Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov

Präsenzübungen zur Vorlesung

Diskrete Mathematik II

SS 2012

Blatt 4 / 05./06. Juni 2012

AUFGABE 1:

Sei $G = (V, E)$ ein Graph. Ein Pfad in G, der jeden Knoten genau einmal enthält, heißt *Hamiltonscher Pfad*. Ein Hamiltonscher Pfad heißt *Pfad von s nach t*, falls er im Knoten $s \in V$ beginnt und im Knoten $t \in V$ endet. Wir definieren

$$\text{UH-Pfad} := \{G \mid G = (V, E) \text{ ungerichtet}, G \text{ besitzt einen } \textit{Hamiltonschen Pfad.}\}$$

$$\text{UH-st-Pfad} := \{(G, s, t) \mid G = (V, E) \text{ ungerichtet}, s, t \in V, G \text{ besitzt einen } \textit{Pfad von } s \textit{ nach } t.\}$$

Zeigen Sie UH-Pfad $\leq_p$ UH-st-Pfad.

AUFGABE 2:

Sei p prim und g ein Generator von $\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\}$. Wir definieren die Sprachen

$$\text{DDH} := \{(g^\alpha, g^\beta, g^y) \mid g^y = g^{\alpha\beta} \bmod p\} \subseteq (\mathbb{Z}_p^*)^3$$

$$\text{ElGamal} := \{(g^a, g^r, m, x) \mid x = m \cdot g^{ar} \bmod p\} \subseteq (\mathbb{Z}_p^*)^4$$

Betrachten Sie folgende Reduktionsabbildung $f : (\mathbb{Z}_p^*)^3 \to (\mathbb{Z}_p^*)^4$ aus der Vorlesung:

Algorithmus 1 Funktion f für DDH $\leq_p$ ElGamal

Eingabe : $(g^\alpha, g^\beta, g^y) \in (\mathbb{Z}_p^*)^3$, Gruppe: $[g, p, q = p-1]$
Ausgabe : $(g^a, g^r, m, x) \in (\mathbb{Z}_p^*)^4$

$g^a \leftarrow g^\alpha$
$g^r \leftarrow g^\beta$
$m \in_R \mathbb{Z}_p^*$ // zufällig, gleichverteilt [muss formal deterministisch gewählt werden]
$x \leftarrow m \cdot g^y \bmod p$
return (g^a, g^r, m, x)

Sei $p = 17$ und $g = 3$. Angenommen wir haben ein ElGamal-Orakel, das uns folgende Informationen liefert:

$$(11, 14, 3, 1),\ (5, 7, 13, 7) \in \textsc{ElGamal},\ (15, 8, 11, 1) \notin \textsc{ElGamal}$$

Entscheiden Sie für folgende Tupel, ob sie in der Sprache DDH liegen:

$$(11, 14, 6),\ (11, 14, 9),\ (5, 7, 13),\ (5, 7, 11),\ (15, 8, 14)$$

AUFGABE 3:

Sei $p = 31$. Berechnen Sie das Legendre-Symbol $\left(\frac{a}{p}\right)$ für die angegebenen $a \in \mathbb{N}$. Sie sollten die Rechenregeln auf Folie 98 und das Quadratische Reziprozitätsgesetz (Folie 99) verwenden. Entscheiden Sie jeweils, ob a ein quadratischer Rest modulo p ist. Führen Sie alle Berechnungen ohne Taschenrechner durch und geben Sie alle Zwischenschritte an.

(a) $a = 2$

(b) $a = 3$

(c) $a = 7$

(d) $a = 21$

AUFGABE 4:

Sei $n = 55$. Entscheiden Sie für folgende $a \in \mathbb{N}$ ob a ein quadratischer Rest modulo n ist. Falls vorhanden, geben Sie alle Lösungen der Gleichung $b^2 = a \bmod n$ an (Quadratwurzeln von a).

Berechnen Sie dazu einer Liste aller Quadrate modulo jedem Teiler von n und lesen Sie daraus die Wurzeln modulo den Teilern ab. Setzen Sie diese dann mit dem Chinesischen Restsatz zu einer Wurzel modulo n zusammen.

Bestimmen Sie zudem jeweils das Jacobi-Symbol $\left(\frac{a}{n}\right)$. Führen Sie alle Berechnungen ohne Taschenrechner durch und geben Sie alle Zwischenschritte an.

(a) $a = 14$

(b) $a = 20$

(c) $a = 38$

(d) $a = 43$

Hinweis: Es gilt $11^{-1} = 1 \bmod 5$ und $5^{-1} = -2 \bmod 11$.