Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 04.12.2015

Einführung in Kryptographie

WS 2015/2016

Präsenzübungszettel 4

AUFGABE 1:
Welche der in DES verwendeten Funktionen *Expansion*, *Permutation*, *Substitiution* S_1 ist linear und welche nicht? Beweisen Sie die Linearität in $\mathbb{Z}_2^m$ für entsprechendes m.

AUFGABE 2:
Führen Sie die Operationen des AES-Kryptosystems an den folgenden Beispielen exemplarisch durch. Achten Sie darauf, dass Ihr Rechenweg stets nachvollziehbar bleibt.

a) Wir betrachten AES aus der Vorlesung. Der aktuelle Zustand eines Nachrichtenbytes (in hexadezimaler Notation) sei ED und das dazugehörige Rundenschlüsselbyte sei D2. Berechnen Sie das resultierende Byte nach der AES Operation AddRoundKey.

b) Eine Eingabe für den Substitionsschritt sei das Byte 9D. Berechnen Sie das Ergebnis der Operation SubBytes auf diesem Byte.

c) Der aktuelle Zustand einer Nachricht sei gegeben durch die folgende Matrix:

75	5E	E4	31
6F	7D	93	EF
AA	6D	44	1E
3B	65	93	41

Bestimmen Sie den Zustand nach der Operation ShiftRows.

AUFGABE 3:
Gegeben seien die Primzahlen $p = 5$ und $q = 17$, und sei $N = pq$. Berechnen Sie:

a) $x \equiv 53^{33} \pmod{N}$ mit $x \in \mathbb{Z}_N$

b) $y \equiv 7^{64064006402} \pmod{N}$ mit $y \in \mathbb{Z}_N$