Analyse zur Fleissner-Schablone

Inhaltsverzeichnis

Fleissner-Schablone

Was ist die Fleissner-Schablone?

- Kategorie: Transpositionsverfahren
- Entwickelt 1881 von Eduard Fleissner von Wostrowitz
- Jules Verne griff das Verfahren 1885 in seinem Roman „Mathias Sandorf“ auf.
- Die Schablone wurde im ersten Weltkrieg auf deutscher Seite genutzt.
- Das Verfahren ist mittlerweile veraltet und heute nicht mehr sicher.

Was ist die Fleissner-Schablone?

Beispiel einer 12 $\times$ 12-Schablone

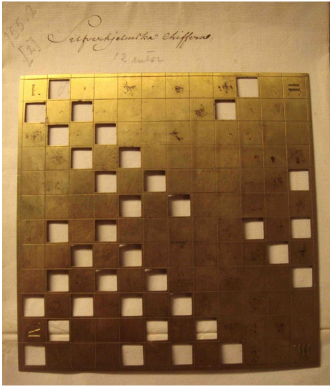

Abbildung: Quelle: http://scienceblogs.de/klausis-krypto-kolumne/2017/01/13/fleissner-challenge-can-this-cryptogram-be-broken/

Wie erstellt man eine Fleissner-Schablone?

- Eine quadratische Schablone der Seitenlänge n, die in n^2 kleinere Quadrate unterteilt wird
- Nach einem (selbst-)bestimmten Muster werden einige kleinere Quadrate ausgeschnitten
- Der Entwurf des Musters ist dabei Restriktionen ausgesetzt, da die Schablone bei ihrer Anwendung drei mal gedreht wird, und dabei keine Buchstaben übereinander geschrieben werden dürfen

Wie erstellt man eine Fleissner-Schablone?

$\Rightarrow$ Beginnend mit dem Index 0 und der Bezeichnung (Spalte, Zeile) für eine Koordinate, wobei $(0,0)$ das Feld oben links und $(3,3)$ das Feld unten rechts bezeichnet, fallen beispielsweise bei der Wahl von $(x,y) = (0,1)$ für $n = 4$ die drei Koordinaten $(n-1-y, x) = (2,0)$, $(n-1-x, n-1-y) = (3,2)$ und $(y, n-1-x) = (1,3)$ weg.

Ausgewählte Koordinate: Kreis
Blockierte Koordinaten: Grau

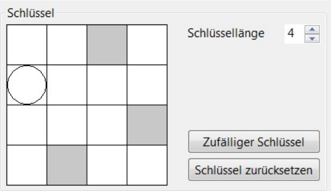

Abbildung: Quelle: JCrypTool

Wie erstellt man eine Fleissner-Schablone?

- Ein fertiges Muster kann als Abfolge von Koordinaten der ausgeschnittenen Quadrate der Form (Spalte,Zeile,Spalte,Zeile,...) beschrieben werden

Beispiel: Beginnend mit dem Index 0

Muster

$$(\underbrace{0,1}_{\text{1. Koord.}}, \underbrace{2,1}_{\text{2. Koord.}}, \underbrace{0,3}_{\text{3. Koord.}}, \underbrace{2,3}_{\text{4. Koord.}})$$

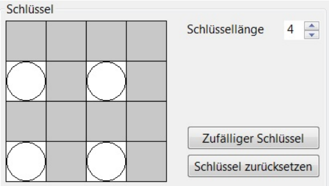

Abbildung: Quelle: JCrypTool

Wie wendet man die Schablone an?

- Die fertige Schablone wird auf ein Blatt gelegt und ausgeschnittene Quadrate von links nach rechts und von oben nach unten mit Klartextbuchstaben ausgefüllt.
- Schablone wird um 90° gedreht.
- Wiederholung dieses Vorgangs, bis die Schablone in allen Rotationspositionen ausgefüllt wurde.

Eine Verschlüsselungsrunde

Gegeben ist der Klartext „WIKIPEDIA DIE FREIE ONLINE ENZYKLOPAEDIE“. Leerzeichen zwischen Worten werden ignoriert. Hier ist $n = 6$.

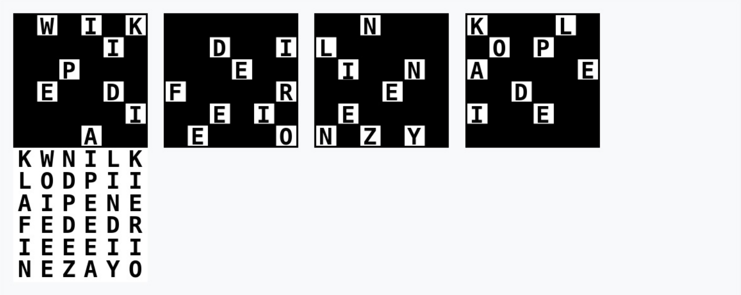

Abbildung: Quelle:
`https://de.wikipedia.org/wiki/Flei%C3%9Fnersche_Schablone`

Analyse

Idee der Analyse

- Fleissner-Schablone ist eine Transpositionschiffre
  $\Rightarrow$ Die Häufigkeit der Buchstaben bleibt unverändert.
- Jede Sprache besitzt häufige und weniger häufige Buchstabenkombinationen
- Buchstabenkombinationen verschiedener Längen N werden als „N-Gramme“ bezeichnet
- N-Gramme besitzen der Sprache entsprechende Auftrittswahrscheinlichkeiten
- Je mehr N-Gramme mit hohen Auftrittswahrscheinlichkeiten im vorliegenden Text auftauchen, desto eher liegt ein korrekter Text in der jeweiligen Sprache vor.
- In einem Analyseverfahren wird der „Wert“ des Textes durch eine Kostenfunktion bestimmt, der zuvor N-Gramme mit (log-)Wahrscheinlichkeiten übergeben wurden.

Ansatz für die Analyse

- Die Anzahl der möglichen Schablonen hängt von der Schablonengröße ab und bestimmt die Analysemethode
- Ist die Anzahl der möglichen Schablone „klein genug“, wählt man die „Brute-Force“-Methode. Dabei werden alle möglichen Schablonen (Schlüssel) durchlaufen und für jeden Durchlauf die Kostenfunktion berechnet
- Bei ansteigender Anzahl der Möglichkeiten bietet sich „Hill-Climbing“ an

Hill-Climbing (Bergsteigeralgorithmus)

- Heuristisches Optimierungsverfahren
- Verschiedene Startpunkte, so dass verschiedene Extrempunkte erreicht werden können
- Schritt-für-Schritt Verbesserungen
- Abbruch, nachdem über längere Zeit keine Verbesserung mehr erzielt wurde
  $\Rightarrow$ Bei „ausreichend“ vielen Neustarts wird der richtige Schlüssel mit hoher Wahrscheinlichkeit gefunden.

Parameter

- Schlüsselmenge (Menge unterscheidbarer, quadratischer Schablonen) Ω, wobei $|\Omega| \hat{=}$ Anzahl der Elemente von Ω,
- Schlüssel (Schablone) $S \in \Omega$,
- Länge $n \in \mathbb{N}_{\geqslant 2}$ der Schablone,
- Anzahl Löcher h (wie „holes“)

Berechnung der Parameter

Bedingungen für die Modellierung:

1. Für gerade n soll nach Anwendung der Schablone kein Feld frei bleiben, für ungerade n soll das mittlere Feld frei bleiben.
2. Mit der Wahl eines Felds dürfen die drei Felder, die durch die Drehung der Schablone angenommen werden, nicht mehr zur Wahl stehen.

Wegen (1) stehen n^2 Felder für gerade n und $n^2 - 1$ Felder für ungerade n für die Wahl von h zur Verfügung. Wegen (2) muss aber noch durch 4 geteilt werden.

$$\Rightarrow h = \begin{cases} \frac{n^2}{4}, & \text{falls } n \text{ gerade} \\ \frac{n^2-1}{4}, & \text{falls } n \text{ ungerade} \end{cases}$$

Berechnung der Parameter

Auswahl der Löcher kann wie Urnenmodell aufgebaut werden:

Es wird aus h Urnen jeweils eine aus vier möglichen Kugeln gezogen (hier: Jede Urne enthält die vier zusammengehörigen Felder, die durch Drehungen der Schablone angenommen werden).
Die Menge der Schablonen kann dann als

$$\Omega = \{\{a_{i,1}, \ldots, a_{i,h}\} \mid i \in \{1, \ldots, 4\}\}$$

beschrieben werden.
Ohne Beachtung der Reihenfolge, da jede Permutation der Elemente eines $S = \{a_{i,1}, \ldots, a_{i,h}\} \in \Omega$ die gleiche Schablone erzeugt.
Die Anzahl[1] $|\Omega|$ berechnet sich dann zu

$$|\Omega| = \binom{h}{h} \cdot 4^h = 4^h$$

[1] siehe Anhang

Anzahl der Möglichkeiten für $n \in \{2, \ldots, 12\}$

n	h	$\lvert\Omega\rvert$	Verfahren	Laufzeit[2] (in ms)
2	1	4	Brute-Force	102,4 (Erfolg 10/10)
3	2	16	Brute-Force	302,7 (Erfolg 10/10)
4	4	256	Brute-Force	4411,2 (Erfolg 10/10)
5	6	4.096	Hill-Climbing	1946,9 (Erfolg 10/10)
6	9	262.144	Hill-Climbing	2522,2 (Erfolg 10/10)
7	12	16.777.216	Hill-Climbing	3236 (Erfolg 9/10)
8	16	4.294.967.296	Hill-Climbing	4216,2 (Erfolg 9/10)
9	20	1.099.511.627.776	Hill-Climbing	5299,9 (Erfolg 7/10)
10	25	1.125.899.906.842.624	Hill-Climbing	6544,9 (Erfolg 7/10)
11	30	1.152.921.504.606.846.976	Hill-Climbing	7987,3 (Erfolg 2/10)
12	36	4.722.366.482.869.645.213.696	Hill-Climbing	9696,5 (Erfolg 4/10)

[2] Durchschnitt nach 10 Durchläufen (Durchlauf $\hat{=}$ Neustart des Analyseprogramms), Restarts (für Hill-Climbing): 50, Textlänge: 963 Zeichen (ohne Leerzeichen), Sprache: Deutsch

Anwendung

4×4-Schablone

- 4×4-Schablone
- Schablone $S = (0, 1, 2, 1, 0, 3, 2, 3)$
- Analysemethode: Brute-Force ($|\Omega| = 4^4 = 256$)

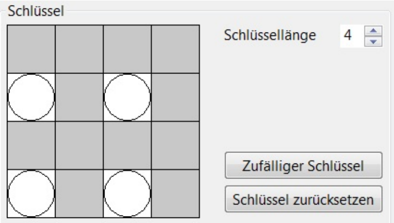

Abbildung: Quelle: JCrypTool

Analyse zur 4 × 4-Schablone

```
Aug 02, 2018 3:38:40 PM FleissnerGrilleSolver main
INFORMATION: best template: 01210323
Aug 02, 2018 3:38:40 PM FleissnerGrilleSolver main
INFORMATION:

Grille with length of template: 4 found at try: 195, in Restart: 0


Filled:
----
X-X-
----
X-X-

Aug 02, 2018 3:38:40 PM FleissnerGrilleSolver main
INFORMATION: Method: Brute-Force
Aug 02, 2018 3:38:40 PM FleissnerGrilleSolver main
INFORMATION:

Decrpyted text:

DURCHDIETEILUNGDESRÖMISCHENREICHESINWESTROMUNDOSTROMWOKONSTANTINDASALTEBYZANTIONZURNEUENHAUPTSTADT
KONSTANTINOPELAUSBAUTEENTWICKELNSICHZWEIUNTERSCHIEDLICHEKONFESSIONENDIEIHREDIFFERENZENZUEINEMNICHT
GERINGENTEILIMJEWEILIGENUMGANGMITDENBILDERNDESHEILIGENSEHENWÄHRENDDASALTEROMNACHDENSTÜRMENDER
VÖLKERWANDERUNGSZEITZUMZENTRUMDERRÖMISCHKATHOLISCHENKIRCHEAUFSTEIGTENTFALTETSICHINKONSTANTINOPELDAS
ORTHODOXECHRISTENTUMZUDENLEISTUNGENDERBYZANTINISCHENKUNSTGEHÖRTDIEENTWICKLUNGEINESMOBILENKULTBILDES
DERIKONEDIEZUEINEMZENTRALENBESTANDTEILDERORTHODOXENLITURGIEWIRDSOLITÄRODERALSBILDERWANDIKONOSTASE
STEHTSIEIMZENTRUMDERBILDERVEREHRUNGUNDBILDETVIELENEUEDARSTELLUNGSFORMENAUSIHRERFOLGRUFTALSGEGENBEWEGUNG
DENBILDERSTREITHERVORINDEMSICHDIEBEIDENGRUNDSÄTZLICHENHALTUNGENZUBILDERNFÜRDIEGESAMTEGESCHICHTEDERKUNST
EXEMPLARISCHGEGENÜBERSTEHENIKONOKLASTENUNDIKONODULENUNTERKAISERJUSTINIANENTSTEHENNEUEKULTURELLEZENTREN
AUCHIMWESTENBESONDERSRAVENNAWIRDMITBAUWERKENUNDBILDERSCHMUCKAUFGEWERTETXXXXXXXXXXXXXX
Aug 02, 2018 3:38:40 PM FleissnerGrilleSolver main
INFORMATION: Accurateness: 10188.111965461652 (where alltimelow is 10188.111965461652)
Aug 02, 2018 3:38:40 PM FleissnerGrilleSolver main
INFORMATION: Finished analysis in 2582 miliseconds
```

Abbildung: Ausgabe nach Brute-Force

5×5-Schablone

- 5×5-Schablone
- Schablone $S = (2, 0, 0, 1, 3, 1, 1, 2, 0, 3, 0, 4)$
- Analysemethode: Hill-Climbing ($|\Omega| = 4^6 = 4096$)

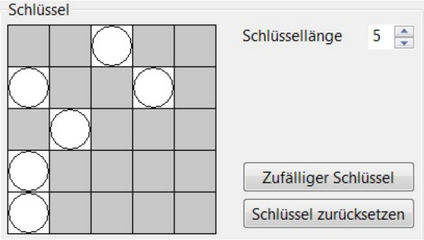

Abbildung: Quelle: JCrypTool

Analyse zu 5 × 5-Schablone

```
Aug 02, 2018 3:29:05 PM FleissnerGrilleSolver main
INFORMATION: Improvement by 1 rotation(s).
Aug 02, 2018 3:29:05 PM FleissnerGrilleSolver main
INFORMATION: best template: 200131120304
Aug 02, 2018 3:29:05 PM FleissnerGrilleSolver main
INFORMATION:

Grille with length of template: 5 found at try: 4, in Restart: 50


Filled:
--X--
X--X-
-X---
X----
X----

Aug 02, 2018 3:29:05 PM FleissnerGrilleSolver main
INFORMATION: Method: Hill-Climbing
Aug 02, 2018 3:29:05 PM FleissnerGrilleSolver main
INFORMATION:

Decrpyted text:

DURCHDIETEILUNGDESRÖMISCHENREICHESINWESTROMUNDOSTROMWOKONSTANTINDASALTEBYZANTIONZURNEUENHAUPTSTADT
KONSTANTINOPELAUSBAUTEENTWICKELNSICHZWEIUNTERSCHIEDLICHEKONFESSIONENDIEIHREDIFFERENZENZUEINEMNICHT
GERINGENTEILIMJEWEILIGENUMGANGMITDENBILDERNDESHEILIGENSEHENWÄHRENDDASALTEROMNACHDENSTÜRMENDER
VÖLKERWANDERUNGSZEITZUMZENTRUMDERRÖMISCHKATHOLISCHENKIRCHEAUFSTEIGTENTFALTETSICHINKONSTANTINOPELDAS
ORTHODOXECHRISTENTUMZUDENLEISTUNGENDERBYZANTINISCHENKUNSTGEHÖRTDIEENTWICKLUNGEINESMOBILENKULTBILDES
DERIKONEDIEZUEINEMZENTRALENBESTANDTEILDERORTHODOXENLITURGIEWIRDSOLITÄRODERALSBILDERWANDIKONOSTASE
STEHTSIEIMZENTRUMDERBILDERVEREHRUNGUNDBILDETVIELENEUEDARSTELLUNGSFORMENAUSIHRERFOLGRUFTALSGEGENBEWEGUNG
DENBILDERSTREITHERVORINDEMSICHDIEBEIDENGRUNDSÄTZLICHENHALTUNGENZUBILDERNFÜRDIEGESAMTEGESCHICHTEDERKUNST
EXEMPLARISCHGEGENÜBERSTEHENIKONOKLASTENUNDIKONODULENUNTERKAISERJUSTINIANENTSTEHENNEUEKULTURELLEZENTREN
AUCHIMWESTENBESONDERSRAVENNAWIRDMITBAUWERKENUNDBILDERSCHMUCKAUFGEWERTETXXXXXXXXXXXXXXXXXXXXXX
Aug 02, 2018 3:29:05 PM FleissnerGrilleSolver main
INFORMATION: Accurateness: 10288.744661414286 (where alltimelow is 10288.744661414286)
Aug 02, 2018 3:29:05 PM FleissnerGrilleSolver main
INFORMATION: Finished analysis in 2955 miliseconds
```

Abbildung: Ausgabe nach Hill-Climbing

8 × 8-Schablone

- 8 × 8-Schablone
- Schablone $S =$ $(1, 0, 5, 0, 2, 1, 4, 1, 6, 1, 1, 2, 7, 2, 0, 3, 3, 3, 5, 3, 1, 4, 3, 5, 5, 5, 7, 6, 0, 7, 4, 7)$
- Analysemethode:
  Hill-Climbing
  $(|\Omega| = 4^{16} > 4 \text{ Mrd.})$

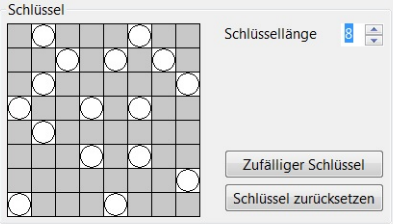

Abbildung: Quelle: JCrypTool

Analyse zu 8 × 8-Schablone

```
Aug 02, 2018 3:48:25 PM FleissnerGrilleSolver main
INFORMATION: Improvement by 3 rotation(s).
Aug 02, 2018 3:48:25 PM FleissnerGrilleSolver main
INFORMATION: best template: 10502141611272033353143555760747
Aug 02, 2018 3:48:25 PM FleissnerGrilleSolver main
INFORMATION:

Grille with length of template: 8 found at try: 7, in Restart: 50


Filled:
-X---X--
--X-X-X-
-X-----X
X--X-X--
-X------
---X-X--
-------X
X---X---

Aug 02, 2018 3:48:25 PM FleissnerGrilleSolver main
INFORMATION: Method: Hill-Climbing
Aug 02, 2018 3:48:25 PM FleissnerGrilleSolver main
INFORMATION:

Decrpyted text:

DURCHDIETEILUNGDESRÖMISCHENREICHESINWESTROMUNDOSTROMWOKONSTANTINDASALTEBYZANTIONZURNEUENHAUPTSTADT
KONSTANTINOPELAUSBAUTEENTWICKELNSICHZWEIUNTERSCHIEDLICHEKONFESSIONENDIEIHREDIFFERENZENZUEINEMNICHT
GERINGENTEILIMJEWEILIGENUMGANGMITDENBILDERNDESHEILIGENSEHENWÄHRENDDASALTEROMNACHDENSTÜRMENDER
VÖLKERWANDERUNGSZEITZUMZENTRUMDERRÖMISCHKATHOLISCHENKIRCHEAUFSTEIGTENTFALTETSICHINKONSTANTINOPELDAS
ORTHODOXECHRISTENTUMZUDENLEISTUNGENDERBYZANTINISCHENKUNSTGEHÖRTDIEENTWICKLUNGEINESMOBILENKULTBILDES
DERIKONEDIEZUEINEMZENTRALENBESTANDTEILDERORTHODOXENLITURGIEWIRDSOLITÄRODERALSBILDERWANDIKONOSTASE
STEHTSIEIMZENTRUMDERBILDERVEREHRUNGUNDBILDETVIELENEUEDARSTELLUNGSFORMENAUSIHRERFOLGRUFTALSGEGENBEWEGUNG
DENBILDERSTREITHERVORINDEMSICHDIEBEIDENGRUNDSÄTZLICHENHALTUNGENZUBILDERNFÜRDIEGESAMTEGESCHICHTEDERKUNST
EXEMPLARISCHGEGENÜBERSTEHENIKONOKLASTENUNDIKONODULENUNTERKAISERJUSTINIANENTSTEHENNEUEKULTURELLEZENTREN
AUCHIMWESTENBESONDERSRAVENNAWIRDMITBAUWERKENUNDBILDERSCHMUCKAUFGEWERTETXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Aug 02, 2018 3:48:25 PM FleissnerGrilleSolver main
INFORMATION: Accurateness: 10791.908141177457 (where alltimelow is 10791.908141177457)
Aug 02, 2018 3:48:25 PM FleissnerGrilleSolver main
INFORMATION: Finished analysis in 5207 miliseconds
```

Abbildung: Ausgabe nach Hill-Climbing

Anhang: Mathematische Modellierung zum Aufbau der Fleißner-Schablone

Anhang

Mathematische Modellierung zum Aufbau der Fleißner-Schablone

Inhaltsverzeichnis

1 Parameter

- Schlüsselmenge (Menge unterscheidbarer, quadratischer Schablonen) Ω,
- Schlüssel (Schablone) $S \in \Omega$,
- Länge $n \in \mathbb{N}_{\geqslant 2}$ der Schablone,
- Anzahl Löcher h (wie „holes“)

2 Einführung

Die ***Fleißner-Verschlüsselung*** ist eine Transpositionschiffre und vertauscht bei Anwendung die Reihenfolge der Buchstaben eines Klartextes. Als Schlüssel dient hierfür die ***Fleißner-Schablone***.

Im Folgenden werde ich einige Modellierungsansätze für die Menge der möglichen Schablonen, abhängig von den gesetzten Bedingungen, vorstellen. Ich möchte erst ein paar Ansätze für Modellierungen zu ***gültigen Schlüsseln*** angeben, wobei gültig hier heißt, dass eine Fleißner-Schablone (ein Schlüssel $S \in \Omega$), durch die ein Geheimtext erzeugt wurde, durch abermalige Anwendung (als einzige Schablone) auch wieder den eindeutigen Klartext erzeugen kann. Geht man davon aus, dass durch die Schablone nicht gefüllte Felder manuell mit Zufallsbuchstaben gefüllt werden (damit die Form der gewählten Schablone nicht offensichtlich ist) und bezeichnet man die Anzahl der zu stanzenden Löcher als h, so ist ein $S \in \Omega$ genau dann ein gültiger Schlüssel, wenn die beiden folgenden Bedingungen erfüllt sind:

1. $h \in \{1, \dots, \lfloor \frac{n^2}{4} \rfloor\}$,
2. Mit der Wahl eines Felds dürfen die drei Felder, die durch die Drehung der Schablone angenommen werden, nicht mehr zur Wahl stehen. (Im Aufbau durch Quadranten geschieht das per Definition)

Wählt man h größer, so würden bei der Anwendung der Schablone Buchstaben übereinander geschrieben (Schubfachprinzip) und der Geheimtext wäre nicht mehr korrekt dekodierbar. Dies wäre dann ein ***ungültiger Schlüssel***.

Ω entspricht dabei immer unserer Gesamtereignismenge, also der Menge aller, den jeweiligen Bedingungen entsprechenden, unterscheidbaren Fleißner-Schablonen

3 Anzahl gültiger Schlüssel

3.1 Aufbau durch einzelne Quadranten

Da auf diesem Wege nur Schablonen mit gerader Seitenlänge $n = 2k,\ \forall k \in \mathbb{N}$ erstellt werden können, hat jeder Quadrant die Größe $k \times k$ und damit k^2 Felder.

Wird die Fleißner-Schablone durch einzelne Quadranten aufgebaut, so wählt man einen der vier Quadranten des $n \times n$-großen Feldes. In diesen Quadranten werden die Ziffern $1, \dots, 4$ in h der k^2 Felder eingetragen. Die Reihenfolge darf dabei vernachlässigt werden, da jede Permutation der ausgewählten Koordinaten die gleiche Schablone bildet. Wenn die Zahlen im Quadranten nun zu einer Schablone geformt werden sollen, wird jede 1, die im Quadranten eingetragen wurde auf die gleichen Koordinaten im $(n \times n)$-Feld übertragen. Dann wird der erste Quadrant gedreht und auf den zweiten Quadranten gelegt (Die Drehung, sowie die Nummerierung der Quadranten verläuft im Uhrzeigersinn und beginnt mit dem ersten Quadranten links oben und endet mit dem vierten Quadranten links unten). Alle Felder, die die Ziffer 2 enthalten, werden dann im zweiten Quadranten auf die entsprechenden Felder eingetragen. Dieses Vorgehen wird so auch auf den dritten und vierten Quadranten angewandt. In diesem Fall haben wir im ersten Quadranten begonnen; welcher Quadrant für die Erzeugung der Schablone genutzt wird, ist aber nicht von Bedeutung, da jede mögliche (gültige) Schablone durch jeden Quadranten erzeugt werden kann. Für jedes einzelne Feld hat man vier Möglichkeiten, eine einzutragende Ziffer zu wählen.

Da die Anzahl der Löcher h hier auch kleiner als k^2 sein darf, muss außerdem die Anzahl der Möglichkeiten beachtet werden, h Felder aus k^2 Feldern zu wählen.

Nummeriert man die Felder in einem Quadranten mit $a_1, \dots, a_{k^2}$, so erhält man

$$\begin{aligned} \Omega \ &= \left\{ (a_1, \dots, a_h) \;\middle|\; a_i \in \{1, \dots, 4\}, h \in \{1, \dots, k^2\} \right\}, && \text{bzw.} \\ \Omega_h &= \{ (a_1, \dots, a_h) \mid a_i \in \{1, \dots, 4\} \}, && \text{für festes } h \end{aligned}$$

Für die Anzahl der Möglichkeiten hat man also

$$\begin{aligned} |\Omega| \ &= \sum_{i=1}^{k^2} \binom{k^2}{i} \cdot 4^h, \ \text{bzw.} \\ |\Omega_h| &= \binom{k^2}{h} \cdot 4^h, \end{aligned}$$

Für den Spezialfall $h = k^2 = \left(\frac{n}{2}\right)^2 = \frac{n^2}{4}$ hat man

$$|\Omega_h| = \binom{k^2}{k^2} \cdot 4^{\frac{n^2}{4}} = 1 \cdot 4^{\left(\frac{n^2}{4}\right)} = 4^{\left(\frac{n^2}{4}\right)}$$

Der Ansatz des Aufbaus einer Schablone durch einen Quadranten ist nur für gerade n möglich. Der allgemeine Fall wird zum Abschluss des nächsten Kapitels erläutert.

3.2 Aufbau ohne Quadranten

Wir betrachten nun das gesamte Brett mit n^2 Feldern. Im weiteren Verlauf werde ich jedes Feld auf dem $(n \times n)$-großen Brett wie einen Eintrag in einer Matrix als $a_{i,j}$ mit $i, j \in \{1, \dots, n\}$ beschreiben, wobei hier i der Spalte und j der Zeile entspricht.

Bei der Erzeugung einer Schablone ohne Quadranten muss die zweite Bedingung für einen gültigen Schlüssel manuell eingehalten werden. Dazu kann man für jedes Feld $a_{i,j}$ die zugehörigen drei Felder

$$a_{n-j+1,i}$$
$$a_{n-i+1,n-j+1}$$
$$a_{j,n-i+1}$$

berechnen, die durch Drehen der Schablone ebenfalls angenommen werden.

3.2.1 Schablonenlänge gerade, also $n = 2k,\ \forall k \in \mathbb{N}$

Die Menge aller Felder kann als paarweise disjunkte Vereinigung von vierelementigen Teilmengen dargestellt werden:

$$\{a_{i,j} \mid i,j \in \{1,\dots,n\}\} = \dot{\bigcup}_{i,j\in\{1,\dots,n\}} \{a_{i,j}, a_{n-j+1,i}, a_{n-i+1,n-j+1}, a_{j,n-i+1}\}$$

Damit ergeben sich $\frac{n^2}{4}$ verschiedene Teilmengen.

Die Modellierung kann man sich wie das bekanntere Urnenmodell vorstellen. Dabei bildet jede Teilmenge eine Urne, die vier verschiedene Felder enthält. Wenn $h \in \{1,\dots,\frac{n^2}{4}\}$ gewählt wird, muss außerdem die Anzahl der Möglichkeiten beachtet werden, h Teilmengen aus $\frac{n^2}{4}$ zu wählen. Im Urnenmodell wäre das eine zufällige Auswahl der h Urnen, aus denen gezogen werden kann.

Zur Vereinfachung der Modellierung passen wir die Indizes an das Urnenmodell an: Jedes Feld wird als $a_{i,j}$ bezeichnet, wobei i eine der vier verschiedenen Möglichkeiten in jeder Urne bezeichnet und j die Urne, aus der gezogen wurde.

Die Menge der Schablonen kann dann als

$$\begin{aligned} \Omega\ &= \left\{\{a_{i,1},\dots,a_{i,h}\} \;\middle|\; i \in \{1,\dots,4\}, h \in \{1,\dots,\tfrac{n^2}{4}\}\right\}, && \text{bzw.} \\ \Omega_h &= \{\{a_{i,1},\dots,a_{i,h}\} \mid i \in \{1,\dots,4\}\}, && \text{für festes } h \end{aligned}$$

modelliert werden.

Die Anzahl der Schablonen kann nun wie im Abschnitt 3.1 berechnet werden. Alternativ kann man sich in diesem Fall auch überlegen, dass für die Wahl des ersten Feldes n^2 Möglichkeiten bestehen (da alle Elemente unterscheidbar sind). Für das zweite Feld stehen noch $n^2 - 4$ Möglichkeiten zur Auswahl, für das dritte dann nur noch $n^2 - 2\cdot 4$, bis beim letzten Feld noch $n^2 - (h-1)\cdot 4 = n^2 - 4h + 4$ zur Wahl stehen. Die hier mitberücksichtigte Reihenfolge muss im Nenner wieder abgezogen werden.

Damit ergibt sich

$$\begin{aligned} |\Omega|\ &= \sum_{h=1}^{\frac{n^2}{4}} \prod_{k=0}^{h-1} \frac{n^2 - 4\cdot k}{k+1} = \sum_{h=1}^{\frac{n^2}{4}} \frac{n^2\cdot(n^2-4)\cdot\ldots\cdot(n^2-(h-1)\cdot 4)}{1\cdot\ldots\cdot h} \\ &= \sum_{h=1}^{\frac{n^2}{4}} 4^h \cdot \frac{\frac{n^2}{4}\cdot\left(\frac{n^2}{4}-1\right)\cdot\ldots\cdot\left(\frac{n^2}{4}-h+1\right)}{h!} = \sum_{h=1}^{\frac{n^2}{4}} 4^h \cdot \binom{\frac{n^2}{4}}{h}, && \text{bzw.} \\ |\Omega_h| &= \prod_{k=0}^{h-1} \frac{n^2-4\cdot k}{k+1} = 4^h \cdot \binom{\frac{n^2}{4}}{h}, && \text{für festes } h \end{aligned}$$

Für den Spezialfall $h = \frac{n^2}{4}$ hat man

$$|\Omega_h| = 4^{\frac{n^2}{4}} \binom{\frac{n^2}{4}}{\frac{n^2}{4}} = 4^{\left(\frac{n^2}{4}\right)} \cdot 1 = 4^{\left(\frac{n^2}{4}\right)}$$

3.2.2 Schablonenlänge ungerade, also $n = 2k+1,\ \forall k \in \mathbb{N}$

Ist n ungerade, so muss beachtet werden, dass das Feld $a_{\lceil\frac{n}{2}\rceil,\lceil\frac{n}{2}\rceil}$ leer bleiben muss, da es durch Drehungen der Schablone nicht seine Position verändert. Da nun ein Feld weniger zur Verfügung steht, hat man $h \in \{1,\dots,\frac{n^2-1}{4}\}$. Und es gilt $\frac{n^2-1}{4} \in \mathbb{N}$, da $\frac{n^2-1}{4} = \frac{(2k+1)^2-1}{4} = \frac{4k^2+4k+1-1}{4} = \underbrace{k^2+k}_{\in\mathbb{N}}$.

Die sonstige Modellierung kann wie im Fall n gerade übernommen werden. Es ist also

$$\begin{aligned} \Omega\ &= \left\{\{a_{i,1},\dots,a_{i,h}\} \;\middle|\; i \in \{1,\dots,4\}, h \in \{1,\dots,\tfrac{n^2-1}{4}\}\right\}, && \text{bzw.} \\ \Omega_h &= \{\{a_{i,1},\dots,a_{i,h}\} \mid i \in \{1,\dots,4\}\}, && \text{für festes } h \end{aligned}$$

und die Anzahl der möglichen Schablonen erhält man durch

$$\begin{aligned} |\Omega|\ &= \sum_{h=1}^{\frac{n^2-1}{4}} \prod_{k=0}^{h-1} \frac{n^2-(4\cdot k+1)}{k+1} = \sum_{h=1}^{\frac{n^2-1}{4}} \frac{(n^2-1)\cdot(n^2-5)\cdot\ldots\cdot(n^2-1-4h+4)}{1\cdot\ldots\cdot h} \\ &= \sum_{h=1}^{\frac{n^2-1}{4}} 4^h \cdot \frac{\frac{n^2-1}{4}\cdot\left(\frac{n^2-1}{4}-1\right)\cdot\ldots\cdot\left(\frac{n^2-1}{4}-h+1\right)}{h!} = \sum_{h=1}^{\frac{n^2-1}{4}} 4^h \cdot \binom{\frac{n^2-1}{4}}{h}, && \text{bzw.} \\ |\Omega_h| &= \prod_{k=0}^{h-1} \frac{n^2-(4\cdot k+1)}{k+1} = 4^h \cdot \binom{\frac{n^2-1}{4}}{h}, && \text{für festes } h \end{aligned}$$

Für den Spezialfall $h = \frac{n^2-1}{4}$ hat man

$$|\Omega_h| = 4^{\frac{n^2-1}{4}} \binom{\frac{n^2-1}{4}}{\frac{n^2-1}{4}} = 4^{\left(\frac{n^2-1}{4}\right)} \cdot 1 = 4^{\left(\frac{n^2-1}{4}\right)}$$

3.2.3 Schablonenlänge beliebig, also $n \in \mathbb{N}_{\geqslant 2}$

Die Unterscheidung der vorangegangenen Abschnitte betrifft nur die Anzahl der Felder, die ausgeschnitten werden dürfen. Diese Unterscheidung kann auch zu einer Abbildung in Abhängigkeit von n zusammengefasst werden, die jedem $n \in \mathbb{N}_{\geqslant 2}$ einen Wert $h_{\max}$ zuordnet, der die maximale Anzahl ausschneidbarer Felder bezeichnet. Man hat dann

$$h_{\max}(n) = \begin{cases} \frac{n^2}{4}, & n \text{ gerade} \\ \frac{n^2-1}{4}, & n \text{ ungerade} \end{cases}$$

Alternativ kann man $h_{\max}$ auch mit Hilfe der Gauß-Klammer beschreiben als $h_{\max} = \lfloor \frac{n^2}{4} \rfloor$. Somit gilt für alle $n \in \mathbb{N}_{\geqslant 2}$: $h \in \{1, \ldots, \lfloor \frac{n^2}{4} \rfloor\}$.

Mit den Erkenntnissen aus den vorangegangenen Abschnitten, kann man

$$\begin{aligned} \Omega &= \left\{ a_{i,1}, \ldots, a_{i,h} \,\middle|\, i \in \{1, \ldots, 4\}, h \in \{1, \ldots, \lfloor \frac{n^2}{4} \rfloor\} \right\}, && \text{bzw.} \\ \Omega_h &= \{a_{i,1}, \ldots, a_{i,h} \mid i \in \{1, \ldots, 4\}\}, && \text{für festes } h \end{aligned}$$

als Menge der möglichen Schablonen modellieren.

Für $|\Omega|$ und $|\Omega_h|$ kann die Berechnung aus Abschnitt 3.2.1 übernommen werden.

In vielen Beschreibungen zur Fleißner-Schablone [1,2,3] wird die Anzahl der zu stanzenden Löcher nicht explizit vorgegeben. Aus den verwendeten Beispiel leitet sich aber die Nutzung von $h = \lfloor \frac{n^2}{4} \rfloor$ Löchern als geeignet ab. Für alle $n \in \mathbb{N}_{\geqslant 2}$ ergibt sich die Anzahl der Schablonen dann durch

$$|\Omega_h| = 4^h = 4^{\lfloor \frac{n^2}{4} \rfloor}$$

Die Anzahl der **gültigen Schlüssel (Schablonen)** wird also als ***Permutation mit Wiederholung*** modelliert.

[1] http://kryptografie.de/kryptografie/chiffre/fleissner.htm
[2] https://de.wikipedia.org/wiki/Flei%C3%9Fnersche_Schablone
[3] https://www.kryptographiespielplatz.de/index.php?aG=6a74ce6c9e2398be3cca10d25177e00ca450a1e1

4 Menge aller Schablonen (gültige und ungültige Schlüssel)

Ist h frei wählbar (mit $h \leqslant n^2$), so liegt eine ***Kombination ohne Wiederholung*** vor. Da mit $h > \lfloor \frac{n^2}{4} \rfloor$ die Bedingungen für einen gültigen Schlüssel nicht eingehalten werden können (siehe 2), betrachtet man lediglich die verschiedenen Möglichkeiten, h Löcher aus n^2 Feldern auszuschneiden. Mit der Bezeichnung a_i, mit $i \in \{1, \ldots, n^2\}$ für die Felder erhält man

$$\Omega = \left\{ \{a_1, \ldots, a_h\} \,\middle|\, h \in \{1, \ldots, n^2\} \right\}$$

Dadurch berechnet sich die Anzahl der möglichen Schablonen durch

$$|\Omega| = \sum_{h=1}^{n^2} \binom{n^2}{h}$$

für $n \in \mathbb{N}_{\geqslant 2}$ und $h \in \{1, \ldots, n^2\}$. Die Basis 4, die in den anderen Modellen stets verwendet wurde, wird hier nicht angewandt, da der Umstand der Anwendbarkeit hier nicht berücksichtigt wird. Die Reihenfolge der Auswahl der Felder kann auch hier unberücksichtigt bleiben.