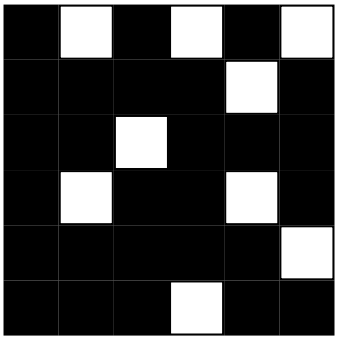
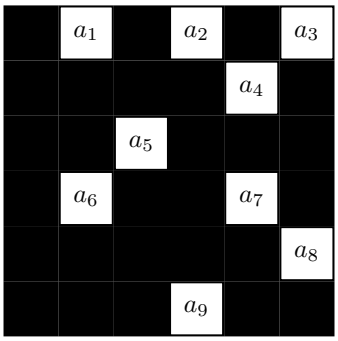
4. Drehraster-Chiffrierung

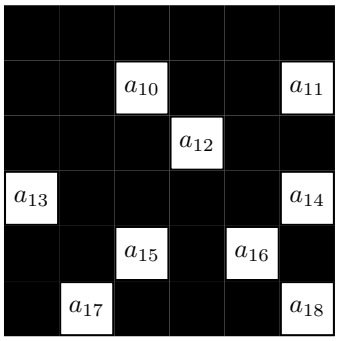
Wir stellen die Drehraster-Chiffrierung anhand einer Verschlüsselung mit einer 6×6-Chiffrierschablone vor. Als Schlüssel benutzt man eine (geeignet gewählte) Schablone mit 6×6 Feldern, die 9 Löcher hat, was in folgendem Beispiel die weißen Felder sein sollen:

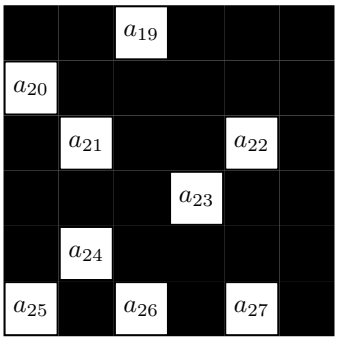


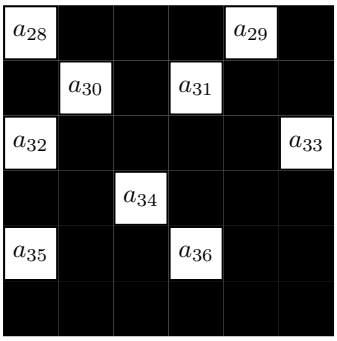
Der Ausgangstext wird in Blöcke mit jeweils 36 Zeichen aufgeteilt, wobei der letzte Block eventuell noch aufgefüllt werden muss. Um die Zeichenfolge $a_1\ a_2\ \ldots a_{36}$ zu verschlüsseln, geht man so vor: Man legt die Schablone auf ein Blatt Papier und schreibt die ersten 9 Zeichen $a_1, \ldots, a_9$ an den freien Stellen der Schablone der Reihe nach auf das Papier:



Dann dreht man die Schablone um 90 Grad im Uhrzeigersinn und schreibt die nächsten 9 Zeichen aufs Papier, und so fort, bis man 36 Zeichen eingetragen hat. Man erhält dann nacheinander:







Nimmt man jetzt die Schablone weg, so hat man

a_{28}	a_1	a_{19}	a_2	a_{29}	a_3
a_{20}	a_{30}	a_{10}	a_{31}	a_4	a_{11}
a_{32}	a_{21}	a_5	a_{12}	a_{22}	a_{33}
a_{13}	a_6	a_{34}	a_{23}	a_7	a_{14}
a_{35}	a_{24}	a_{15}	a_{36}	a_{16}	a_8
a_{25}	a_{17}	a_{26}	a_9	a_{27}	a_{18}

Schreibt man die Zeichen zeilenweise aus, so erhält man die verschlüsselte Nachricht: $a_{28}\ a_1\ a_{19} \ldots a_9\ a_{27}\ a_{18}$. (Die Schablone muss so gemacht sein, dass nach 4 Drehungen alle 36 Felder ein Zeichen enthalten.)

Beispiel: Wollen wir den Satz 'In der Erzählung Mathias Sandorf von Jules Verne wird ein Drehraster zur Verschlüsselung verwendet' mit obigem Drehraster verschlüsseln, so wandeln wir in Großbuchstaben um, lassen die Zwischenräume weg und ergänzen X, bis die Zeichenzahl durch 36 teilbar ist:

```
INDERERZAEHLUNGMATHIASSANDORFVONJULE
SVERNEWIRDEINDREHRASTERZURVERSCHLUES
SELUNGVERWENDETXXXXXXXXXXXXXXXXXXXX
```

Verschlüsselt ergibt dies dann:

```
RIHNFDIVEOEHNARLSJUEUSRNLAGEMZNADAOT
ESAVRESSDCREHTNIELNEURWDEZRSEIUHRRVR
XSXEXLXXWXUEXXNNXXDGXXVEXXTXXEXXXRXX
```

Zur Konstruktion von Schablonen: Wir numerieren die Felder einer 6×6-Schablone mit (i, j), wobei $1 \leq i, j \leq 6$ gilt. Durch Drehung geht (i, j) nacheinander in $(j, 7-i)$, $(7-i, 7-j)$, $(7-j, i)$ über. Die Felder werden dadurch in folgende 9 Bahnen zerlegt:

$$\{(1,1),(1,6),(6,6),(6,1)\}$$
$$\{(1,2),(2,6),(6,5),(5,1)\}$$
$$\{(1,3),(3,6),(6,4),(4,1)\}$$
$$\{(1,4),(4,6),(6,3),(3,1)\}$$
$$\{(1,5),(5,6),(6,2),(2,1)\}$$
$$\{(2,2),(2,5),(5,5),(5,2)\}$$
$$\{(2,3),(3,5),(5,4),(4,2)\}$$
$$\{(2,4),(4,5),(5,3),(3,2)\}$$
$$\{(3,3),(3,4),(4,4),(4,3)\}$$

Für eine gültige Schablone muss man aus jeder Bahn genau ein Element auswählen. Daher gibt es $4^9 = 2^{18} = 262144$ Schablonen.