TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

2. Übung Kryptographie

1. Aufgabe

Zur Verallgemeinerung des Meet-in-the-Middle (MITM) Angriffs betrachten wir endliche Mengen A_1, A_2, B der Kardinalitäten n_1, n_2, m, Elemente $a_1 \in A_1$, $a_2 \in A_2$ und Funktionen $f_{1,i} : A_1 \to B$, $f_{2,i} : A_2 \to B$ mit $f_{1,i}(a_1) = f_{2,i}(a_2)$ für $1 \leq i \leq r$. Ziel ist es, alle $(a_1', a_2') \in A_1 \times A_2$ zu finden mit $f_{1,i}(a_1') = f_{2,i}(a_2')$ für alle i.

(a) Gebt einen Meet-in-the-Middle Angriff für die obige Situation an. Wie groß ist der Speicher- und Arbeitsaufwand? Formuliert den Meet-in-the-Middle Angriff auf die Zwei-Schlüssel Kombination aus der Übung in der obigen Notation.

(b) Betrachtet den Meet-in-the-Middle Angriff auf die Zwei-Schlüssel Kombination aus der Übung mit $\#M = \#C = \#K$ und mit zwei Plaintext-Ciphertext-Paaren umformuliert in obige Notation. Bestimmt die (ungefähre) Wahrscheinlichkeit, daß $a_1' = a_1$ und $a_2' = a_2$ ist. Ungefähre bedeutet sowas wie „unter sinnvollen vereinfachenden Annahmen“.

(c) Wie kann man das Verhältnis von benötigter Zeit und benötigtem Speicher verändern? (Hinweis: A in disjunkte Mengen A_j gleicher Größe für $1 \leq j \leq s$ aufteilen.) Wie groß sind nun Speicher- und Zeitbedarf? Was kann über deren Produkt gesagt werden?

(6 Punkte)

2. Aufgabe

Zeigt, dass bei DES für alle Klartexte m und Schlüssel k gilt

$$\overline{DES(m,k)} = DES(\overline{m}, \overline{k}),$$

wobei $\bar{\cdot}$ die Abbildung mit $\overline{1} = 0$ und $\overline{0} = 1$ ist.

(4 Punkte)

3. Aufgabe

Aus einem Kryptosystem mit Ver- und Entschlüsslungsfunktion $e : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ bzw. $d : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ und $d(k, e(k,m)) = m$ für alle $k, m \in \{0,1\}^n$ kann man ein neues Kryptosystem definieren, bei dem durch die Abbildung $E : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n, (m, k_1, k_2, k_3) \mapsto e(k_3, d(k_2, e(k_1, m)))$ verschlüsselt wird. Gebt einen MITM Angriff auf diese ede Kombination an. Wieviele Schlüssel müssen durchprobiert werden, wieviel muss man speichern? Gebt die Größenordnung der für diesen Angriff benötigten Anzahl an Klartext-Chiffretext-Paaren an.

(4 Punkte)

4. Aufgabe

Ein unbekannter Verschlüsselungsalgorithmus wurde in einem Stück Kommunikationshardware verwendet. Die technische Abteilung konnte die Maschineninstruktionen auslesen und hat den Verschlüsselungsalgorithmus nachimplementiert. Es handelt sich um eine Doppelverschlüsselung mit zwei unterschiedlichen Schlüsseln (ee Kombination). Auch konnte festgestellt werden, aus welchen Zeichen das Schlüsselalphabet A besteht und von welcher Form die Schlüssel sind. Des weiteren wurden zwei Klar- und Chiffretextpaare und ein weiterer Chiffretext gefunden. Führen Sie einen MITM Angriff auf den Chiffre aus. Alles Nötige befindet sich in der Datei mitm.k.

(6 Punkte)