

# 11. Übungsblatt Kryptographie I (SS 2006)

Stefan Lucks, Dirk Stegemann, Emin Islam Tatli

**Besprechung:** Mittwoch, 12. Juli 2006

## Modes of Operation

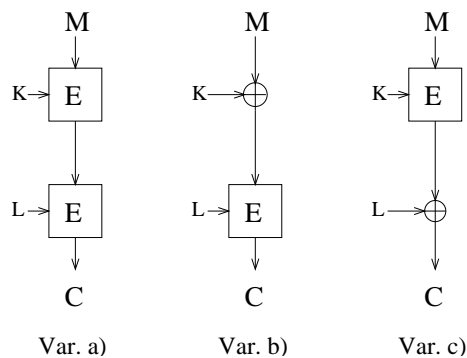
**Aufgabe 1** Sei  $E$  eine Substitutionschiffre mit Blocklänge 2 Bit. Der Schlüssel  $k$  sei bekannt, und es gilt:

$$\begin{aligned} E_k(0) &= 3 \\ E_k(1) &= 1 \\ E_k(2) &= 0 \\ E_k(3) &= 2 \end{aligned}$$

Verschlüssele (per Rechner oder von Hand) den Klartext '3012201113'

- a) im *Electronic Codebook Mode*,
- b) im *Cipher Block Chaining Mode* mit Initialwert '2',
- c) im *Output Feedback Mode* mit Initialwert '2',
- d) im *Cipher Feedback Mode* mit Initialwert '2' und
- e) im *Counter Mode* mit Initialwert '2'.

**Aufgabe 2** Gegeben sei eine Blockchiffre  $E$  mit Block- und Schlüssellänge  $k$ . Dabei sei  $k$  so klein, dass ein Brute-Force-Angriff gegen  $E$  möglich ist. Daher soll mit Hilfe von  $E$  eine neue Blockchiffre mit Schlüssellänge  $2k$  konstruiert werden. Ein Klartextblock  $M$  wird unter einem Schlüssel  $(K, L)$  verschlüsselt wie in der nachfolgenden Abbildung dargestellt:



- a) Gib für die linke Chiffre einen Angriff an, der den Schlüssel  $(K, L)$  rekonstruiert.
- b) Gib für die mittlere bzw. die rechte Chiffre einen Angreifer an, der den Schlüssel  $(K, L)$  rekonstruiert und dazu nur linearen Speicherplatz benötigt.

**Bem.:** Die Varianten b) und c) sind durch Modifikation der DESX-Konstruktion entstanden.

## Krypto-Schnitzeljagd

**Aufgabe 3** Dieses Jahr bieten wir euch etwas ganz besonderes: eine Krypto-Schnitzeljagd. Los gehts bei

<http://th.informatik.uni-mannheim.de/teach/Krypto-06/uebungen/Schnitzeljagd/>

Viel Spass und viel Erfolg!