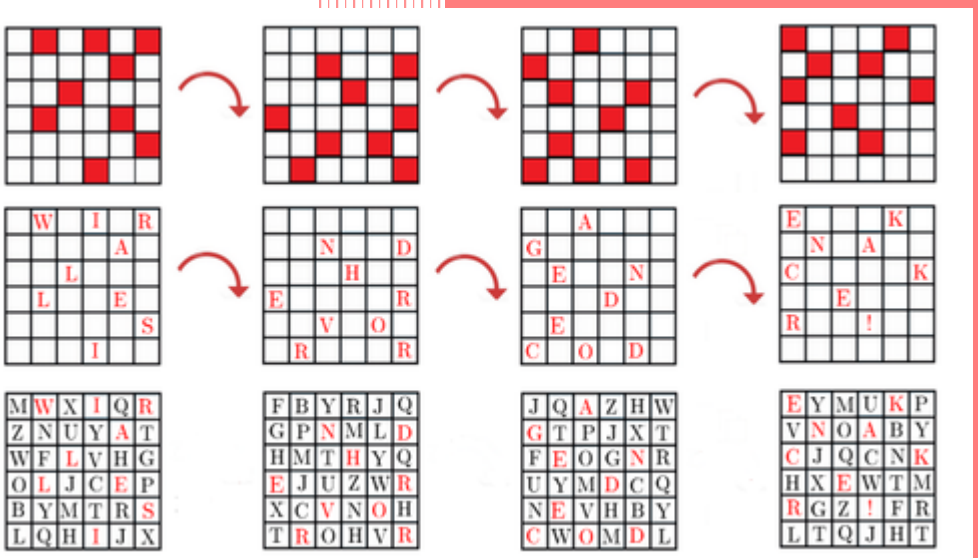
Informatik

Fleissner Schablone



https://de.wikiversity.org/wiki/Datei:Beispiel_Fleissner-Schablone.png

Hannah Keller

GymInf Fachdidaktik I

Grundlagen der Informatik für Maturitätsschulen

Prof. Dr. Juraj Hromkovic, Regula Lacher

Inhalt

Bemerkungen für die Lehrperson

Didaktische Einbettung

Die erarbeitete Lerneinheit besitzt folgende Parameter:

Adressaten	Gymnasium 9. – 10. Klasse
Fach	Informatik-Grundlagenfach (OInf)
Dauer	2 Lektionen
Vorwissen	Grundbegriffe aus der Kryptographie wie: Klar- und Geheimtext Chiffrierung und Dechiffrierung Substitutions- und Transpositionschiffrierung (analog zu den Seiten 48 – 61 aus Informatik – Data Science und Sicherheit)
	Beispiele von Geheimschriften wie: Skytale Caesar Polybios (analog zu den Seiten 48 – 61 aus Informatik – Data Science und Sicherheit)
	Grundlagen der Kombinatorik
Hilfsmittel	Fleissner Schablonen (siehe Material) Raster für Geheimtexte (siehe Material) Schere
Didaktische Ziele	Vertiefung der Grundbegriffe Kennenlernen einer weiteren Transpositionschiffrierung Eigene Auseinandersetzung mit der Fleissner Schablone Eigene Überlegungen und Erkenntnisse zur Sicherheit dieser Verschlüsselungsmethode Erkennen der Einbettung des Themas in der Informatik generell und speziell im Bereich Datensicherheit

Lektionsablauf

Abschnitt	Zeit		Details
Auftragserteilung	5′	Begrüssung	Der Auftrag und das Ziel der Lektion werden den Schüler*innen kommuniziert.
Einstiegsrätsel	10′	Erarbeitung	Material vorbereiten, Einstieg ins Thema finden
Geheimschriften: Wie funktioniert es?	0′		Lösung des Einstiegsrätsels, eingebettet im Abschnitt Einstiegsrätsel
Selbst einen Geheimtext erstellen: Wie funktioniert es?	20′		Chiffrierung und Dechiffrierung eines eigenen Geheimtexts
Die Fleissner Schablone unter der Lupe I und II	30′	Konsolidierung	Repetition der Fachbegriffe zur Kryptographie Eigene Überlegungen zur Anzahl möglicher Schablonen Eigene Überlegungen zur Sicherheit des Systems
Geheimschriften: Was steckt dahinter?	10′	Einbettung	Text lesen Reflexion Vertiefung der Thematik Datensicherheit bei der Nachrichtenübertragung
Diskussion	15′	Abschluss	Zusammentragen der zentralen Ergebnisse / kritische Diskussion im Plenum Aufgreifen von Fragen der Schüler*innen

Reflexion

Die Unterrichtssequenz ist als Leitprogramm gedacht. Die Schüler*innen haben also die Möglichkeit, den Auftrag zu zweit im eigenen Lerntempo zu erarbeiten. Alle Lernmaterialen und Lösungen befinden sich im Dossier, das den Schüler*innen zur Verfügung gestellt wird.

Interventionen der Lehrpersonen in den einzelnen Lerntandems sollten eine Selbstverständlichkeit sein. Eine gemeinsame Reflexion im Plenum bietet sich im Verlauf der Bearbeitung des Auftrages nach der Konsolidierungsphase und unbedingt als Abschluss der Unterrichtssequenz an.

Im Anschluss folgt das Material, das die Schüler*innen zur Bewältigung der Aufgabe benötigen. Hier wird bewusst auf die Weiterführung der Kopf- und Fusszeilen sowie Seitennummerierung verzichtet. So kann das Material ohne Anpassungen den Schüler*innen zur Verfügung gestellt werden.

Einstiegsrätsel

Blättern Sie erst weiter, wenn Sie das Rätsel gelöst haben – oder wenn Sie gar nicht weiterkommen.

Sie beobachten Ihre beiden Banknachbar*innen schon eine Weile beim Austausch von geheimen Botschaften. Am Schluss der Lektion bleiben bei ihnen drei Dinge auf dem Tisch liegen:

- ein Blatt mit einem Raster (siehe Material)
- eine Schablone (siehe Material)
- ein Zettel mit der Botschaft

Versuchen Sie die geheime Nachricht zu dechiffrieren!

Tipps:

- Falls Sie die Schablone noch ausschneiden müssen, schneiden Sie nicht genau den Linien entlang, sondern etwas weiter innen (sonst fällt die Schablone auseinander).
- Schliessen Sie sich zu zweit zusammen – dann haben Sie mehr Ideen.
- Kommen Sie gar nicht weiter, blättern Sie um und studieren Sie die Vorgehensweise.

Geheimschrift entziffern: Wie funktioniert es?

Die Geheimtexte, die gemäss dem Verfahren des österreichischen Oberst Eduard Fleissner von Wostrowitz aus dem 19. Jahrhundert entstanden sind, können wie folgt dechiffriert werden:

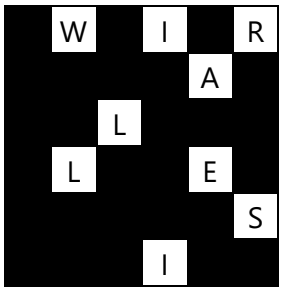
1. Den Geheimtext in ein 6x6-Gitter eintragen.
2. Eine Schablone auf das Gitter legen. Die sichtbaren Buchstaben werden von links oben nach rechts unten hintereinander notiert.
3. Die Schablone um 90 Grad nach rechts drehen und die sichtbaren Buchstaben wieder von links oben nach rechts unten hinter die bereits notierten Buchstaben schreiben.
4. Schritt 3 noch zweimal wiederholen.

Beispiel:
`E W A I K R G N N A A D C E L H N K E L E D E R R E V ! O S C R O I D R`

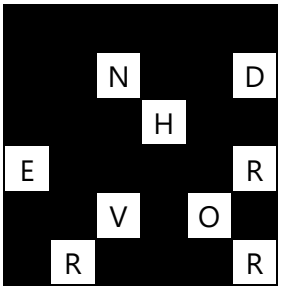
1. Geheimtext in Gitter eingetragen.

E	W	A	I	K	R
G	N	N	A	A	D
C	E	L	H	N	K
E	L	E	D	E	R
R	E	V	!	O	S
C	R	O	I	D	R

2. Schablone auf Text legen. Ersten Teil der Nachricht notieren: `WIRALLESI`



3. Schablone nach rechts drehen. Zweiten Teil der Nachricht notieren: `NDHERVORR`



4. Schritt 3 zweimal wiederholen. Dritten und vierten Teil der Nachricht notieren: `AGENDECOD` und `EKNACKER!`

So ergibt sich die Nachricht:
`WIRALLESINDHERVORRAGENDECODEKNACKER!`

bzw. `WIR ALLE SIND HERVORRAGENDE CODEKNACKER!`

Selbst einen Geheimtext erstellen: Wie funktioniert es

Chiffrieren Sie eine Nachricht, die Ihr*e Partner*in im Anschluss dechiffriert.

Falls Ihnen das Vorgehen noch nicht klar wurde, finden Sie im Folgenden eine detaillierte Beschreibung.

Aus der Nachricht entsteht der Geheimtext wie folgt:

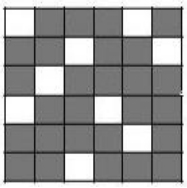
1. Denken Sie sich eine geheime Nachricht (Klartext) mit 36 Buchstaben aus. Wenn die Nachricht nicht exakt 36 Buchstaben enthält, dann füllt man sie (ihn) auf mit zufälligen Buchstaben oder Symbolen . Leerzeichen werden in der Regel weggelassen.
2. Die Schablone über leeres Gitter legen. Die ersten neun Buchstaben der Nachricht in die freien Felder schreiben. Man arbeitet von links nach rechts und von oben nach unten.
3. Schablone um 90 Grad drehen und die nächsten neun Buchstaben der Nachricht in freie Felder des Gitters schreiben.
4. Schritt 3 zweimal wiederholen, bis das ganze Gitter mit Buchstaben / Zeichen gefüllt ist.
5. Der Geheimtext entsteht, indem die Buchstaben im Gitter der Reihe nach von links oben nach rechts unten aneinandergereiht werden.

Beispiel

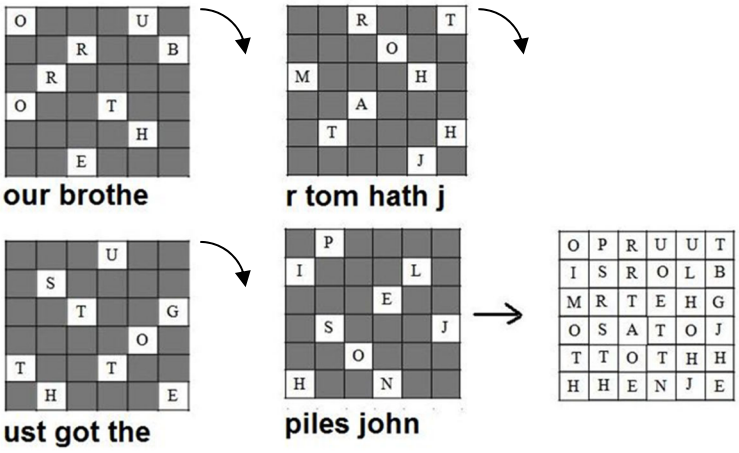
Nachricht:

OUR BROTHER TOM HATH
JUST GOT THE PILES JOHN[1]

Schablone:



Geheimtext erstellen:



Der Geheimtext lautet also:
O P R U U T I S R O L B M R T E H G O S A T O J T T O T H H H H E N J E

[1] Aus Jonathan Swifts Gulliver's Travels

Die Fleissner Schablone unter der Lupe I

Beantworten Sie folgende Fragen zur Repetition der bereits bearbeiteten Lerninhalte:

Beschreiben Sie in eigenen Worten in Bezug auf die Fleissner Schablone den Klartext, Geheimtext, das Chiffrierungs- und Dechiffrierungsverfahren.

Gehört die Fleissner Schablone in eine der Kategorien Transpositions- oder Substitutionschiffren? Falls ja, wieso? Halten Sie Ihre Erkenntnisse fest.

Das Vorgehen zur Chiffrierung und Dechiffrierung wurde bis jetzt sehr starr gehalten, im Sinne von Übertrag des Texts in das Raster, fixer 1. Position der Schablone, Drehrichtung, …

Überlegen Sie und halten Sie Alternativen fest, wie man mit der Fleissner Schablone ebenfalls Texte chiffrieren könnte.

Die Fleissner Schablone unter der Lupe II

Bis jetzt haben Sie die vorgegebene Schablone verwendet. Sie machen sich im weiteren Verlauf Gedanken dazu, wie viele Schablonen tatsächlich möglich sind. Dazu werden Sie mit einer kleineren Schablone (siehe Material) einige Experimente durchführen.

Schneiden Sie zuerst alle sechs 4x4-Raster aus (noch ohne Aussparungen).

Überlegen Sie sich eine Nachricht mit maximal 16 Buchstaben, die Sie chiffrieren wollen.

_____

Tipp:

Fällt Ihnen keine Nachricht ein, können Sie auch folgenden Text verwenden:

G A R N I C H T S O S C H W E R

Erstellen Sie nun aus einem der ausgeschnittenen Raster eine Fleissner Schablone, indem Sie 4 Felder ausschneiden. Denken Sie daran, schneiden Sie nicht genau den Linien entlang, sondern etwas zum Inneren versetzt (sonst kann die Schablone auseinanderfallen).

Chiffrieren Sie Ihren Text mit Ihrer erstellten Schablone mithilfe eines zweiten Rasters.

Hat Ihre Schablone funktioniert?
Falls ja, was denken Sie, haben Sie richtig gemacht?
Falls die Schablone nicht funktioniert hat, was könnte das Problem sein?

_____

_____

Wiederholen Sie die letzten beiden Aufträge noch zweimal mit den anderen ausgeschnittenen 4x4-Rastern (jeweils eines für die Schablone und eines für die Chiffrierung). Berücksichtigen Sie unbedingt Ihre Erkenntnisse aus dem ersten Versuch.

Haben Ihre Schablonen funktioniert?
Haben Sie ein Vorgehen entwickelt?

_____

_____

Überlegen Sie und halten Sie in diesem Setting (4x4-Raster mit vier Aussparungen) fest, wie viele Schablonen möglich sind. Nutzen Sie dazu Ihre Erkenntnisse aus den Aufträgen auf der vorherigen Seite.

Tipp: Vielleicht hilft Ihnen das folgende Raster weiter:

1	2	3	1
3	4	4	2
2	4	4	3
1	3	2	1

Übertragen Sie nun Ihre Überlegungen zum 4x4-Raster auf das alte Setting (6x6-Raster mit neun Aussparungen) und halten Sie fest, wie viele Schablonen möglich sind.

Tipp:

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Nicht alle möglichen Schablonen sind auch sinnvoll. Überlegen Sie und halten Sie fest, wieso bestimmte Schablonen nicht sinnvoll sind.

_____

_____

_____

_____

Überlegen Sie und halten Sie fest, ob dieses Verfahren in der heutigen Zeit noch sicher ist.

_____

_____

Geheimschriften: Was steckt dahinter?

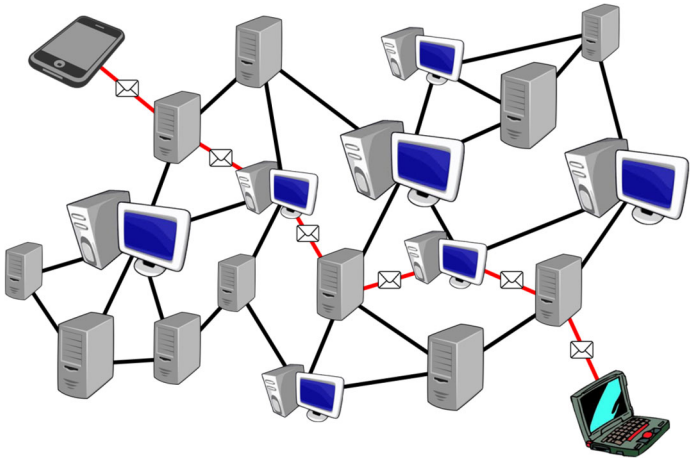
Lesen Sie zum Schluss den Text auf der nächsten Seite und nehmen Sie Stellung zu folgenden Aussagen.

Wieso ist es heute wichtig, unsere Daten verschlüsselt zu versenden?

Was ist der Unterschied zwischen modernen Verschlüsselungsverfahren und der Fleissner Schablone?

Ihre Erkenntnisse:

Täglich verschicken und empfangen Sie über Ihren Computer, Laptop, Ihr Tablet oder Smartphone Unmengen von Daten. Möglich macht dies eine Erfindung, deren Ursprünge bis in die 1970er Jahre zurückreichen: das Internet. Über das Internet sind viele Millionen Geräte in einem Netzwerk miteinander verbunden und können miteinander kommunizieren.



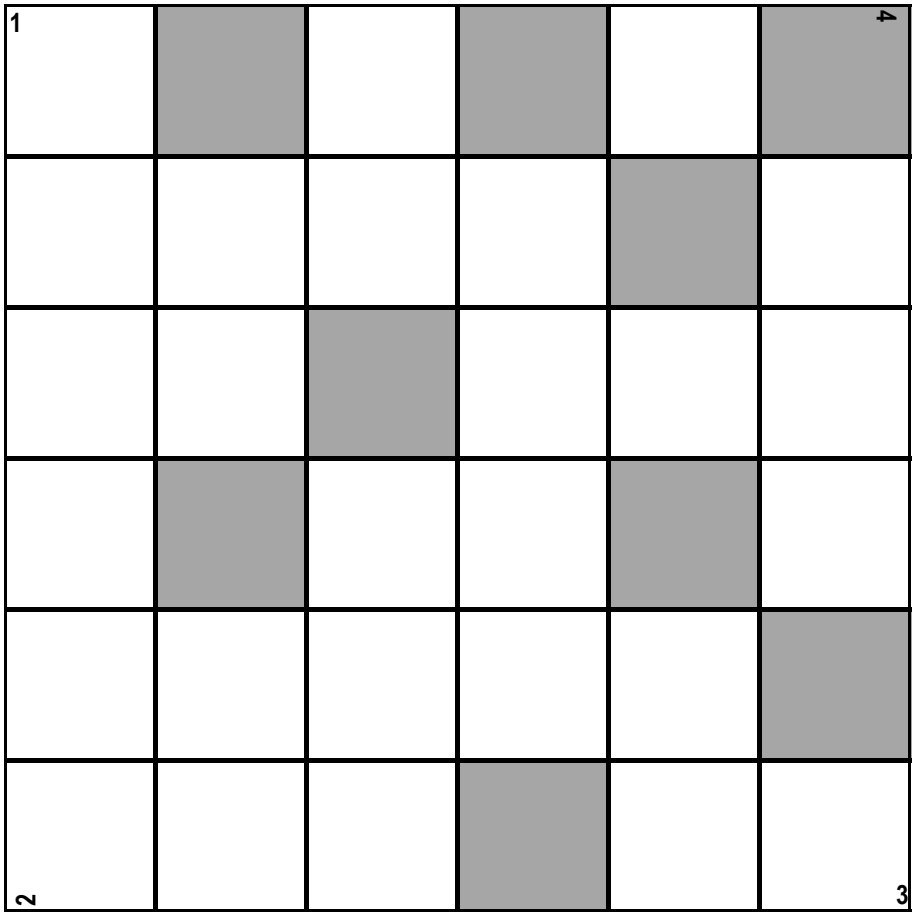
Das Internet ermöglicht die Kommunikation. Es stellt aber nicht sicher, dass niemand mitlesen kann. Soll niemand mitlesen können, so muss man selbst sicherstellen, dass die verschickte Nachricht verschlüsselt wird. Verschlüsseln bedeutet die Nachrichten so zu verändern, dass sich ihre Bedeutung nur den gewünschten Personen erschliesst.

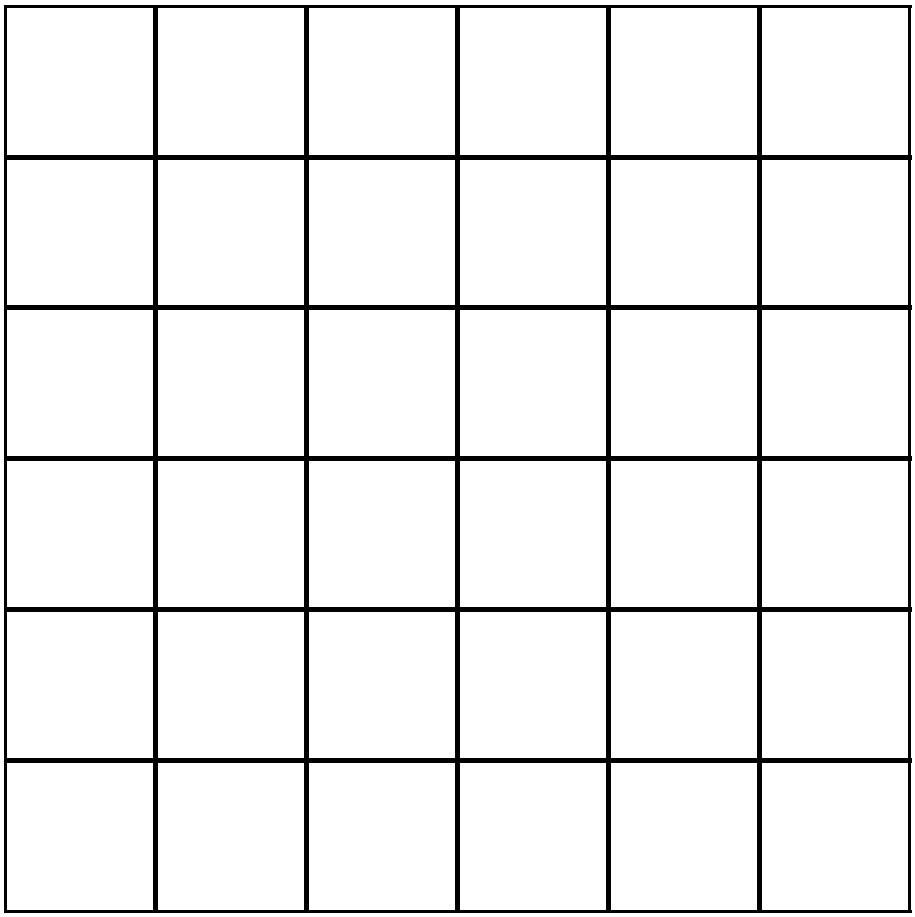
Das hier verwendete Verschlüsselungsverfahren nennt sich Fleissner Schablone. Es ist nach dem österreichischen Oberst Eduard Fleissner von Wostrowitz benannt, der dieses 1881 veröffentlichte. Bei diesem Verfahren wird die ursprüngliche Nachricht verschleiert, indem die Buchstaben scheinbar beliebig vermischt werden. Je nachdem, welche Schablone man verwendet, wird eine Nachricht unterschiedlich verschlüsselt. Die Schablone ist bei diesem Verfahren daher der sogenannte Schlüssel. Der Sender braucht den Schlüssel für das Verschlüsseln der Nachricht, der Empfänger für das Entschlüsseln.

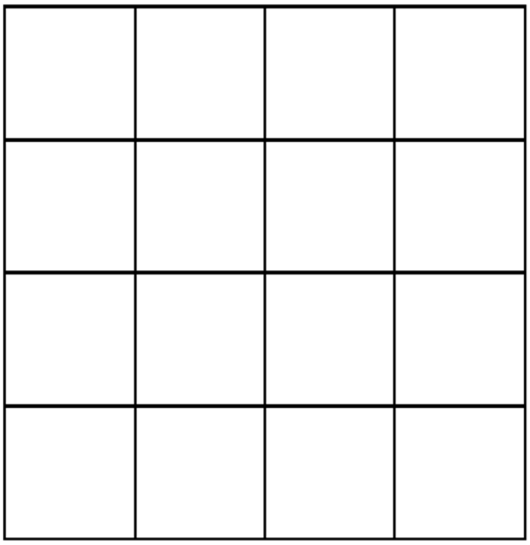
Mit der Fleissner Schablone verschlüsselte Nachrichten lassen sich heute auch ohne Schlüssel mit einem einfachen Smartphone in Sekundenbruchteilen entschlüsseln. Das Verfahren eignet sich also nicht für die Verschlüsselung der Kommunikation über das Internet. Verschlüsselungsverfahren, die heute im Einsatz sind, sind deutlich komplizierter. Sie arbeiten im Grundsatz aber sehr ähnlich wie die Fleissner Schablone. Sie arbeiten auch mit einem Schlüssel. Und sie verändern die Nachricht ebenfalls, indem sie die einzelnen Zeichen der Nachricht durchmischen.

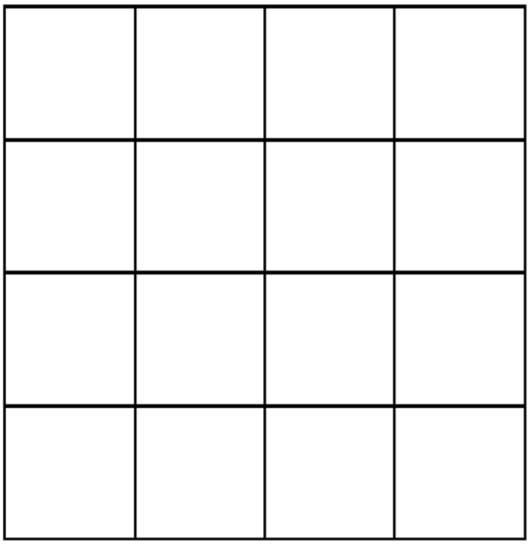
Was moderne Verfahren zudem machen, ist, einzelne Zeichen der Nachricht mit anderen Zeichen zu ersetzen. Das Vermischen und Ersetzen der Zeichen wird dabei mehrfach wiederholt. Die verwendeten Schlüssel sind riesig. Würde man sie mit deutschen Textzeichen darstellen, würden sie aus mindestens 2^{127} (= $4.2 \cdot 10^{37}$, was einer Zahl mit 37 Ziffern entspricht!) Textzeichen bestehen.

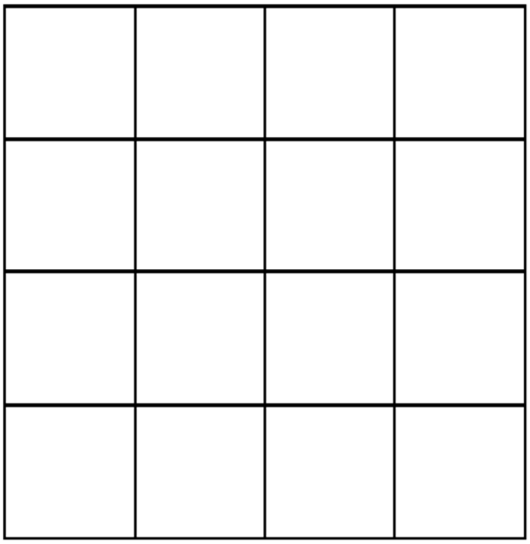
Material

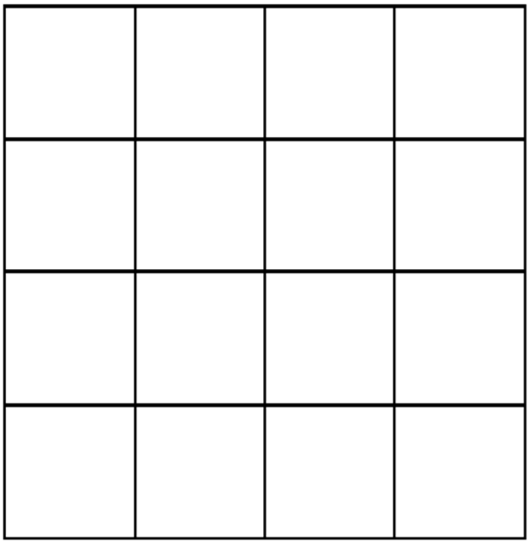


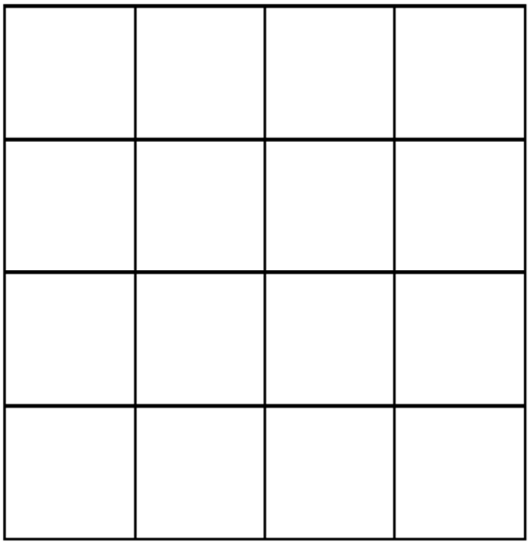


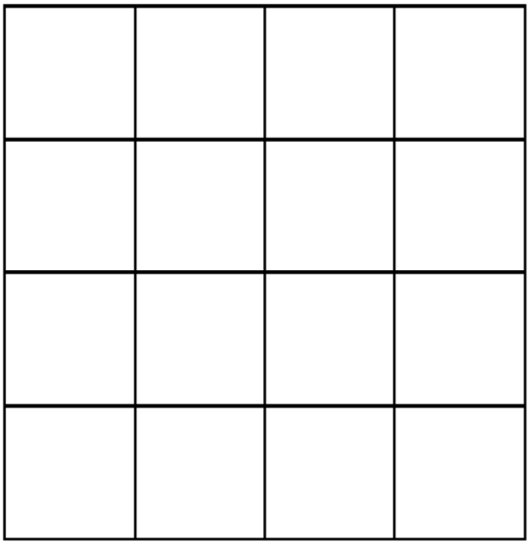












Lösungen zur Fleissner Schablone unter der Lupe I

Beschreiben Sie in eigenen Worten in Bezug auf die Fleissner Schablone den Klartext, Geheimtext, das Chiffrierungs- und Dechiffrierungsverfahren.

Klartext	der zu chiffrierende Text
Geheimtext	der chiffrierte Text
Chiffrierungsverfahren	Klartext in das Raster von oben links nach unten rechts eintragen, Schablone darauflegen, sichtbare Buchstaben von oben links nach unten rechts übertragen, Schablone nach rechts drehen und Schritte wiederholen
Dechiffrierungsverfahren	analoges Vorgehen

Gehört die Fleissner Schablone in eine der Kategorien Transpositions- oder Substitutionschiffren? Falls ja, wieso? Halten Sie Ihre Erkenntnisse fest.

Es handelt sich um eine Transpositionschiffre, da die Buchstaben nicht verändert werden, sondern nur neu angeordnet werden.

Überlegen Sie und halten Sie Alternativen fest, wie man mit der Fleissner Schablone ebenfalls Texte chiffrieren könnte.

- Den Klartext nicht von links oben nach rechts unten eintragen, sondern z. B. spaltenweise, rückwärts, … oder in einer anderen (mit dem*der Empfänger*in abgesprochenen) Art.
- Schablone nicht mit Position 1 als Startposition hinlegen, sondern mit einer anderen Position.
- Schablone nicht nach rechts drehen, sondern nach links.
- Geheimtext nicht von links oben nach rechts unten aus dem Raster übertragen.

Lösungen zur Fleissner Schablone unter der Lupe II

Überlegen Sie und halten Sie in diesem Setting (4x4-Raster mit vier Aussparungen) fest, wie viele Schablonen möglich sind. Nutzen Sie dazu Ihre Erkenntnisse aus den Aufträgen auf der vorherigen Seite.

Bedingungen für die Erzeugung einer möglichen Fleissner Schablone sind[2]:

- Die Anzahl der gesamten Felder ist durch 4 teilbar (die Schablone wird viermal aufgelegt).
- Ein Viertel der Felder wird ausgeschnitten.
- Keine Symmetrie (gemeinsame Schablonenfelder) besteht innerhalb der ausgeschnittenen Felder bei einer Drehung um 90 Grad.

[2] https://de.wikipedia.org/wiki/Fleissnersche_Schablone, aufgerufen am 14.10.2022

Das heisst zum Beispiel, dass wenn das erste Feld in der ersten Zeile ausgeschnitten wird, dürfen keine weiteren «Ecken» ausgespart werden, ansonsten werden im Raster nicht alle Felder mit Buchstaben befüllt und andere Felder würden mit mehreren Buchstaben befüllt werden.

Wenn man sich das Raster aus der Aufgabenstellung zu Hilfe nimmt, kommt man zu dem Schluss, dass man jede Zahl von 1 bis 4 nur genau einmal ausschneiden darf. Für jede Zahl hat man also 4 Möglichkeiten, dies ergibt insgesamt $4^4 = 256$ Möglichkeiten.

Übertragen Sie nun Ihre Überlegungen zum 4x4-Raster auf das alte Setting (6x6-Raster mit neun Aussparungen) und halten Sie fest, wie viele Schablonen möglich sind.

Wenn man sich das Raster aus der Aufgabenstellung zu Hilfe nimmt, kommt man zu dem Schluss, dass man jede Zahl von 1 bis 9 nur genau einmal ausschneiden darf. Für jede Zahl hat man also 4 Möglichkeiten, dies ergibt insgesamt $9^4 = 262'144$ Möglichkeiten.

Nicht alle möglichen Schablonen sind auch sinnvoll. Überlegen Sie und halten Sie fest, wieso bestimmte Schablonen nicht sinnvoll sind.

Zum Schluss kann man sich noch überlegen, dass wenn Felder nebeneinander ausgeschnitten werden, dies die Dechiffrierung einfacher gestaltet. Deswegen ist es wünschenswert, dass die Aussparungen möglichst gleichverteilt auf die 4 Quadranten ist, das ergibt dann $4 \cdot \binom{9}{3}\binom{6}{2}\binom{4}{2}\binom{2}{2} = 30'240$.

Überlegen Sie und halten Sie fest, ob dieses Verfahren in der heutigen Zeit noch sicher ist.

Die Anzahl möglicher Schablonen ist gering (im Vergleich zur Rechenleistung heutiger Computer), deswegen ist das Verfahren nicht mehr sicher.

Lösungen zu Geheimschriften: Was steckt dahinter?

Wieso ist es heute wichtig, unsere Daten verschlüsselt zu versenden?

Wir übermitteln via Internet heute täglich Daten, die nur für den*die Empfänger*in bestimmt sind. Dazu müssen wir unsere Daten verschlüsselt verschicken.

Was ist der Unterschied zwischen modernen Verschlüsselungsverfahren und der Fleissner Schablone?

Moderne Verschlüsselungsverfahren verwenden eine Mischung aus Transpositions- und Substitutionsmethoden. Zudem sind die Schlüssel viel grösser.