

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 10 / 21. Dezember 2011

AUFGABE 1:

Geben Sie eine Verallgemeinerung des k -Listen Algorithmus (Folie 39) an, so dass man $x_i \in L_i$ findet mit

$$x_1 \oplus \dots \oplus x_k = c$$

für beliebiges $c \in \{0,1\}^n$. Der Algorithmus sollte die gleiche Laufzeit $\tilde{O}(k2^{\frac{n}{\log k+1}})$ haben. Begründen Sie kurz die Korrektheit.

AUFGABE 2:

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.

AUFGABE 3:

Lösen Sie das folgende 4-Listen Problem mit dem Algorithmus von Bellare und Micciancio (Folie 49):

$$L_1 = \{1010, 0111, 0100\}$$

$$L_2 = \{1100, 0010, 1011\}$$

$$L_3 = \{1011, 0111, 0011\}$$

$$L_4 = \{0110, 0011, 1001\} .$$

Frohe Weihnachten und einen Guten Rutsch!