2. Übung Kryptographie

(Modes, Meet-in-the-middle Angriff, DES und AES)

1. Aufgabe

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

(2 Punkte)

2. Aufgabe

- (a) Welche Auswirkung hat es, wenn man beim DES die Rundenschlüssel k_i in der umgekehrten Reihenfolge anwendet?
- (b) Das Bitkomplement sei mit $\bar{\cdot}$ bezeichnet. Also $\bar{1} = 0$ und $\bar{0} = 1$. Zeigen Sie, dass $DES(\overline{m}, \bar{k}) = \overline{DES(m, k)}$ gilt.

(5 Punkte)

3. Aufgabe

- (a) Sei $p = 30259$ und $\alpha = 11235$ gegeben. Berechnen Sie $\alpha^{-1} \in \mathbb{F}_p$ mit Hilfe des erweiterten euklidischen Algorithmus. Schreiben Sie jeden Rechenschritt auf.
- (b) Im Rijndael-Verfahren (AES) wird in einem endlichen Körper $K := \mathbb{F}_{2^8}$ gerechnet. Dazu wird ein festes Polynom $f(x) = x^8 + x^4 + x^3 + x + 1 \in K$ vorgegeben. Die Elemente von K lassen sich als Polynome in $\mathbb{F}_2[x]$ auffassen und haben den Grad ≤ 7 . Berechnen Sie das inverse Element von $g(x) = x^7 + x^3 + x + 1$, d.h. ein Element $g^{-1} \in \mathbb{F}_2[x]$ mit der Eigenschaft $g \cdot g^{-1} \equiv 1 \pmod{f}$. Benutzen Sie dazu den erweiterten euklidischen Algorithmus. Schreiben Sie jeden Rechenschritt auf.
- (c) Sei $B := \{1, \zeta, \zeta^2, \dots, \zeta^7\} \subseteq K$ eine Basis des $\mathbb{F}_2$ -Vektorraumes K und $\alpha = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 \in K$. Außerdem gilt $\zeta^8 + \zeta^4 + \zeta^3 + \zeta + 1 = 0$. Bestimmen Sie die Darstellende Matrix bezüglich der Basis B für die Abbildung

$$\phi : K \longrightarrow K, \quad x \longmapsto \alpha \cdot x.$$

- (d) Zeigen Sie, dass die Funktionen ϕ und ϕ^{-1} vom Skript Seite 22 in der Tat Inverse zueinander sind.

(10 Punkte)

4. 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, welches aber mit TextToNumbers als Zahlen wahrgenommen wird, das heißt, dass die Schlüssel alle von der Form $k_1 = I_n$ und $k_2 = a^n$ mit $n \leq 4$ sind, wobei I_n die Einheitsmatrix mit n Zeilen und $a \in \mathbb{Z}/31\mathbb{Z}$ 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 und $m \in A^*$ 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?

$(m_1, c_1) = \left(\text{„WENN SIE DIESEN TEXT ENTSCHLUESSELT HABEN“}, \right.$
 $\left. \text{„WGFNBKIGWDK.SGF V.XVWEPLSE LW.SU.LVWHCYEPX“} \right)$

$(m_2, c_2) = \left(\text{„DANN HABEN SIE DAMIT BEWIESEN, DASS SIE“}, \right.$
 $\left. \text{„DCFNB AD.NBKIGWDCEIVWBGOIGKEPS FXSUWSK.“} \right)$

$c_3 = \text{„EKF IMTGJ MJYRLONGGGWSKFDCX“}$

(6 Punkte)

5. Aufgabe

Implementieren Sie AES mit den Schlüssellängen 128, 192 und 256 in KASH3. Ver- und entschlüsseln Sie Ihre Matrikelnummern, die durch Anfügen von „F“s auf die richtige Blocklänge gebracht werden (d.h. verwenden Sie ihre Matrikelnummern sowohl als Klartext als auch als Chiffretext). Zur Hilfestellung gibt es ein paar vorprogrammierte Funktionen in der Datei AES.k auf der Webseite der VL.

Hinweis (Stand: 02.11.2007): Die praktische Aufgabe 5 kann bis zum 09.11.07 abgegeben werden. Die praktische Aufgabe 4 kann bis zum 16.11.07 abgegeben werden.

(8 Punkte)