G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 2

Aufgabe 1 *Delta-Sets*
Zur Erinnerung:
Definition Ein Δ-Set ist eine Menge von AES Zuständen. In einem Delta-Set sind alle Positionen *aktiv* oder *passiv*. D.h. für je zwei verschiedenen Elemente gilt

$$\forall a, b \in \Delta \quad a \neq b \Rightarrow \begin{cases} a_{ij} = b_{ij} & (i,j) \text{ ist passiv} \\ a_{ij} \neq b_{ij} & (i,j) \text{ ist aktiv} \end{cases}$$

Konstruieren Sie

1. ein Menge mit 3 Elementen an, die ein Δ-Set ist.
2. ein Menge mit 3 Elementen an, die kein Δ-Set ist.

Weisen Sie folgende Eigenschaften von Delta-Sets nach

1. Jede Menge von weniger als drei AES Zuständen ist ein Delta-Set.
2. Die maximale Grösse eines Delta-Sets ist 256.

Aufgabe 2 *Square Attacke*
Verfolgen Sie die Veränderungen eines Delta Set mit 256 Elementen und genau einer aktiven Position, bei der Verschlüsselung mit AES reduziert auf 4 Runden (die letzte Runde ist eine AES *final round*. Zeigen Sie insbesondere, dass für die Zustände vor der vierten Runde Δ' gilt

$$\sum_{a \in \Delta'} a_{ij} = 0 \quad \forall i, j.$$

Aufgabe 3 *Alternative Darstellungen von AES*

1. Zeigen Sie, das die Reihenfolge von **ByteSub** und **ShiftRows** vertauscht werden kann.
2. Überlegen Sie, wie man durch *einfache* Änderungen am Key Scheduling auch die Operationen **MixColumn** und **KeyAdd** vertauschen kann.
3. Nutzen Sie diese Vertauschungen um bei der Entschlüsselung von AES die selbe Reihenfolge aller Operationen zu erhalten wie bei der Verschlüsselung. Lediglich die einzelne Operationen sollen durch ihre Inversen ausgetauscht werden müssen.

Aufgabe 4 *Effiziente Implementierung auf 32-Bit Prozessoren*
Auf 32-Bit Prozessoren kann man die Operationen

1. **ByteSub**

2. **ShiftRows**

3. **MixColumn**

durch große Tabellen und lediglich 4 XOR-Operationen durchführen und somit eine sehr effiziente Umsetzung von AES zu erhalten. Überlegen Sie, wie eine solche Implementierung funktionieren kann.