Martin Braun (1249080), Julian Neuberger(1252734)

Aufgabe 4.1

a)
Schritt 1: Man schickt eine Nachricht, von der man die verschlüsselte Form kennt oder vorhersagen kann. (→ zb. 15 mal 0). Man bekommt so den permutierten Initialisierungsvektor.

Schritt 2: Nun verändert man die Nachricht systematisch um die Permutationsmatrix zu bestimmen. Zum Beispiel indem man an jede Stelle i der in Schritt 1 verwendeten Nachricht einmal eine 1 schreibt. Nun vergleicht man die verschlüsselte Nachricht mit der in Schritt 1 erhaltenen. Nun weiß man auf welche Stelle j die originale Stelle i in der verschlüsselten Nachricht abgebildet wird → Man erhält so systematisch die Permutationsmatrix:

$(i1\ i2\ ..\ in)$
$(j1\ j2\ ..\ jn)$

b)
Schritt 1:
Klartext: 00000 00000 00000
Chiffriert: `01110 01011 11001 → permutierter Initialisierungsvektor`

Schritt 2:

i	chiffrierte Nachricht	abgebildet auf
1	01110 01011 11011	14
2	01110 01011 01001	11
3	00110 01011 11001	2
4	01110 01011 11000	15
5	01111 01011 11001	5
6	01110 01010 11001	10
7	01010 01011 11001	3
8	01110 11011 11001	6
9	01110 01011 10001	12
10	01110 00011 11001	7
11	01110 01111 11001	8

12	01110 01011 11101	13
13	01110 01001 11001	9
14	11110 01011 11001	1
15	01100 01011 11001	4

Permutationsmatrix:

```
(1  2  3  4  5  6  7  8  9  10 11 12 13 14 15)
(14 11 2  15 5  10 3  6  12 7  8  13 9  1  4 )
```

IV:

```
(01110 11011 00101)
```

Aufgabe 4.1

a)
Invers, wenn: k x k^{-1} = Identität

```
(11 8)x(7  18) soll sein (1 0)
(3  7) (23 11)           (0 1)
```

Matrixmultiplikation:

```
(11x7+8x23 11x18+8x11) = (261 286) = (1 0)
(3x7+7x23  3x18+7x11)    (182 131)   (0 1)
```

➔ Ist Inverse

b)
Zum kompilieren: Siehe README

c)

Using the message basketball with key [[13.0, 2.0, 9.0, 1.0], [3.0, 6.0, 25.0, 10.0], [7.0, 22.0, 22.0, 11.0], [8.0, 5.0, 13.0, 4.0]]
Multiplying: key x [[1.0], [0.0], [18.0], [10.0]]=[[185.0], [553.0], [513.0], [282.0]],
which is: dhtw
Multiplying: key x [[4.0], [19.0], [1.0], [0.0]]=[[99.0], [151.0], [468.0], [140.0]],
which is: vvak
Multiplying: key x [[11.0], [11.0], [0.0], [0.0]]=[[165.0], [99.0], [319.0], [143.0]],
which is: jv
Result: **dhtwvvakjv**

d)

Using the message tdeuxzvgwxvltxmn with key [[5.0, 9.0, 9.0, 10.0], [25.0, 0.0, 1.0, 17.0], [19.0, 2.0, 3.0, 8.0], [1.0, 21.0, 10.0, 24.0]]
Multiplying: key x [[19.0], [3.0], [4.0], [20.0]]=[[358.0], [819.0], [539.0], [602.0]],
which is: unte
Multiplying: key x [[23.0], [25.0], [21.0], [6.0]]=[[589.0], [698.0], [598.0], [902.0]],
which is: rwas
Multiplying: key x [[22.0], [23.0], [21.0], [11.0]]=[[616.0], [758.0], [615.0], [979.0]],
which is: serr
Multiplying: key x [[19.0], [23.0], [12.0], [13.0]]=[[540.0], [708.0], [547.0], [934.0]],
which is: ugby
Result: **unterwasserrugby**