*_{601}. Ihr öffentlicher Schlüssel ist (p, g, g^a) mit $p = 601$, $g = 7$ und $g^a \equiv 362 \bmod p$. Ihr geheimer Schlüssel ist a. Die Botschaft m, an deren Entschlüsselung Bob interessiert ist, ist verschlüsselt als $(g^r, c) = (54, 101)$ (alles in der klassischen Variante, also $c \equiv mk \bmod p$ mit $k = (g^a)^r$). Bob wählt eine Nachricht m_0 und eine Zufallszahl r_0, verschlüsselt diese als (g^{r_0}, c_0). und bittet Alice, $(g^{r'}, c') := (g^r g^{r_0}, c\, c_0)$ zu entschlüsseln. Das tut Alice und gibt die entschlüsselte Nachricht m' an Bob. Bob berechnet $m' m_0^{-1}$ und erhält so m.

(a) Wieso funktioniert das?

(b) Schildern Sie den Angriff an Hand der obigen Werte mit dem konkreten Zahlenbeispiel $m_0 = 234$ und $r_0 = 5$. Dabei dürfen Sie zum Entschlüsseln Alices privaten Schlüssel $a = 51$ benutzen.

Das gehashte ElGamal aus der Vorlesung verhindert diesen Angriff, denn das hat nicht die multiplikative Eigenschaft $f^*(m)f^*(m') = f^*(mm')$; vgl. auch A 26 von Blatt 7.

Abgabe bis Mittwoch 23.6.2021 bis 14 Uhr per Email an den Tutor.

Jan-Philipp Brünger jbruenger@techfak.de
Leonard Simon Ellinghaus lellinghaus+krypto@techfak.de
Kallias Stoupas kstoupas+krypto@techfak.de