Dr. Dirk Frettlöh 28.5.2025

Übungen zur Vorlesung Kryptographie

Blatt 8

Aufgabe 29: (ElGamal mod p)
Der öffentliche ElGamal-Schlüssel von Alice ist $(G, g, g^a) = (Z_{101}^*, 2, 18)$.

(a) Was berechnet Bob, um die Nachricht $m = 11$ mit der Zufallszahl $r = 7$ zu verschlüsseln? Welche Werte sendet er genau an Alice?

(b) Was ist Alice geheimer Schlüssel a?

(c) Was berechnet Alice, um die Nachricht $(c, g^r) = (23, 27)$ zu entschlüsseln?

(d) Nun schickt Bob $(c, g^r) = (77, 37)$. Welches r hat Bob gewählt?

(Teil (b) und (d) gehen natürlich nur, weil die hier verwendeten Zahlen unrealistisch klein sind.)

Aufgabe 30: (Eve vs Shamirs Three-Pass-Protokoll)
Zeigen Sie, dass Shamirs Three-Pass-Protokoll mit $G = Z_p^*$ höchstens so schwierig zu knacken ist wie das Berechnen des diskreten Logarithmus mod p. Genauer: Angenommen, Eve entwickelt eine Methode, den diskreten Logarithmus $\mathrm{dlog}_g(x) \bmod p$ effizient zu berechnen. Zeigen Sie, dass sie dann aus m^a, m^{ab} und $m^{aba'}$ die Nachricht m berechnen kann. *(Tipp: was ist* $\mathrm{dlog}_{m^{ab}}(m^a)$*?)*

Aufgabe 31: (Schmidt-Samoa-Verschlüsselung)
Es gibt neben ElGamal und RSA erstaunlich wenige andere Private-Key-Verschlüsselungsverfahren. Hier sollen Sie eines untersuchen.

Vorab: Alice wählt zwei große Primzahlen p, q und berechnet $N = p^2q$. Außerdem berechnet Sie $d \equiv N^{-1} \bmod R$, wobei R das kleinste gemeinsame Vielfache von $p-1$ und $q-1$ ist.

N ist der öffentliche Schlüssel, p, q, R und d sind geheim.

Verschlüsseln: Bob wählt ein m mit $0 \le m < pq$ und sendet $c \equiv m^N \bmod N$ an Alice.

Entschlüsseln: Alice berechnet m als $m \equiv c^d \bmod pq$.

(a) Zeigen Sie, dass das Verfahren korrekt ist.

(b) N ist ja viel größer als pq. Warum die Einschränkung "m mit $0 \le m < pq$"?

(c) Worauf beruht die Sicherheit dieses Verfahrens? (Also, was müsste Eve können, um das Verfahren zu knacken?)

Aufgabe 32: (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 $1 \le j < i$.

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

(c) Wie kann Alice nun schnell eine Primitivwurzel mod p finden?

Abgabe bis Mittwoch 4.6.2025 bis 14 Uhr per Email an die Tutorin.
Lisa Harms lharms+krypto@techfak.de
Lisa Henetmayr lhenetmayr+krypto@techfak.de