RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Hausübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 10 / 18. Dezember 2012 / Abgabe bis spätestens 8. Januar 2013, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (3 Punkte)**:**
Konstruieren Sie einen Algorithmus, der das k-Listen Problem für $k = 2^m + j$ mit $0 < j < 2^m$ mit Komplexität $\tilde{O}(2^m 2^{\frac{n}{m+1}})$ löst.
Bemerkung: Die Begründung für Korrektheit und Laufzeit kann sehr kurz ausfallen.

AUFGABE 2 (7 Punkte)**:**

(a) Sei $n \in \mathbb{N}$ gerade. Seien $a_0, \ldots, a_{n-1} \in \mathbb{N}$ und $S \in \mathbb{N}$, wobei es eine Menge $I \subset \{0, \ldots, n-1\}$ gibt mit $\sum_{i \in I} a_i = S$ und $|I| = \frac{n}{2}$.

Zeigen Sie, dass es ein $k \in \{0, \ldots, n-1\}$ gibt, so dass für die *zklisch* permutierte Folge $a'_0, \ldots, a'_{n-1}$ mit $a'_i = a_{i+k \bmod n}$ gilt:
Es existiert $I' \subset \{0, \ldots, n-1\}$ mit $\sum_{i \in I'} a'_i = S$, $|I'| = \frac{n}{2}$ und $|I' \cap \{0, \ldots, \frac{n}{2} - 1\}| = \lfloor \frac{n}{4} \rfloor$.

(b) In der Vorlesung hatten wir das Subset Sum Problem kennen gelernt, bei der wir genau die Hälfte der Elemente genommen hatten. Wir wollen dies verallgemeinern zu einem Algorithmus, der das Problem für niedrigeres (bekanntes) Gewicht $\frac{1}{3}$ löst:

Gegeben seien $a_1, \ldots, a_n, S \in \mathbb{N}$.
Gesucht: $I \subset \{1, \ldots, n\}$ mit $|I| = \lceil \frac{n}{3} \rceil$ mit $\sum_{i \in I} a_i = S$.

Verallgemeinern sie den Meet-In-The-Middle Angriff aus der Vorlesung von $|I| = \frac{n}{2}$ auf den hier vorliegenden Fall $|I| = \frac{n}{3}$ und geben Sie dessen Laufzeit in der Form $\widetilde{O}(2^{\gamma n})$ an.

Bemerkung: (a) zeigt, dass man den Meet-In-The-Middle Algorithmus aus der Vorlesung deterministisch machen kann mit höchstens n Permutationen, wenn man diese als zyklische Permutationen wählt.
Hinweis: Für (a) ist es hilfreich, die Grösse $\Delta = |I' \cap \{0, \ldots, \frac{n}{2} - 1\}| - |I' \cap \{\frac{n}{2}, \ldots, n-1\}|$ zu betrachten. Wenn man I' als das Bild von I unter zyklischer Permuation wählt, wie verändert sich Δ, wenn man k um 1 vergrössert? Wie verändert sich Δ, wenn man k um $\frac{n}{2}$ verändert?

Frohe Weihnachten und einen Guten Rutsch!