Aufgabe 3.1 (2 Pkt.)

Sie haben in der Vorlesung 3DES mit zwei Schlüsseln kennen gelernt, wobei eine Nachricht $m \in \{0,1\}^{64}$ mit der Chiffre c,

$$c \leftarrow \mathrm{DES}\Big(\mathrm{DES}^{-1}\big(\mathrm{DES}(m,k_1),k_2\big),k_1\Big),$$

verschlüsselt wird. Die Schlüssel in $\{0,1\}^{56}$ werden mit t_i bezeichnet, $i = 1,\ldots,2^{56}$. Betrachten Sie folgende Chosen-Plaintext-Attacke:

for $i \leftarrow 1$ **to** 2^{56} **do**
  $a_i \leftarrow \mathrm{DES}^{-1}(0^{64}, t_i)$
  trage (a_i, t_i) in eine Tabelle T ein
for $i \leftarrow 1$ **to** 2^{56} **do**
  $c_i \leftarrow \mathrm{DES}\Big(\mathrm{DES}^{-1}\big(\mathrm{DES}(a_i,k_1),k_2\big),k_1\Big)$
  $b_i \leftarrow \mathrm{DES}^{-1}(c_i, t_i)$
  if *in* T *gibt es ein* a_j *mit* $a_j = b_i$ **then**
    gib (t_i, t_j) als mögliches Schlüsselpaar aus
    stop

Zeigen Sie, dass zumindest für das Paar (a_i, c_i) das Schlüsselpaar (t_i, t_j) korrekt ist.

Anmerkung: Der Algorithmus führt $\approx 2^{56}$ Operationen aus statt $\approx 2^{112}$. Ob (t_i, t_j) tatsächlich das richtige Schlüsselpaar ist, kann durch das Verschlüsseln weiterer Klartexte festgestellt werden.

Aufgabe 3.2 (2+2 Pkt.)

Betrachten Sie eine Feistel-Chiffre mit Blocklänge 8 und einer Abbildung

$$\{0,1\}^4 \times \{0,1\}^4 \to \{0,1\}^4 \times \{0,1\}^4, \quad (L_{i-1}, R_{i-1}) \mapsto (L_i = R_{i-1}, R_i = L_{i-1} \oplus f_{k_i}(R_{i-1}))$$

in der i-ten Runde. Die Funktion $f_{k_i}\colon \{0,1\}^4 \to \{0,1\}^4,\ R_{i-1} \mapsto P(R_{i-1} \oplus k_i)$ sei gegeben durch den Schlüssel $k_i \in \{0,1\}^4$ der i-ten Runde, P vertausche die Bits gemäß der Permutation (134)(2) (d. h. das Bit an Position 1 wird zu Position 3 verschoben usw.). Der Klartext `01011001` werde mit n Runden dieser Chiffre zu `10010000` verschlüsselt.

a) Bestimmen Sie den Rundenschlüssel k_1, falls $n = 1$.

b) Bestimmen Sie die Rundenschlüssel k_1 und k_2, falls $n = 2$.

Aufgabe 3.3 (3+1 Pkt.)

Gegeben sei ein linear rückgekoppeltes Schieberegister mit unbekannter Rückkopplungsfunktion $f : \{0,1\}^n \mapsto \{0,1\}$. Auch die Initialisierung des Registers sei unbekannt. Wir bezeichnen mit $s_0, s_1, s_2, \ldots$ die Ausgabebits in der Reihenfolge ihrer Generierung und definieren für $i \in \mathbb{N}_0$ die n-Tupel $b_i := (s_i, \ldots, s_{i+n-1})$. Weiter sei t_0 die kleinste Zahl, sodass die Vektoren $b_0, \ldots, b_{t_0}$ linear abhängig sind.

a) Zeigen Sie: Man benötigt höchstens $t_0 + n$ aufeinanderfolgende Ausgabebits, um auf den Schlüssel und die gesamte Ausgabesequenz schließen zu können.

b) Zeigen Sie, dass $2n$ aufeinanderfolgende Ausgabebits stets genügen, um das in a) beschriebene Problem zu lösen.

Aufgabe 3.4 (3 Pkt.)

Lösen Sie die SPOX-Aufgabe Autokey-Chiffre, die die Autokey-Variante 2 behandelt.

Aufgabe 3.5 (2+1 Pkt.)

In der Vorlesung wurde der Aufbau der Enigma-Verschlüsselungsmaschine beschrieben.

Die Walzen der Enigma bewirken eine Permutation A der 26 Buchstaben des Alphabets, die von der Auswahl und Stellung der Walzen abhängt und sich nach jedem kodierten Zeichen ändert. A besteht aus 13 disjunkten Transpositionen (paarweisen Vertauschungen), in Zyklenschreibweise:

$$A = (a_1 a_2)(a_3 a_4) \cdots (a_{25} a_{26}) \quad \text{mit} \quad \{a_1, \ldots, a_{26}\} = \{\mathtt{A}, \ldots, \mathtt{Z}\}\,.$$

a) Wir nehmen an, nach dem Verschlüsseln einer gewissen Anzahl an Buchstaben entsprächen die Walzen einer Permutation B,

$$B = (b_1 b_2)(b_3 b_4) \cdots (b_{25} b_{26}) \quad \text{mit} \quad \{b_1, \ldots, b_{26}\} = \{\mathtt{A}, \ldots, \mathtt{Z}\}\,.$$

Begründen Sie: Die Häufigkeit jeder Zyklenlänge in der Permutation $B \circ A$ ist gerade.

b) Das Steckerfeld der Enigma entspricht einer weiteren Permutation S. Es bewirkt, dass auf die Klartextzeichen nicht die Walzenpermutation A angewandt wird, sondern die Permutation $T := S^{-1} \circ A \circ S$. Beweisen Sie: Die Häufigkeiten der Zyklenlängen in A und der Zyklenlängen in T stimmen überein. (Diese Eigenschaft gilt für beliebige Permutationen A und S.)