Prof. J. Rothe Düsseldorf, 24.11.2009

Übung zur Vorlesung
Kryptologie 2

Blatt 7, Abgabe: 03.12.2009 bis 15:00 Uhr

Dieses Übungsblatt geht nicht mehr in die Wertung zur Klausurzulassung ein, daher sind Bearbeitung und Abgabe freiwillig. Falls Sie zur eigenen Kontrolle eine Korrektur Ihrer Lösungen wünschen, so können Sie **bis zu drei** Aufgaben dafür kennzeichnen.

Aufgabe 1 (freiwillig): Zeigen Sie:

- $\gamma = 10$ ist ein primitives Element modulo 17,
- in $\mathbb{Z}_{31}^*$ gibt es 8 primitive Elemente,
- $8 \in \mathrm{QR}_{23}$,
- $8 \in \mathrm{QR}_{47}$,
- $21 \in \mathrm{QR}_{59}$,
- $\mathrm{DLogBit}\left(\langle 17, 10, 12, 1\rangle\right) = 1$,
- $\mathrm{DLogBit}\left(\langle 101, 2, 56, 1\rangle\right) = 0$ und
- $\mathrm{DLogBit}\left(\langle 101, 8, 48, 1\rangle\right) = 1$.

Aufgabe 2 (freiwillig): Berechnen Sie:

(a) $3^{15} \mod 100$ mit square-and-multiply,

(b) $5^{17} \mod 50$ mit square-and-multiply,

(c) $21^{-1} \mod 101$ mit dem erweiterten Algorithmus von Euklid,

(d) $49^{-1} \mod 101$ mit dem erweiterten Algorithmus von Euklid,

(e) alle primitiven Elemente modulo 17,

(f) die primitiven Elemente von $\mathbb{Z}_{53}^*$,

(g) $\log_{11} 17 \mod 23$ mit dem Algorithmus von Shanks und

(h) $\log_5 17 \mod 23$ mit dem Pohlig-Hellman-Algorithmus.

Aufgabe 3 (freiwillig): Betrachten Sie das Schlüsseltauschprotokoll von Diffie und Hellman mit $p = 101$, $\gamma = 3$, $a = 65$ und $b = 47$. Berechnen Sie den gemeinsamen Schlüssel k_A (bzw. k_B). Die Angabe des gesamten Protokolls ist optional.

Aufgabe 4 (freiwillig): Seien $p = 23$ und $q = 47$ die Primzahlen in Rabins Kryptosystem. Bestimmen Sie alle möglichen Klartexte zu $c = 8$.

Aufgabe 5 (freiwillig): Finden Sie mit dem Chinesischen Restesatz ein x, für das

$$\begin{aligned} 5x &\equiv 7 \mod 87 \\ 30x &\equiv 45 \mod 97 \end{aligned}$$

gilt.

Aufgabe 6 (freiwillig): Betrachten Sie die Protokolle von ElGamal mit $p = 401$ und $\gamma = 3$.

(a) Wählen Sie $a = 10$, $b = 15$, $m = 323$ und berechnen Sie den Geheimtext (α_1, α_2).

(b) Berechnen Sie anhand von (α_1, α_2) und β aus Aufgabenteil (a) die ursprüngliche Nachricht m (natürlich sollen Ihnen dabei a und b unbekannt sein).

(c) Wählen Sie $s = 231$ und signieren Sie die Nachricht $m = 286$.

(d) Führen Sie einen Known-Message-Angriff auf das Signatur-Protokoll durch (existenzielle Fälschung).

Aufgabe 7 (freiwillig): Gegeben seien $p = 1889$ und $b = 666$. Konstruieren Sie eine superwachsende Folge mit zehn Elementen für das Verfahren von Merkle und Hellman.

(a) Interpretieren Sie $m = 808$ als Binärzahl und verschlüsseln Sie die Bitfolge, die Sie erhalten.

(b) Überprüfen Sie das Ergebnis, indem Sie die verschlüsselte Nachricht wieder entschlüsseln.

Aufgabe 8 (freiwillig): Gegeben seien die Permutationen $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 3 & 1 & 4 \end{pmatrix}$ und $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix}$. Wählen Sie sich einen passenden Graphen G_0 und führen Sie das Zero-Knowledge-Protokoll für Graphisomorphie mit $m = 0$ und $a = 1$ durch. Geben Sie die Graphen dabei jeweils als Adjazenzmatrix an.