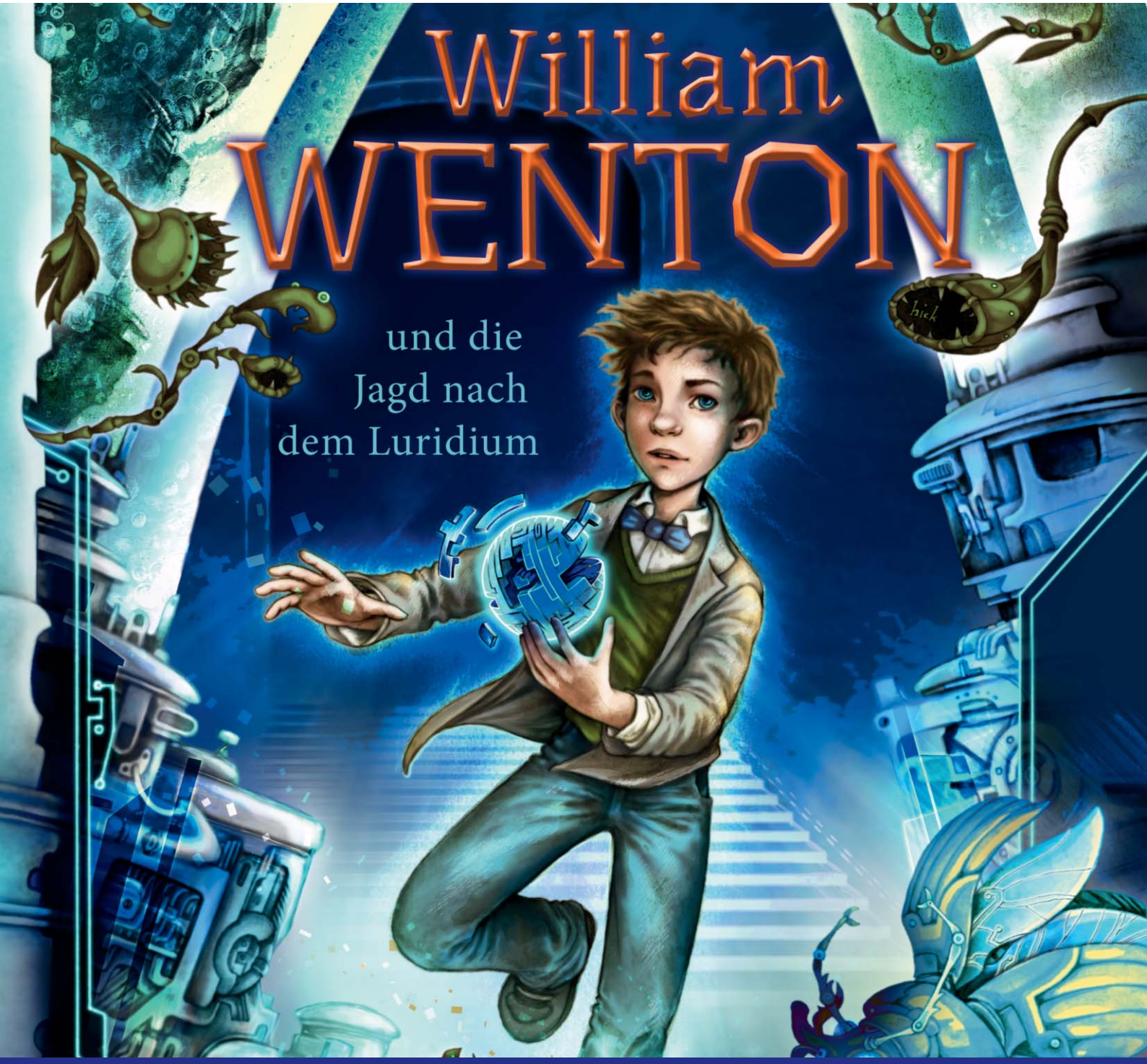
Stiftung **Lesen**



Codeknacker gesucht!
Die Kunst der Kryptologie

Ideen für den Unterricht für die Klassenstufen 5 bis 8

MIT GROSSEM WETTBEWERB
EINSENDESCHLUSS: 12. MAI 2017

in Kooperation mit CARLSEN

Wir alle haben Geheimnisse. Manchmal muss eine Notlüge herhalten, um ein Geheimnis zu bewahren. In anderen Situationen ist ein Code die bessere Wahl, um eine Nachricht vor Dritten geheim zu halten. Kryptologie (griech. *kryptós*: versteckt, verborgen, geheim) ist die Wissenschaft, die sich mit der Verschlüsselung und Entschlüsselung von Informationen befasst.

Schon seit dem **Altertum** verschlüsseln Menschen Botschaften, um sie vor unerwünschtem Zugriff zu schützen. Dazu nutzten sie zunächst Schreibwerkzeuge oder Buchstabenscheiben. Um 1920 begann das Zeitalter der Verschlüsselungsmaschinen – raffinierte Geräte, von Ingenieuren entwickelt. Die Computer lösten die mechanischen Geräte um **1970** ab.

Das Zeitalter der Computer-Verschlüsselung dauert bis heute an und hat ungeahnte Möglichkeiten eröffnet. Fragen der Informationssicherheit sind hochaktuell und haben Auswirkungen auf unsere alltägliche Kommunikation.

Geheimschriften zu entwickeln und zu entziffern begeistert Kinder und Jugendliche. Die Freude am Lesen zu fördern, das Interesse am Medium Schrift in allen Facetten zu wecken, gelingt über die Beschäftigung mit diesem faszinierenden Thema, das Jungen wie Mädchen gleichermaßen anspricht.

Lösungen zu allen Rätseln gibt es unter www.derlerlehrerclub.de/codeknacker

Faszination verspricht auch das Jugendbuch „William Wenton und die Jagd nach dem Luridium“ von Bobbie Peers (im Folgenden nur noch „William Wenton“ genannt) aus dem Carlsen Verlag – ein spannender Science-Fiction-Roman über den weltbesten Codeknacker und sein rätselhaftes Verschwinden. Das Buch bietet einen guten Einstieg in die Beschäftigung mit dem Thema Kryptologie.

Wir stellen Ihnen dazu in Kooperation mit dem Carlsen Verlag Unterrichtsimpulse **für die Klassen 5 bis 8** zur Verfügung. Unser Fachautor Klaus Schmeh, einer der weltweit führenden Experten für Kryptologie, stellt unterschiedliche Verschlüsselungsmethoden sowie ungelöste Rätsel vor und gibt Tipps zur Entschlüsselung. Die Rätsel laden die Schülerinnen und Schüler ein, ihre Entschlüsselungskunst zu trainieren; die Aufgaben führen mehr in die Tiefe.

Die Arbeitsblätter 9, 10 und 13 sind eher für ältere Schülerinnen und Schüler ab Klasse 7 geeignet und können in den Fachunterricht Geschichte sowie Mathematik eingebunden werden. Die Ansprache in den Impulsen richtet sich direkt an die Schülerinnen und Schüler, sodass Sie die Rätsel und Aufgaben als Kopiervorlage verwenden können.

Eine inhaltliche Zusammenfassung des Titels „William Wenton und die Jagd nach dem Luridium“ finden Sie auf der rechten Seite. Im Material gibt es allerlei Bezüge zum Buch in Form von Zitaten. Weitere Lese- und Linktipps finden Sie auf den Seiten 15 und 16.

INHALTSVERZEICHNIS

William Wenton und Glossar	**3**
Historische Verschlüsselungsverfahren	**4**
Wie man eine Geheimschrift knackt	**10**
Ungelöste Rätsel	**12**
Moderne Verschlüsselungsverfahren	**14**
Impulse für den Unterricht	**15**
Lese- und Medientipps	**16**

IMPRESSUM

Herausgeber und Verleger:
Stiftung Lesen, Römerwall 40, 55131 Mainz, www.stiftunglesen.de
Verantwortlich: Dr. Jörg F. Maas
Programme: Sabine Uehlein
Fachautor: Klaus Schmeh, Kryptologe
Fachliche Beratung: Anne-Marie Ensgraber, Oberstudienrätin
Redaktion: Petra Petzhold, Silke Schuster
Gestaltung: Harald Walitzek, Plugin Design, Undenheim;
Irrtümer und Preisänderungen vorbehalten.

WILLIAM WENTON UND DIE JAGD NACH DEM LURIDIUM

von Bobbie Peers, übersetzt von Gabriele Haefs

Niemand kann Rätsel besser lösen als William Wenton! Seit er sich jedoch unter dem Namen William Olsen mit seinen Eltern in Norwegen verstecken muss, ist er gezwungen, diese Fähigkeit geheim zu halten. Eines Tages erfährt er durch einen Zeitungsartikel von einer Ausstellung, die einen angeblich unlösbaren Code präsentiert.

Tatsächlich gelingt es William den Code zu knacken. Doch nun ist es vorbei mit dem Verstecken: Er wird von geheimnisvollen Fremden ans Institut für Posthumane Forschung entführt. Hier erfährt er, dass er zu den sogenannten „Kandidaten" gehört, deren Aufgabe es ist, die Welt vor dem gefährlichen Luridium zu schützen. Dabei soll ihm ein Orbis helfen, eine Art fliegende Kugel, deren Form und Größe sich ständig verändert. Doch William hat scheinbar übermächtige Gegner und ein Wettlauf gegen die Zeit beginnt.

Die Leseprobe des Carlsen Verlags vermittelt Ihnen einen ersten Eindruck der Geschichte:
www.derlehrerclub.de/codeknacker

GLOSSAR

CODE
Das Wort „Code" wird oft anstelle von „Verschlüsselung" verwendet. Im engeren Sinne versteht man darunter eine Verschlüsselung, bei der jedes Wort eines Texts durch ein Codewort (dies kann auch eine Zahl sein) aus einem Codebuch verwendet wird.

DECHIFFRIEREN
Das Entschlüsseln von Geheimtexten.

ENIGMA
Verschlüsselungsmaschine, die im Zweiten Weltkrieg von den Deutschen genutzt wurde. Die Enigma ähnelt äußerlich einer Schreibmaschine.

GEHEIMSCHRIFT
Eine Geheimschrift entsteht, wenn man statt dem üblichen Alphabet (ABCDE…) andere Zeichen verwendet. Zum Beispiel A=#, B=§, C=%, D=$, E=+, F=@, …
Sie zählt zur einfachsten Form der Verschlüsselung.

KLARTEXT
Text, der zu verschlüsseln ist.

KRYPTOGRAMM
Geheimtext zum Entschlüsseln / Dechiffrieren.

KRYPTOLOGIE
Die Kryptologie ist die Lehre vom Verschlüsseln.

STEGANOGRAFIE
So bezeichnet man das Verstecken von Informationen, beispielsweise in einem Bild oder in einem Text.

VERSCHLÜSSELUNG
Damit bezeichnet man alle Methoden, die dazu dienen, eine Botschaft unlesbar zu machen, ohne sie jedoch zu verstecken. Auch Chiffrierung genannt.

„Bald hatten sie den Deckel durch die ganze Symbolreihe hin und her gedreht. Nur ein Zeichen war noch übrig. Sie drehten den Deckel das letzte Stück. ‚Klick', machte er und der Deckel ging auf." (William Wenton, Buch Seite 198)

HISTORISCHE VERSCHLÜSSELUNGS-VERFAHREN

PIGPEN-GEHEIMSCHRIFT

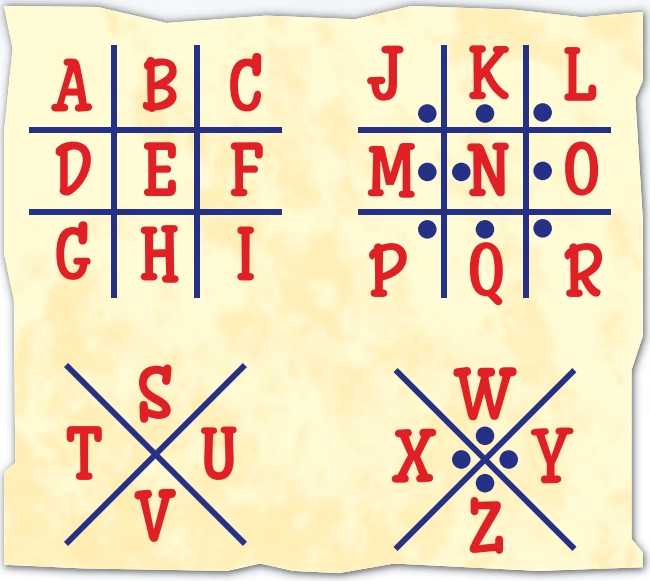


Foto: © Klaus Schmeh

Die Pigpen-Geheimschrift, auch Schweineschrift genannt, ist eine der ältesten und bekanntesten Geheimschriften. Sie ist mindestens 500 Jahre alt. Es gibt sie in unterschiedlichen Varianten. Postkarten, Grabinschriften, Urkunden und viele andere Dinge wurden mit der Pigpen-Geheimschrift beschrieben. Der Geheimbund der Freimaurer nutzte sie ebenfalls.

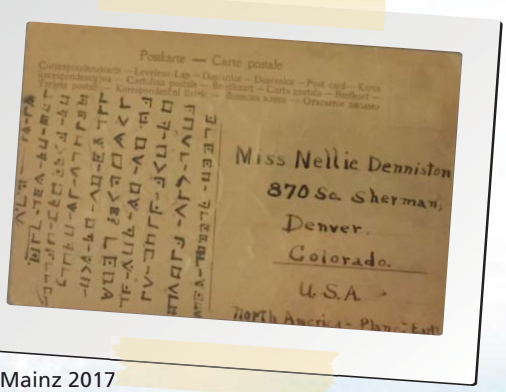
Bei dieser Geheimschrift ist die Position eines Buchstabens in einem der vier Raster von Bedeutung. Der jeweilige Buchstabe wird durch ein Symbol ersetzt.

RÄTSEL

Entschlüssle das folgende Wort mithilfe der Pigpen-Methode. Schreibe das Wort in Klarschrift darunter. Wirf mal einen Blick in die Leseprobe „William Wenton". Auf welcher Seite findest du dort das Wort?

RÄTSEL

Entschlüssle die folgende Botschaft und schreibe den Text in Klarschrift darunter.



AUFGABE

Verfasse einen Postkartentext in Geheimschrift an Bobbie Peers, den Autor von „William Wenton", und verschlüssle den Text. Zum Beispiel: „Die Leseprobe fand ich … Es würde mich interessieren, wie es weitergeht."

„Die Zeichen lösten sich vom Zylinder.
Sie schwebten um Williams Kopf wie Schmetterlinge."
(William Wenton, Buch Seite 31)

DIE SKYTALE

Die Skytale ist ein Verschlüsselungswerkzeug, das bereits den alten Griechen bekannt war. Eine Skytale ist ein rundes Stück Holz, um das der Absender einen Lederstreifen wickelte, um den Klartext draufzuschreiben. Heute würde man stattdessen wohl einen Papierstreifen verwenden. Der Empfänger benötigte einen Stab gleichen Durchmessers. Um diesen wickelte er den Streifen und konnte dann die Botschaft lesen. Nach heutigen Maßstäben ist die Skytale nicht besonders sicher – wer ein paar Stäbe unterschiedlicher Dicke durchprobiert, wird früher oder später die richtige Lösung finden.

Foto: © Klaus Schmeh

MORSEALPHABET

Schon lange bevor das Telefon, das Internet oder Sprechfunkgeräte aufkamen, konnte man einfache Signale, wie zum Beispiel Stromstöße, über größere Entfernungen übermitteln. Der US-Amerikaner Samuel Morse entwickelte um 1840 einen Code, mit dem man jeden Buchstaben des Alphabets mit Hilfe von kurzen (Punkt) und langen Signalen (Strich) übermitteln konnte: das Morsealphabet.

A ·−	J ·−−−	S ···
B −···	K −·−	T −
C −·−·	L ·−··	U ··−
D −··	M −−	V ···−
E ·	N −·	W ·−−
F ··−·	O −−−	X −··−
G −−·	P ·−−·	Y −·−−
H ····	Q −−·−	Z −−··
I ··	R ·−·	

Geübte Morsefunker schaffen es, über 100 Buchstaben pro Minute zu übertragen. Die bekannteste Morsenachricht ist SOS: kurz, kurz, kurz, lang, lang, lang, kurz, kurz, kurz. Diese Nachricht steht seit Anfang des 20. Jahrhunderts für einen Notruf. Die Buchstaben SOS wurden gewählt, weil die zugehörigen Morsezeichen selbst für Laien leicht erkennbar sind und weil auch ein ungeübter Funker sie übermitteln kann. Die Buchstaben an sich hatten ursprünglich keine Bedeutung. Heute legt man sie oft als Abkürzung von „Save our souls" („Rettet unsere Seelen") oder „Save our ship" („Rettet unser Schiff") aus.

Das Morsealphabet wurde manchmal auch als Verschlüsselungsverfahren eingesetzt – zum Beispiel auf Postkarten. Besonders sicher war das zwar nicht, doch immerhin konnte man auf diese Weise den Postboten am Mitlesen hindern, sofern dieser das Morsealphabet nicht beherrschte.

RÄTSEL

Versuche, die folgende Morsebotschaft zu entschlüsseln:

−·· ·− ··· ·· ··· − ··· − ·−· ·· −·− − −−· · ···· · ·· −−

CÄSAR-VERSCHLÜSSELUNG

Um eine Botschaft zu verschlüsseln, benötigst du keine besonderen Zeichen. Stattdessen kannst du auch Buchstaben durch Buchstaben ersetzen. Eine Methode dazu ist die Cäsar-Verschlüsselung. Dabei wird jeder Buchstabe im Alphabet verschoben. Die folgende Tabelle verschiebt beispielsweise jeden Buchstaben um zwei Positionen (A auf C, B auf D usw.):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Das Wort **ORBIS** verschlüsselt sich auf diese Weise in **QTDKU**. William verwendet eine magische fliegende Kugel, Orbis genannt, deren Form und Größe sich ständig verändert.

AUFGABE

Die Cäsar-Verschlüsselung lässt sich besonders einfach ausführen, wenn du dir eine Chiffrierscheibe bastelst. Eine große Vorlage findest du unter www.derlehrerclub.de/codeknacker. Schneide dazu die beiden Kreise aus, stanze bei beiden ein Loch in die Mitte und klammere sie so zusammen, dass du die Scheiben drehen kannst.

RÄTSEL

Kannst du das folgende Rätsel nach der Cäsar-Methode entschlüsseln? Die Chiffrierscheibe hilft dir dabei.

OB RKDDO CY FSOV KEC NSOCOX LEOMROBX QOVOBXD. NSXQO, FYX NOXOX SX NOB CMREVO XSO NSO BONO GKB.

FLEISSNER-VERSCHLÜSSELUNG

Die Fleissner-Verschlüsselung ist etwas trickreicher. Du brauchst dafür eine Schablone.

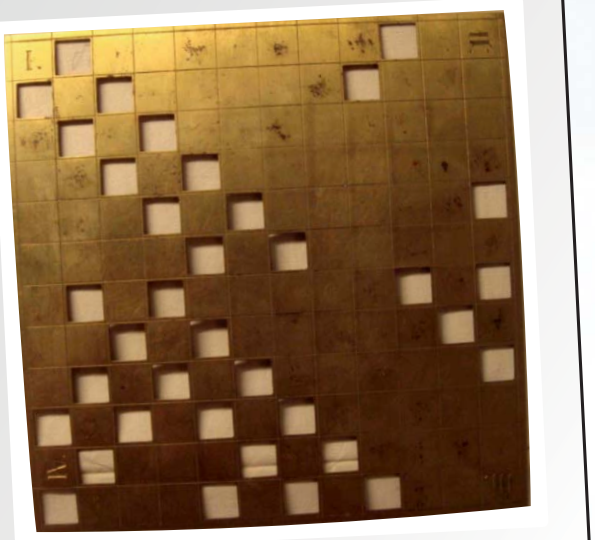


Foto: © Andreas Önnerfors

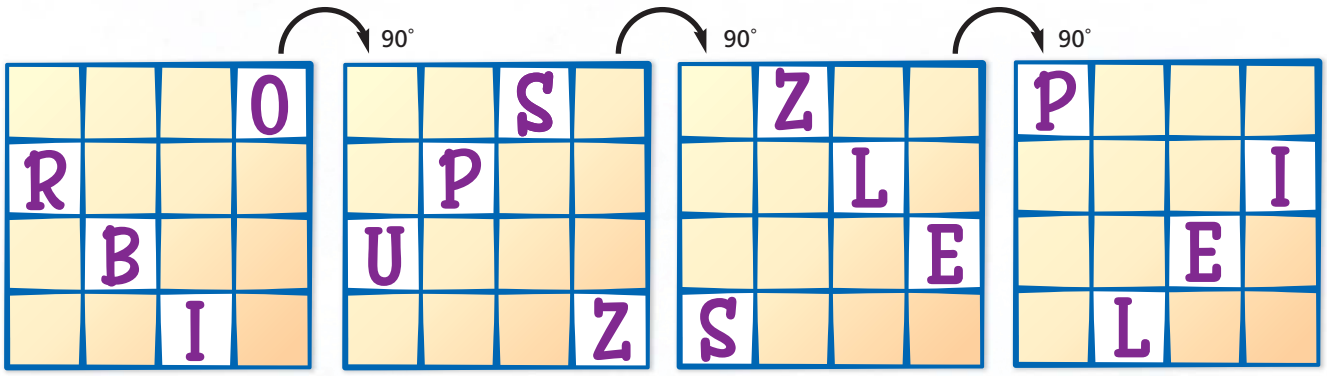
Die Schablone (die passende Schablonenvorlage zur Lösung des untenstehenden Rätsels findest du unter www.derlehrerclub.de/codeknacker) legst du auf ein Blatt, trägst die ersten vier Buchstaben deines Klartextes ein, drehst die Schablone um 90 Grad im Uhrzeigersinn, trägst die nächsten Buchstaben ein und so weiter (maximal vier Mal drehen).

So funktioniert das Prinzip einer Fleissner-Schablone:

- Die Anzahl aller Felder ist durch 4 teilbar. Die Schablone wird viermal jeweils um 90 Grad im Uhrzeigersinn gedreht.
- Ein Viertel der Felder wird ausgeschnitten.
- Die Schablonenfelder dürfen nach einer 90 Grad-Drehung nicht übereinanderliegen.

Am Ende kannst du die leeren Lücken mit irgendwelchen Buchstaben füllen. Das Bild zeigt die Verschlüsselung der beiden fett markierten, unterstrichenen Wörter, die sich dann in folgenden Satz einbinden lassen:

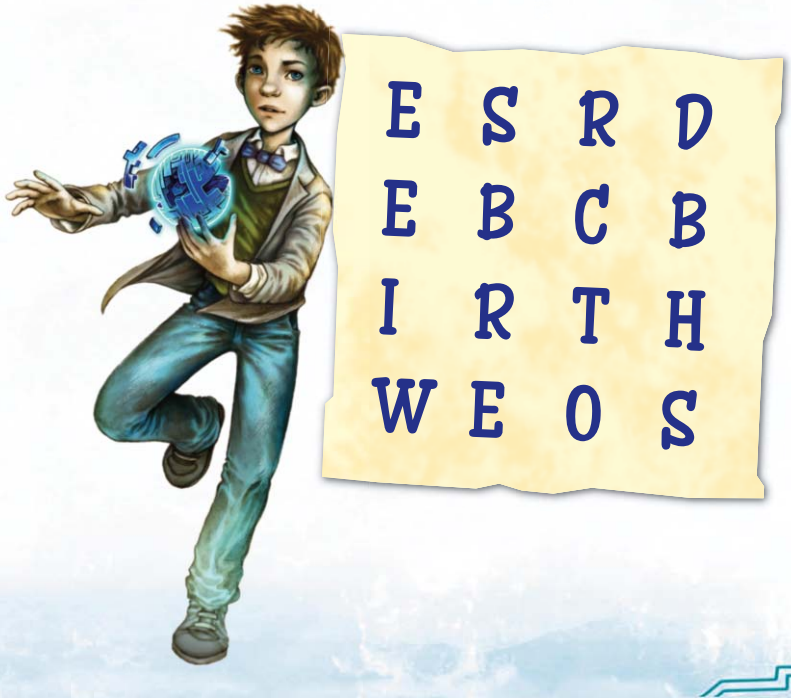
Der Orbis ist vielmehr ein mechanisches Puzzlespiel. (William Wenton, Buch Seite 90)



Geheimtext: PZSO RPLI UBEE SLIZ

RÄTSEL

Kannst du die nebenstehende Fleissner-Verschlüsselung entschlüsseln? Tipp: Verwende dazu die Schablone auf www.derlehrerclub.de/codeknacker.



„Niemand bemerkte einen älteren Mann mit Bart und runder Brille, der durch die Bahnhofshalle rannte."
(William Wenton, Leseprobe Seite 4)

AUFGABE

Bildet in der Klasse zwei Gruppen. Stellt euch vor, jemand würde euch bitten, einer unbekannten Person eine geheime Botschaft persönlich zu überbringen, also nicht per E-Mail oder Ähnliches. Bei Gruppe 1 erfolgt die Bitte durch einen Wildfremden, bei Gruppe 2 durch einen Bekannten oder einen Freund.

Diskutiert: Wie würdet ihr euch verhalten? Würdet ihr sofort ablehnen? Würdet ihr unter bestimmten Bedingungen zusagen? Wie würdet ihr euch bei einer Zusage verhalten, um möglichst wenig aufzufallen?

Besprecht zunächst die Ausgangssituation in eurer Gruppe, um euch über Ablauf und Inhalt des Szenarios einig zu sein. Tauscht anschließend eure Meinungen aus. Wie würdet ihr mit der Situation umgehen und warum?

Vergleicht am Ende die Meinungen in beiden Gruppen. Gibt es Unterschiede, die abhängig davon sind, wer um die Übermittlung der geheimen Botschaft bittet? Wovon hängen eure Entscheidungen ab?

VERSTECKTE BOTSCHAFTEN

Anstatt eine Botschaft zu verschlüsseln, ist es auch möglich, sie zu verstecken. Dies wird auch als Steganografie bezeichnet. Auf diesem Bild aus dem 17. Jahrhundert stehen die Fenster des Hauses jeweils für einen Buchstaben (siehe oben links im Bild). Zusammen ergibt sich eine Botschaft:

WIR HABEN KEIN PULVER MEHR.

Foto: Quelle „Cryptographia" von Friderici aus dem 17. Jahrhundert

RÄTSEL

Findest du das versteckte Wort im folgenden Bild?

Hinweis: Denke an die bisher vorgestellten Verschlüsselungsverfahren.

Foto: © www.pixabay.com

AUFGABE

Beantworte für dich in Stillarbeit schriftlich die Frage: Welche Codes begegnen dir im Alltag? Versuche, dabei ein wenig „über den Tellerrand" zu denken, weg von den hier vorgestellten Verschlüsselungen.

Wofür werden die Codes eingesetzt? Warum musst du sie „enträtseln"?

Tauscht anschließend eure Ideen in der Klasse aus.

„Eigentlich war fast alles ein Code. Ein Garten. Ein Haus. Ein Auto. Alles, was er im Fernsehen sah oder in einem Buch las. Es war wie ein Puzzlespiel. Und sein Gehirn schaltete sich sofort ein." (William Wenton, Leseprobe Seite 8/9)

AUFENTHALTSGENEHMIGUNGEN MIT GEHEIMCODE

In dieser Aufenthaltsgenehmigung aus Frankreich aus dem 18. Jahrhundert sind zahlreiche Informationen über den Inhaber dieses Papiers versteckt. Allerdings geht es dieses Mal nicht um Buchstaben, sondern darum, dass nahezu jeder Bestandteil des Dokuments eine bestimmte Bedeutung hat.

Band um den Rahmen: verheiratet

Sonnenblume: mittelmäßig schön und freundlich

Punkt hinter dem Namen: katholisch

Achteckiger Rahmen: zwischen 30 und 45 Jahre alt

Vier Punkte im Rahmen: wohlhabend, aber nicht reich

Schlangenlinie: leichtsinnig

Foto: Quelle „Kryptographik" aus dem 19. Jahrhundert

AUFGABE

a) Stellt im Kunstunterricht einige Kriterien zusammen, die für die Beschreibung einer Person aus eurer Sicht wichtig sind, zum Beispiel Alter, Geschlecht, Haarfarbe, Größe, charakteristische Eigenschaften wie sportlich, kreativ, musikalisch usw.
b) Ordnet den definierten Kriterien dann bestimmte Symbole zu.
c) Erstellt anschließend in Partnerarbeit Steckbriefe voneinander. Solltet ihr dafür weitere Kriterien benötigen, könnt ihr diese in einer Art „Codebuch" festhalten. Auf die Weise kann die Partnerin bzw. der Partner ihren bzw. seinen Steckbrief lesen. Wichtig: Es dürfen ausschließlich neutral-beschreibende und positive Eigenschaften genutzt werden!

„‚Und aus dir ist ein ziemlich guter Codeknacker geworden, wenn ich das richtig verstanden habe.' ‚Mhm', sagte William. ‚Aber ich glaube, ich lass die Codes jetzt erst mal eine Weile ruhen.'"
(William Wenton, Buch Seite 234)

WIE MAN EINE GEHEIMSCHRIFT KNACKT

Es gibt viele verschiedene Geheimschriften. Das Bild unten zeigt beispielsweise einen Text aus dem 16. Jahrhundert, der in einer Geheimschrift verfasst ist.

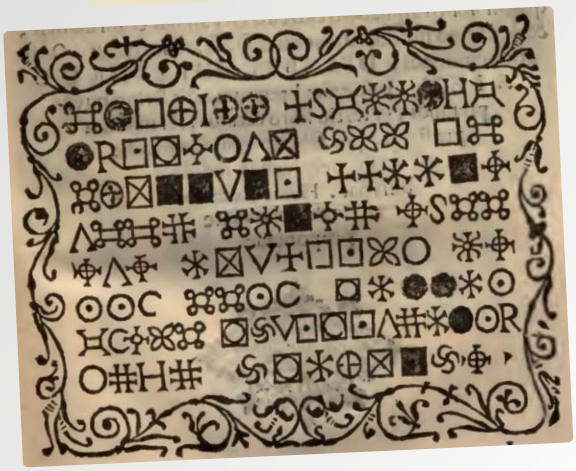


Foto: Quelle „De furtivis literarum notis" aus dem 16. Jahrhundert

> „Jedes Jahr nimmt das Institut eine Handvoll Kandidaten auf, die sich in den Fächern Code-knacken und Problemlösung ausgezeichnet haben." (William Wenton, Buch Seite 56)

Nahezu jede Geheimschrift lässt sich entschlüsseln. Dazu muss man wissen, dass in der deutschen Sprache das E der häufigste Buchstabe ist, gefolgt vom N. Zum Lösen muss man also zunächst die Buchstaben zählen und dann versuchen, diese beiden Buchstaben zu ermitteln. Die restlichen Buchstaben lassen sich oft erraten.

Es gibt noch eine andere Methode zum Entschlüsseln einer Geheimschrift: Du kannst, zum Beispiel mit dem kostenlosen Computer-Programm CrypTool, nach auffälligen Wortmustern suchen. Das Geheimschriftwort §%$!#?&?*§ hat beispielsweise das Muster ABCDEFGFIA. Auf dem Bild unten siehst du, welche Wörter mit diesem Muster CrypTool gefunden hat.

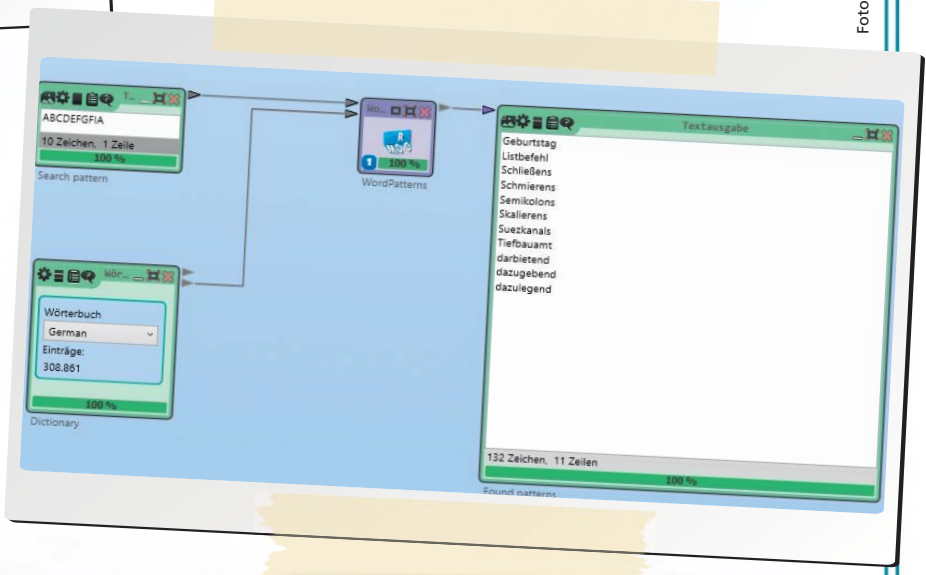


Foto: © www.cryptool.org | Screenshot

RÄTSEL

Kannst du die folgende Geheimbotschaft entschlüsseln?

4 9 5 19 5 13 2 15 12 5 1 14 4 5 13
7 18 15 19 19 5 14 20 15 18
16 1 12 19 9 5 18 20 5 14 9 14 2 12 1 1

CODEBÜCHER

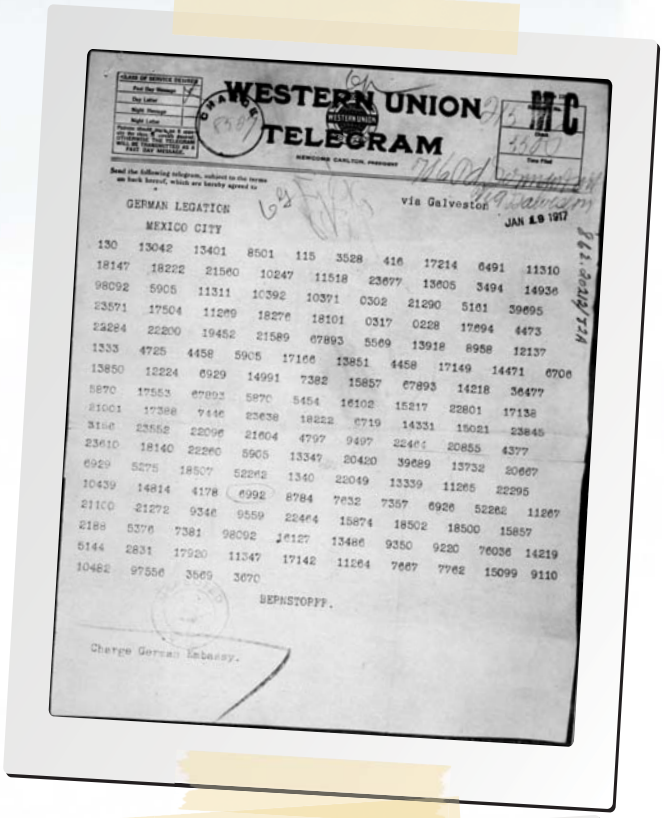
Manche Verschlüsselungsverfahren basieren darauf, dass man für jedes zu verschlüsselnde Wort ein Codewort aus einem Buch (Codebuch) heraussucht – ähnlich wie aus einem Wörterbuch. Ein Codewort kann auch aus einer Zahl bestehen.

ZIMMERMANN-TELEGRAMM

Während des Ersten Weltkriegs, im Jahr 1917, schickte der deutsche Außenminister Arthur Zimmermann ein Telegramm nach Mexiko. Darin ermutigte er die mexikanische Regierung, einen Krieg gegen die USA zu beginnen. Zimmermann verschlüsselte das Telegramm mit einem Codebuch.

Britische Chiffrierexperten, die das Telegramm zugespielt bekamen, konnten es entschlüsseln. Die Öffentlichkeit in den USA regierte empört auf den deutschen Versuch, einen Krieg zwischen Mexiko und den USA anzuzetteln.

Das Zimmermann-Telegramm trug wesentlich dazu bei, dass die bis dahin neutralen USA im Jahr 1917 gegen Deutschland in den Ersten Weltkrieg eintraten. Der Krieg wurde für die Deutschen dadurch noch aussichtsloser. 1918 mussten sie kapitulieren.


WESTERN UNION TELEGRAM

GERMAN LEGATION
MEXICO CITY

via Galveston

JAN 19 1917

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10462 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.

Foto: https://commons.wikimedia.org/wiki/File%3AZimmermann_Telegram.jpeg | By The U.S. National Archives [No restrictions], via Wikimedia Commons

ENIGMA

Ab etwa 1920 ging man dazu über, spezielle Maschinen zur Verschlüsselung zu verwenden. Die bekannteste Verschlüsselungsmaschine ist die Enigma. Die Deutschen setzten sie im Zweiten Weltkrieg ein. Knapp 30.000 Exemplare wurden gebaut.

Die Enigma arbeitet mit verdrahteten Walzen. Drückt der Bediener eine Taste, fließt Strom durch die Walzen und bringt eine Lampe zum Leuchten. Nach jedem Buchstaben drehen sich die Walzen wie bei einem mechanischen Kilometerzähler weiter.

Die Deutschen hielten die Enigma im Zweiten Weltkrieg für sicher. Doch weit gefehlt: Der britische Mathematiker Alan Turing half dem britischen Geheimdienst dabei, den Code der Wehrmacht zu knacken. Mit speziellen Maschinen und unzähligen Arbeitskräften gelang es, mehrere Hunderttausend Enigma-Funksprüche zu knacken. Dies brachte den Briten entscheidende Vorteile im Krieg.

Foto: © Greg Goebel

Hinweis für Lehrkräfte: Über Alan Turing wurde der Film „The Imitation Game“ gedreht. Hier bietet sich auch das Anschauen des Films (FSK ab 12 Jahren) und die Arbeit mit Filmausschnitten an.

UNGELÖSTE RÄTSEL

DAS RÄTSEL DES SOMERTON-MANNS

Im Jahr 1948 fand man am Somerton-Strand in Adelaide (Australien) die Leiche eines Mannes. Bis heute ist nicht bekannt, wer diese Person war. Bei dem Unbekannten fand man eine verschlüsselte Botschaft, die bis heute niemand entschlüsseln konnte.

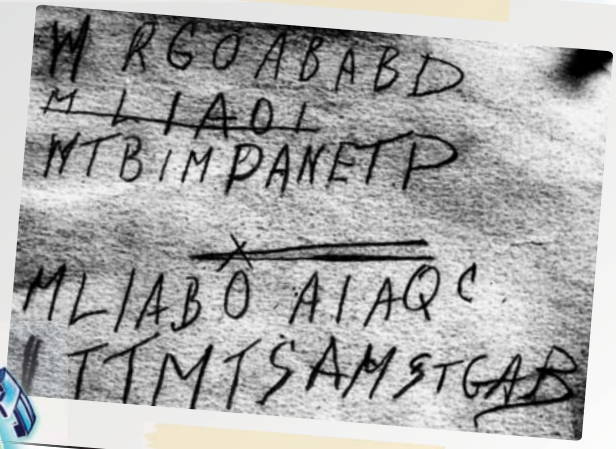


Foto: https://commons.wikimedia.org/wiki/File:SomertonManCode.jpg | By Australian police, via Wikimedia Commons

> „Fast unmöglich zu lösen. Einige der bedeutendsten Entschlüsselungsexperten der Welt hatten es bereits vergeblich versucht."
> (William Wenton, Buch Seite 19)

DAS VOYNICH-MANUSKRIPT

Das Voynich-Manuskript ist ein verschlüsseltes Buch aus dem 15. Jahrhundert. Bis heute hat es niemand geschafft, die Verschlüsselung zu lösen. Der Buchhändler Wilfried Voynich erwarb das später nach ihm benannte Buch im Jahr 1912 von einem Kloster in der Nähe von Rom. Das Voynich-Manuskript ist handgeschrieben, handgemalt und ein Einzelstück. Die Schrift wird in keinem anderen bekannten Schriftstück verwendet.

Manche Verschlüsselungsexperten vermuten, der Text sei auf Latein verfasst worden, andere gehen eher von Deutsch, Englisch, Italienisch oder Griechisch aus. Auch über das verwendete Verschlüsselungsverfahren wurde viel spekuliert. Möglich ist auch, dass das Voynich-Manuskript gar keinen sinnvollen Inhalt hat. Mindestens 40 Personen haben für sich in Anspruch genommen, das Voynich-Manuskipt entschlüsselt zu haben. Fachleute haben keine dieser vermeintlichen Lösungen als korrekt anerkannt.

Foto: © Klaus Schmeh

Die zahlreichen Bilder im Voynich-Manuskript helfen nicht weiter, denn sie sind ziemlich nichtssagend: Pflanzen, die es in der Realität nicht gibt, kreisförmige Muster, nackte Personen. Weder der Text noch die Abbildungen liefern Anhaltspunkte darüber, wer das Buch wann und wo geschrieben hat. Immerhin: Eine Altersbestimmung mit der Radiokarbon-Methode hat ergeben, dass das Papier (genauer: das Pergament) im 15. Jahrhundert hergestellt wurde.

„Als ob sie das Kribbeln im Körper kannte, das William immer dann verspürte, wenn er an den Code dachte, den noch niemals irgendwer geknackt hatte.“ (Leseprobe William Wenton, Seite 11)

AUFGABE

Erstellt in Partnerarbeit ein verschlüsseltes Mini-Manuskript. Ihr könnt dafür beispielsweise einen DIN-A3-Karton auf A4 falten, sodass ihr vier Seiten bearbeiten könnt. Verfasst kurze Texte, die mit dem Inhalt des Buches zusammenhängen, zum Beispiel einen Tagebucheintrag von Williams Mutter oder ein Telegramm des Großvaters an die Familie. Anschließend verschlüsselt ihr diese. Wählt aus, ob ihr dafür unterschiedliche Verschlüsselungsmethoden verwendet oder ob ihr euch auf eine Methode beschränkt. Denkbar ist auch eine eigens entwickelte Bild- oder Symbolsprache. Das Manuskript könnt Ihr künstlerisch gestalten und bebildern. Am Ende werden die Manuskripte in der Klasse präsentiert. Versucht in Kleingruppen die Manuskripte der anderen zu entschlüsseln.

KRYPTOS-INSCHRIFT

Die bekannteste verschlüsselte Inschrift der Welt befindet sich auf der Skulptur Kryptos, die auf dem Gelände des Geheimdiensts CIA in der Nähe der US-Hauptstadt Washington steht. Der verschlüsselte Text besteht aus 865 Buchstaben. Inzwischen weiß man, dass er sich aus vier unterschiedlich verschlüsselten Teilen zusammensetzt. Mehrere Codeknacker haben unabhängig voneinander die ersten drei Teile entschlüsselt. Der vierte Teil wartet nun schon seit fast 30 Jahren auf seine Entschlüsselung.

Er lautet:

OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR

Foto: https://commons.wikimedia.org/wiki/File:Kryptos_sculptor.jpg I By Jim Sanborn, via Wikimedia Commons

„Es war nicht irgendein Code, William. Es war der schwierigste Code der Welt. Vermutlich hätten das nur Opa und du geschafft.“ (William Wenton, Buch Seite 40)

BAHNRÄUBER-KRYPTOGRAMM

1916 überfiel ein Unbekannter einen Fahrkartenschalter in Ohio, USA. Laut einem Zeitungsbericht verschickte der Räuber kurz vor oder nach der Tat folgendes Telegramm:

WAS NVKVAFT BY AAKAT TXPXSCK UPBK TXPHN
OHAY YBTX CPT MXHG WAE SXFP ZAVFZ ACK
THERE FIRST TXLK WEEK WAYX ZA WITH THX.

Vermutlich hat der Täter zum Verschlüsseln ein Codebuch verwendet. Einige Wörter (THERE, FIRST, WEEK) hat er dabei im Klartext gelassen. Bis heute sind sowohl der Raubüberfall als auch das verschlüsselte Telegramm ungelöst.

RÄTSEL

Kannst du die untenstehende verschlüsselte Inschrift lösen?

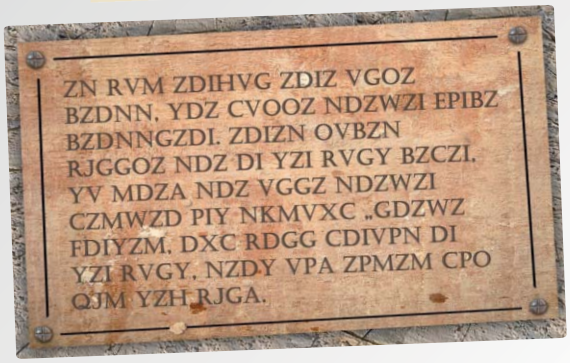


Foto: © Klaus Schmeh

MODERNE VERSCHLÜSSELUNGS-VERFAHREN

Heutzutage gibt es deutlich bessere Verschlüsselungsmethoden als die Pigpen-Verschlüsselung, die Enigma oder Codebücher. Heutige Computer sind außerdem in der Lage, sehr schnell zu ver- und entschlüsseln. Das bekannteste moderne Verschlüsselungsverfahren hat den Namen AES (Advanced Encryption Standard).

E-Mails sind nicht privat. Mit wenig Aufwand können Geheimdienste oder Kriminelle sie abfangen. Es ist bekannt, dass die NSA (National Security Agency) und andere Geheimdienste im großen Stil E-Mails mitlesen. Yahoo musste im Auftrag der NSA sogar sämtliche E-Mails auf dem eigenen Server nach bestimmten Stichworten durchsuchen.

Die Plattform Lavabit, ein international wichtiger Anbieter für sichere E-Mail-Kommunikation, hat 2013 aufgrund des hohen Drucks der US-Regierung ihr Angebot vom Netz genommen. Die Regierung hatte den Anbieter aufgefordert, die privaten SSL-Schlüssel herauszugeben. Mit diesen digitalen Zertifikaten wäre ein Zugriff auf die Daten aller 400.000 Nutzer möglich gewesen.

Soll wirklich kein Dritter Zugriff auf die Informationen einer E-Mail bekommen, ist es unumgänglich, auf Verschlüsselungsmethoden zurückzugreifen.

AUFGABE

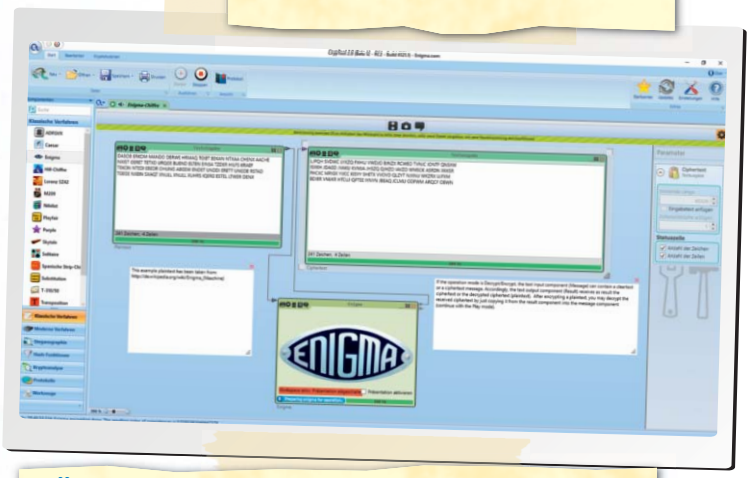
Recherchiere im Internet nach unterschiedlichen Formen zur Verschlüsselung von E-Mails. Welche Möglichkeiten gibt es? Wie funktionieren sie? Auf welche Weise könntest du sie selbst für deine private Kommunikation einsetzen? Erarbeite eine strukturierte und informative Aufstellung. Tauscht euch bei Unklarheiten und offenen Fragen zwischendurch aus.

Vergleicht eure Ergebnisse im Anschluss in der Klasse. Wenn ihr die Möglichkeit habt, testet die Verschlüsselungsmethoden anhand eines realen E-Mail-Verkehrs.

CRYPTOOL

CrypTool ist ein kostenloses Programm, mit dem du über 100 unterschiedliche Verschlüsselungsverfahren anwenden kannst. Eine Enigma-Verschlüsselung ist mit CrypTool genauso möglich wie eine AES-Verschlüsselung. Auch einige Methoden zum Knacken von Verschlüsselungen werden unterstützt, beispielsweise das Zählen von Buchstaben in einem Text.

CrypTool findest du im Internet unter: www.cryptool.org



GNU PG

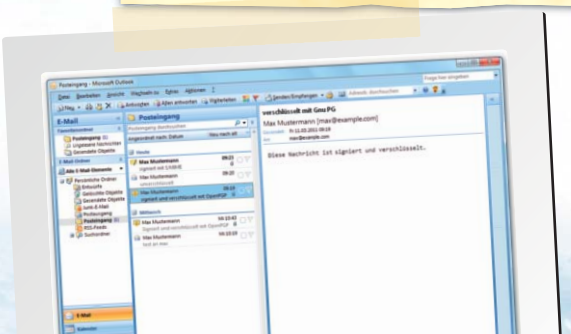
Gnu PG ist ein kostenloses Programm zum Verschlüsseln von E-Mails und Dateien. Es handelt sich dabei um die kostenlose Variante von PGP (Pretty Good Privacy), dem wohl bekanntesten Verschlüsselungsprogramm überhaupt. Gnu PG gilt als so sicher, dass selbst die besten Codeknacker der Welt machtlos sind.

Gnu PG erhältst du kostenlos im Internet unter https://www.gnupg.org.

RÄTSEL

Löse folgende Cäsar-Verschlüsselung mit CrypTool.

TYU AKWUB MQH IE WHEII MYU UYD QFVUB, KDT IYU MQH RUTUSAJ LED IUBJIQCUD PUYSXUD.



Fotos: Screenshots

„Sein Vater hatte Recht gehabt. Um Codes sollte man einen großen Bogen machen." (William Wenton, Buch Seite 204)

IMPULSE FÜR DEN UNTERRICHT

Hinweis: Als Einstieg in das Thema Kryptologie bietet sich die Lektüre der Leseprobe von „William Wenton" auf www.derlehrerclub.de/codeknacker oder auch das Anhören der Hörprobe von ca. 4 Minuten auf www.youtube.com/watch?v=ee1vhvcQDh8 an. Alternativ können auch die ersten Seiten gemeinsam in der Klasse gelesen werden.

Die Lektüre eignet sich sehr gut zum fächerübergreifenden und projektorientierten Arbeiten, zum Beispiel in Deutsch, Mathematik, Kunst und Geschichte.

PRIVATSPHÄRE

Diskutieren Sie mit Ihrer Klasse, in welchen Bereichen den Schülerinnen und Schülern Verschlüsselung wichtig ist. Gab oder gibt es Lebenssituationen, in denen sie eine Nachricht gern geschützt vor anderen verschicken möchten? Warum? In welchem Verhältnis stehen Nutzen und Aufwand? Auf welche Weise ist die Verschlüsselung von Nachrichten möglich?

VERSCHLÜSSELUNG IM ÖFFENTLICHEN LEBEN

Warum nutzt der Mensch im öffentlichen, gesellschaftlichen, politischen Bereich manchmal Verschlüsselungsmethoden – früher und heute? Haben die Schülerinnen und Schüler Ideen, welche Themen schützenswert sein könnten und warum? Wo begegnen ihnen im Alltag Verschlüsselungen?

VERSCHLÜSSELTE NACHRICHTEN

Zwei Schüler einigen sich in Partnerarbeit auf ein Verschlüsselungsverfahren. Auf dessen Basis schicken sie kurze Nachrichten hin und her – ähnlich wie per WhatsApp.

STATIONENLERNEN

Bauen Sie verschiedene Stationen auf, welche die Schülerinnen und Schüler nacheinander – entweder allein oder in Partnerarbeit – bearbeiten sollen. Jede Station widmet sich einer anderen Verschlüsselungsmethode bzw. einem Rätsel. Orientieren Sie sich dafür an den in diesem Material aufgeführten Methoden. Denkbar sind darüber hinaus Puzzle, Bilder- oder Kreuzworträtsel.

DIE UNMÖGLICHKEITSAUSSTELLUNG

In einem Portfolio werden Ideen zu einer „Unmöglichkeitsausstellung" in der Klasse gesammelt. Im Mathematikunterricht können mathematische Rätsel entwickelt werden. Welche bahnbrechenden Erfindungen wünschen sich die Schülerinnen und Schüler? Welche ungelösten Rätsel gibt es?

DER GEHEIME BRIEF

Die Schülerinnen und Schüler verschlüsseln und gestalten einen Brief, den William in einem Ordner mit Unterlagen seines Großvaters gefunden hat. Der Brief hat folgenden Inhalt:

MEIN LIEBER ENKEL WILLIAM,

ICH WUSSTE, DASS DU EINES TAGES DIESE BOTSCHAFT FINDEN WÜRDEST. VOR DIR LIEGT EINE GROSSE AUFGABE. NUR DU KANNST SIE LÖSEN. DU BIST DER EINZIGE AUSSER MIR, DER DIE SYMBOLE ENTSCHLÜSSELN KANN. DU WIRST DAS GEHEIME TOR FINDEN. ICH WÜNSCHE DIR VIEL GLÜCK.

DEIN GROSSVATER

STECKBRIEFE

Anhand der Informationen aus der Leseprobe verfassen die Schülerinnen und Schüler Steckbriefe oder Charakterisierungen von William Wenton, seinem Lehrer Herrn Humburger oder der Museumsführerin Edna. Zusätzlich kann auch ein Steckbrief oder ein Autorenportrait von Bobbie Peers, dem Autor des Buches, verfasst werden. Welche Charakteristika gilt es zu berücksichtigen?

COMIC, BILDERGESCHICHTE ODER DARSTELLENDES SPIEL

Im Deutsch- und Kunstunterricht wird der Inhalt der Leseprobe als Comic oder Bildergeschichte dargestellt. Denkbar ist auch, einzelne Szenen im darstellenden Spiel zu präsentieren, als Film aufzuzeichnen oder einen Trailer zu entwickeln, der Lust macht, die weitere Geschichte um William Wenton kennenzulernen.

BILDERRÄTSEL

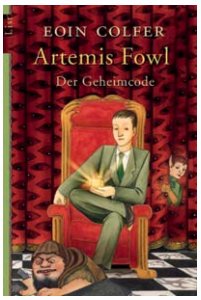
Die Schülerinnen und Schüler entwickeln eigene Bilderrätsel. Dann versuchen sie, die Rätsel der anderen zu lösen.

LESE- UND MEDIENTIPPS

Bobbie Peers
William Wenton und die Jagd nach dem Luridium
Carlsen Verlag, Hamburg 2017,
240 S., 14,99 EUR, ab 10 Jahren

Niemand kann Rätsel besser lösen als William Wenton! Seit er sich jedoch mit seinen Eltern in Norwegen verstecken muss, ist er gezwungen, diese Fähigkeit geheim zu halten. Eines Tages ist es jedoch vorbei mit dem Verstecken: Er wird von geheimnisvollen Fremden ans Institut für Posthumane Forschung entführt. Hier erfährt er, dass er zu den sogenannten „Kandidaten" gehört, deren Aufgabe es ist, die Welt vor dem gefährlichen Luridium zu beschützen.
Weitere Infos und Leseprobe:
www.carlsen.de und
www.derlehrerclub.de/codeknacker

Eoin Colfer
Artemis Fowl
Der Geheimcode
List Verlag, Berlin 2015, 336 S.,
8,99 EUR, ab 12 Jahren



Artemis Vater hat beschlossen, ab jetzt nur noch auf legalen Wegen zu wandern und will auch seinen Sohn bekehren. Doch Artemis kann sich ein Leben ohne Tricksereien und Betrügereien nicht vorstellen. Bevor die Familie Fowl also endgültig in die Legalität rutscht, plant Artemis noch einen letzten großen Coup: Er will den amerikanischen Geschäftsmann John Spiro um ein paar Millionen erleichtern.

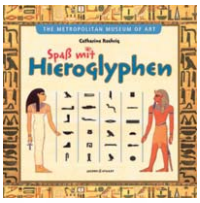
Christoph Dittert
Die drei ???
Geheimnisvolle Botschaften
dtv junior, München 2015, 160 S.,
5,95 EUR, ab 8 Jahren

Die drei ??? sind gerade dabei, sich Attraktionen auf dem Handwerkermarkt anzusehen, da treffen sie nicht nur auf einen zwielichtigen Pergamentmacher, sondern auch auf einen neuen Fall: In Barbaras Haus wurde eingebrochen. Seltsamerweise wurde ein altes, handgefertigtes Buch gestohlen, das nur für Barbaras Vater einen größeren Wert hat. Schon bald finden die Detektive heraus, dass das Buch ein spannendes Rätsel enthält, das zu einem Schatz führen könnte.

Helen Phillips / Birte Schnöinck
Paradiesvoll und geheimnisgrün
Silberfisch Verlag, Hamburg 2013,
4 CDs, Laufzeit 300 Min., € 19,99
ab 11 Jahren

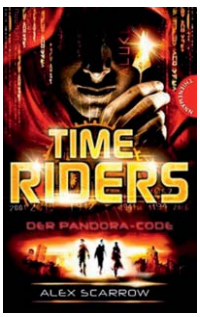
Mad und Ru haben sich mit ihrer Mutter auf die Reise zu einer Vulkaninsel gemacht. Dort hält sich der Vater der Schwestern, ein berühmter Vogelbeobachter, auf. Er hat ihnen zuvor einen merkwürdigen Brief geschrieben. Mad vermutet, dass der Text verschlüsselt ist! Mad und Ru erkennen ihren Vater kaum wieder, so abwesend und verwirrt wie er sich verhält. Als auch ihre Mutter nach einer Weile verrücktspielt, erkennen die Schwestern, dass definitiv etwas nicht stimmt.

Catharine Roehrig
Spaß mit Hieroglyphen
Jacoby & Stuart Verlag, Berlin 2012,
48 S., 24,95 EUR, ab 9 Jahren



Mithilfe dieses Sets, das aus einem Booklet, einem Stempelkissen und Hieroglyphenstempeln besteht, können Hieroglyphen erlernt, angewendet und entziffert werden. Mit spannenden Rätseln und Aufgaben für Leserinnen und Leser!

Alex Scarrow
Time Riders: Der Pandora Code
Thienemann Verlag, Stuttgart 2012,
496 S., 12,95 EUR, ab 12 Jahren



Liam, Maddy und Sal wurden vor die Wahl gestellt, ob sie sterben oder aber „Time Rider" werden wollen. Alle drei haben zu verschiedenen Zeiten gelebt. Liam hätte mit der Titanic versinken sollen. Maddy sollte 2010 bei einem

Flugzeugabsturz sterben und Sal wäre eigentlich 2026 in einem Feuer verbrannt. Doch wenige Augenblicke vor ihrem Tod konnten sie ein anderes Schicksal wählen und leben seitdem in einer Zeitblase in New York City. In ihrem neuen Abenteuer helfen sie Adam, einem britischen Computerhacker, dessen Name in einem verschlüsselten Manuskript aus dem 12. Jahrhundert aufgetaucht ist.

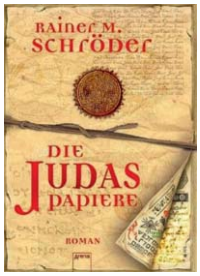
Klaus Schmeh
Codeknacker gegen Codemacher
Die faszinierende Geschichte der Verschlüsselung
W3L-Verlag, Dortmund 2014,
509 S., € 39,90

Codierte Texte, kuriose Illustrationen, kluge Codeknacker – davon erzählt dieses Buch und führt durch die Geschichte der Kryptologie. Angefangen bei der Verschlüsselung von Hand im Altertum, erfährt der Leser viel Spannendes. Faszinierende Lektüre über Spionagefälle, verschlüsselte Tagebücher und andere Kuriositäten!

Hans-J. Schmidt
Stationenlernen Geheimschriften Verschlüsseln & knacken wie der Geheimdienst
Kohl Verlag, Kerpen 2015, 72 S.,
17,80 EUR

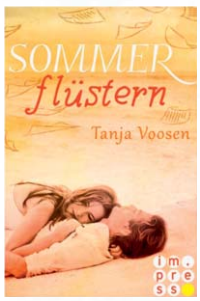
In 32 Stationen von „Verschlüsseln mit der Gartenzaunmethode“ über „Die Geheimschrift des Polybius“ bis hin zu „Verschlüsseln mit Chiffrierschablonen“ werden Schüler und Schülerinnen der Klassen 5 und 6 spielerisch an die Kryptografie herangeführt. Die Stationen sind in drei Niveaustufen eingeteilt, sodass für jede Schülerin bzw. jeden Schüler etwas dabei ist.

Rainer M. Schröder
Die Judas-Papiere
Arena Verlag, Würzburg 2013,
616 S., 9,99 EUR, ab 14 Jahren



Hier geht es um vier Menschen, die unterschiedlicher nicht sein könnten, ein geheimnisvolles Notizbuch und eine schwierige Suche. Harriet, Byron, Alistair und Horatio wurden von Lord Pembroke beauftragt, ein außergewöhnliches Dokument zu finden: das Evangelium des Judas. Mortimer Pembroke, der psychisch kranke Bruder von Lord Pembroke, hat es auf einer seiner Weltreisen an einem unbekannten Ort versteckt.

Tanja Voosen
Sommerflüstern
Carlsen Impress Verlag, Hamburg
2016, 308 S., 12,99 EUR, ab 14 Jahren



Taylor ist seit einigen Monaten auf einer neuen Highschool. Zum Schulanfang findet sie eine seltsame Nachricht in ihrem Spind: Fange an, deinen Lieblingssong zu hassen. Noch ist Taylor nicht dahintergekommen, was das bedeuten soll. Das ändert sich, als Hunter Reeves an die Schule zurückkehrt. Denn Taylors Spind war damals Hunters Spind und die Nachricht ist eigentlich für ihn bestimmt.

Barbara Wernsing
Notsignale und Geheimzeichen
Coppenrath Verlag, Münster 2016,
64 S., 9,99 EUR, ab 8 Jahren

Geheimnisvolle Zeichen, Signale und Geheimschriften warten auf das gekonnte Entschlüsseln. Das Spektrum reicht von Hintergrundwissen über das richtige Verhalten im Notfall über spannende Zeichen wie Tierspuren oder die geheimen Markierungen der Waldläufer, Handzeichen wie Gebärdensprache oder Fingeralphabet bis zu Hörsignalen und Geheimschriften.

Weitere Lesetipps:
www.derlehrerclub.de/service/lese-und-medientipps/

Weitere Linktipps:
www.derlehrerclub.de/codeknacker