G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 1

Aufgabe 1 *DES*
Weisen Sie die komplementär Eigenschaft des DES nach, d.h.

$$\overline{DES(K, M)} = DES(\overline{K}, \overline{M}).$$

Wie kann man das bei einem Brute Force Angriff nutzen?

Aufgabe 2 *Multiple Encryption*

1. Überlegen Sie, warum eine zweifache Verschlüsselung mit DES (mit zwei verschiedenen Schlüsseln) nicht viel sicherer ist als eine einfache Verschlüsselung. Gilt das für jeden Block-Cipher?
2. Überlegen Sie sich ein Verschlüsselungsverfahren, bei dem mehrfach Verschlüsselung keine erhöhte Sicherheit liefert? Wie kann man die nötige Eigenschaft mathematisch formulieren?

Aufgabe 3 *Multiple Encryption II*
Eine Time-Memory-Tradeoff Variante.

1. Wie lässt sich der Angriff auf zweifache Verschlüsselung abwandeln um Speicher zu sparen und dafür einen höheren Rechenaufwand zu betreiben ?
2. Welche Größe ist die Invariante bei all diesen Angriffen? Wie lassen sich somit vollständige Schlüssel Suche und Aufstellen einer einzigen Tabelle hier einordnen?

Aufgabe 4 *DES Kriterien*

1. Überprüfen Sie die Design Kriterien S1 und S3 für die S-Boxen des DES.
2. Überprüfen Sie (beispielhaft) die Design Kriterien S4 und S5 für die S-Boxen des DES.