Gruppe 13: Leonard Bongard , Duy Quang Nguyen , Egemen Ulutürk , Thiemo Ganesha Welsch

# Computersystemsicherheit – Hausübung 1

Aufgabe 2

(a) $Dec(Enc(b_1,...,b_n), \pi) = Dec((b_{\pi(1)}, ..., b_{\pi(n)}), \pi)$
$= (b_{\pi\pi\text{-}1(1)}, ..., b_{\pi\pi\text{-}1(n)})$
(→ Keys heben sich auf) $= (b_{(1)}, ..., b_{(n)})$

(b) Enc ((101,010,101,010), π) = (011,100,011,100)
Der verschlüsselte String ist: 011100011100.

(c) Bei einer **ECB**-Verschlüsselung findet keine Verkettung zwischen den Verschlüsselungen statt, daher wird nur der Block m1 von diesem Fehler beeinflusst.

Bei einer **CBC**-Verschlüsselung werden aber die verschlüsselten Sequenzblöcke an die nächste Block-Verschlüsselung als Vektor weitergegeben. Folglich verfälscht der erste Fehler auch die nachkommende Verschlüsselung.

Aufgabe 3

(a) Uclx : mit dem Abstand 10
Kdfeywtqxp : mit dem Abstand 25

(b) 10 hat die Primfaktoren 2 und 5
25 hat den Primfaktor 5

(c) Die Länge des Schlüssels ist wahrscheinlich 5, da die Fünf der einzige gemeinsame Teiler der Abstände ist.

(d) EckOstgloaUclxatrxmfUclxrvkuikugfqwobxvKdfeywtqxpdbcgkw
CcbomsxxrKdfeywtqxpfhcaxvjclkmubtwafqbgzpdmaafbxvzpjxr
Als Klartext :
derkasiskitestisteintestzumbestimmenderschluessellaengebeikurzenschluesselngehtdiesgutdasiesichoftwiederholen