TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto-ws2006

2. Übung Kryptographie

1. Aufgabe **Perfekte Sicherheit** **(4 Punkte)**

(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 $p(k) = \frac{1}{|K|}$ für alle $k \in K$ ein perfekt sicheres System ist.

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

2. Aufgabe **(6 Punkte)**

Meet-in-the-Middle, time-memory tradeoff. 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 gleichverteilt zufällig gewählte 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) Bestimmen Sie die (ungefähre) Wahrscheinlichkeit, daß $a_1' = a_1$ und $a_2' = a_2$ ist.

(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?

Einen MITM Angriff kann man häufig anwenden, wenn Variablen über den Suchraum in zwei unabhängige Teile aufgeteilt werden können. Als Beispiel betrachten wir die EDE Kombination.

(iv) Geben Sie einen MITM Angriff auf die EDE Kombination mit drei verschiedenen Schlüsseln an. (Hinweis: EDE geeignet in f_1 und f_2 aufteilen.)

(v) Bei der EDE Kombination mit zwei verschiedenen Schlüsseln kann man die Variablen k_1 und k_2 trennen, wenn man einen CPA-Angriff vorausetzt. Wie geht das?

3. Aufgabe **(2 Punkte)**

Modes. Welche Gefahren birgt die Verwendung konstanter IV's in CBC und mehrfach verwendeter Nonces in CTR?

4. Aufgabe **(8 Punkte)**

Praktische Aufgabe. Gegeben sind die unten aufgeführten Klar- und Chiffretextpaare und ein weiterer Chiffretext. 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 die Schlüssel alle von der Form $k \in A^n$ mit $n \leq 5$ sind.

Das Alphabet A und die Ver- und Entschlüsselungsalgorithmen E und D stehen Ihnen in KASH3 zur Verfügung, die Programme sind auf der Webseite abgelegt unter MITM.k. Sie rufen diese mit $E(k, m)$ bzw. $D(k, E(k, m))$ auf wobei $k \in A^n$ ein Schlüssel umd $m \in A^*$ ein Klartext ist.

Führen Sie einen MITM Angriff auf den Chiffre aus! Wie lautet der Klartext zum Chiffretext? Wie sehen die verwendeten Schlüssel der angewandten EE-Chiffrierung aus?

(m_1, c_1) = ("WENN SIE DIESEN TEXT ENTSCHLUESSELT HABEN",
"WGDG U?! F?!SGDXTGNM GDMSE!EUGILENJXHCW!NCVY")
(m_2, c_2) = ("DANN HABEN SIE DAMIT BEWIESEN, DASS SIE",
"DCDG JVZEPULIGU.AO?M DZPIGI!N!U.AUIXSKZX")

c_3 = "EKDXGWJ!RBAKYRJHLQ.! U?GDCVY"

Gesamt: 20 Punkte