TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
www.math.tu-berlin.de/~hess/krypto-ws2008

2. Übung Kryptographie

1. Aufgabe

(a) Sei $(G, \star)$ eine endliche Gruppe. Ein Verschlüsselungssystem benutzt $M = G$ als Klartextraum und es gelte $M = C = K$. Als Verschlüsselungsfunktion wird

$$E : K \times M \longrightarrow C, \quad k \star m = c$$

benutzt. Zeigen Sie, dass dieses System unter der Annahme, dass nur einmal mit einem bestimmten Schlüssel verschlüsselt wird und dass $p(k) = \frac{1}{|K|}$ für alle $k \in K$ gilt, ein perfekt sicheres System ist.

(b) Gibt es Bedingungen unter denen der Cäsar-Chiffre oder Vigenère-Chiffre perfekt sicher ist?

(4 Punkte)

2. Aufgabe

Zur Verallgemeinerung des Meet-in-the-Middle Angriffs betrachten wir endliche Mengen A_1, A_2, B der Kardinalitäten n_1, n_2, m, Elemente $a_1 \in A$, $a_2 \in A_2$ 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.

(i) Geben Sie einen Meet-in-the-Middle Angriff für die obige Situation an. Wie groß ist der Speicher- und Arbeitsaufwand? Formulieren Sie den Meet-in-the-Middle Angriff auf die Zwei-Schlüssel Kombination aus der Vorlesung in der obigen Notation.

(ii) Betrachten sie den Meet-in-the-Middle Angriff auf die Zwei-Schlüssel Kombination aus der Vorlesung mit $\#\mathcal{P} = \#\mathcal{C} = \#\mathcal{K}$ und mit zwei Plaintext-Ciphertext-Paaren umformuliert in obige Notation. Bestimmen Sie die (ungefähre) Wahrscheinlichkeit, daß $a_1' = a_1$ und $a_2' = a_2$ ist. Ungefähre bedeutet sowas wie „unter sinnvollen vereinfachenden Annahmen“.

(iii) 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?

(5 Punkte)

3. Aufgabe

MITM Angriffe lassen sich auf die EDE Kombination aus der Vorlesung anwenden.

(iv) Geben Sie einen MITM Angriff auf die EDE Kombination mit drei verschiedenen Schlüsseln an. Wieviele Schlüssel müssen durchprobiert werden, wieviel muss man speichern.

(v) Bei der EDE Kombination mit zwei verschiedenen Schlüsseln genügt bei einen CPA-Angriff $O(\#\mathcal{K})$ viel Speicher und $O(\#\mathcal{K})$ viel Laufzeit. Wie geht das?

(5 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. Vergleichen sie die Dauer mir einer exhaustive search.

(6 Punkte)