

SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Stationenlernen Geheimschriften - TOP SECRET

Das komplette Material finden Sie hier:

School-Scout.de



INHALT

Station	Stationsname	Seite	●	!★	E/P	benötigte Materialien
1	Rund um Geheimschriften - ein Puzzle	9	●		P	Schere, Klebstoff, Heft, Papier
2	Das Winkeralphabet	11	●		E	Heft, Bleistift, Papier
3	Verschlüsseln durch zufälliges Trennen	13	●		P	Heft, Bleistift, Papier
4	Verschlüsseln mit der Gartenzaunmethode	15	●		E	Geodreieck, Heft, Bleistift, Papier
5	Verschlüsseln in Quadraten	17		!	E	Geodreieck, Heft, Bleistift, Papier
6	Verschlüsseln in Rechtecken	19		!	P	Geodreieck, Heft, Bleistift, Papier
7	Verschlüsseln in Rechtecken mit Blendern	21		★	P	Geodreieck, Heft, Bleistift, Papier
8	Die Chiffre der Freimaurer	23	●		E	Heft, Bleistift, Papier
9	Die Geheimschrift des Polybius	25		!	E	Heft, Bleistift, Papier
10	Rechteck mit Zahlenschlüssel	27		★	P	Heft, Bleistift, Papier
11	Julius Cäsars Geheimschrift (1)	29	●		P	Heft, Bleistift, Papier
12	Cäsars Geheimschrift mit griechischen Buchstaben	31		!	E	Heft, Bleistift, Papier
13	Verschlüsseln mit Chiffrier-Schablonen (1)	33	●		P	Schere, Heft, Bleistift, Papier
14	Verschlüsseln mit Chiffrier-Schablonen (2)	35		★	P	Schere, Heft, Bleistift, Papier
15	Versteckte Nachrichten in Briefen (1)	37	●		P	Heft, Bleistift, Papier
16	Versteckte Nachrichten in Briefen (2)	39		★	P	Heft, Bleistift, Papier
17	Zur Information: Wissenswertes zu Drehscheiben	41		★	P	
18	Drehscheibe für Julius Cäsars Geheimschrift	42	●		E	Schere, Klebstoff

INHALT

Station	Stationsname	Seite	!★	E/P	benötigte Materialien
19	Julius Cäsars Geheimschrift (2)	43	!	P	Heft, Bleistift, Papier, Drehscheibe (Station 18)
20	Cäsar mit Schlüsselwort	45	●	P	Heft, Bleistift, Papier
21	Wie knackt man einen einfachen Cäsar (1)	47	!	P	Heft, Bleistift, Papier, Drehscheibe (Station 18)
22	Wie knackt man einen einfachen Cäsar (2)	49	★	P	Heft, Bleistift, Papier, Drehscheibe (Station 18)
23	Wie knackt man einen Cäsar mit Schlüsselwort (1)	51	!	E	
24	Wie knackt man einen Cäsar mit Schlüsselwort (2)	55	★	P	Heft, Bleistift, Papier, Station 23
25	Wie knackt man einen Cäsar mit Schlüsselwort (3)	57	★	P	Heft, Bleistift, Papier, Station 23
26	Zur Information: Die Vigenère-Verschlüsselung	59	●	E	
27	Schieber für die Vigenère-Verschlüsselung	60	!	P	Schere, Klebstoff
28	Verschlüsseln mit dem Vigenère-Schieber	61	●	P	Heft, Bleistift, Papier, Vigenère-Schieber (Station 27)
29	Wie knackt man eine Vigenère-Verschlüsselung?	63	!	P	Heft, Bleistift, Papier, Vigenère-Schieber (Station 27)
30	Die Kasiski-Methode zur Ermittlung der Schlüssellänge	68	●	E	Heft, Bleistift, Papier
31	Wir knacken die Vigenère-Verschlüsselung (1)	69	!	P	Heft, Bleistift, Papier, Station 30
32	Wir knacken die Vigenère-Verschlüsselung (2)	71	★	P	Heft, Bleistift, Papier, Station 30

ANLEITUNG

Sehr geehrte Kollegen und Kolleginnen,

dieses Werk zum Stationenlernen: Geheimschriften **TOP SECRET** soll Ihnen Ihre alltägliche Arbeit erleichtern. Dabei war es uns besonders wichtig, Stationen zu kreieren, die möglichst schüler- und handlungsorientiert sind und mehrere Lernzugangskanäle ansprechen. Denn nur so kann Wissen langfristig gesichert und auch wieder abgerufen werden. Die Reihenfolge der Stationen ist festgelegt. Dennoch können die Schüler in ihrem individuellen Arbeits- und Lerntempo vorgehen. Die Materialien eignen sich dank der auf allen Stationen gegebenen Hilfestellungen auch hervorragend für das selbstständige Lernen oder die Selbstlernzeit.

Stationen:

Die Stationen sind von 1-32 nummeriert und müssen nicht notwendigerweise nacheinander bearbeitet werden.

Das Puzzle der Station 1 „Rund um Geheimschriften“ dient als Einstieg in das Thema und sollte von allen zuerst bearbeitet werden.

Bei den Stationen 2-16 können Schülerinnen und Schüler selbst entscheiden, welche Station sie bearbeiten.

Den Stationen 18 und 27 kommt besondere Bedeutung zu, weil hier Verschlüsselungshilfen (Drehscheibe für die Cäsar Verschlüsselung bzw. Vigenère-Schieber) gebastelt werden.

Weil Kryptographie zur Zeit ein hochaktuelles Thema ist – man denke an die NSA und an diverse Hackerangriffe auf Datenbanken – und man bei der Verschlüsselung bzw. Entschlüsselung von Daten mit Methoden aus der Mathematik arbeitet, hat die Behandlung dieses Themas im Mathematikunterricht durchaus seine Berechtigung.

Schülerinnen und Schüler der Klassen 5 und 6 können auf spielerische Weise an die Grundprinzipien der Kryptographie herangeführt werden. Das geschieht vor allem durch Stationen wie „Verschlüsseln mit der Gartenzaunmethode“, „Die Geheimschrift des Polybius“ oder „Verschlüsseln mit Chiffrierschablonen“. Kinder haben aber auch ihre eigenen Geheimschriften bzw. Geheimsprachen, die sie im Unterricht vorstellen können.

Anspruchsvoller sind die Stationen 17-32. Zunächst einmal werden die Schüler und Schülerinnen mit monoalphabetischen Geheimschriften wie dem einfachen Cäsar und dem Cäsar mit Schlüsselwort vertraut gemacht. Sie verschlüsseln und entschlüsseln mit der gebastelten Drehscheibe der Station 18 diverse Nachrichten. Will man einen einfachen Cäsar knacken, dann reicht es, wenn man alle 25 Schlüssel durchprobiert. Hier ist dann der Zeitpunkt gekommen für eine Häufigkeitsanalyse. Da in der deutschen Sprache der Buchstabe e mit Abstand am häufigsten vertreten ist, sucht man im Geheimtext nach dem häufigsten Buchstaben und hat damit den Schlüssel vermutlich etwas schneller gefunden als durch Ausprobieren.

ANLEITUNG

Etwas aufwändiger gestaltet sich die Kryptoanalyse eines Cäsars mit Schlüsselwort. Daher wurde in der Station 23 ausführlich dargestellt, wie man einen solchen Geheimtext entschlüsselt. Diese Station dient lediglich der Information und soll zeigen, dass man sehr viel Geduld, Fingerspitzen- und Sprachgefühl benötigt, um eine geheime Nachricht zu knacken.

In Station 25 soll ein deutscher, in Station 26 ein englischer Geheimtext entschlüsselt werden.

Die Stationen 26-32 befassen sich mit der Vigenère-Verschlüsselung und der Methode zum Dechiffrieren solcher polyalphabetischer Mitteilungen. Auch diese Methode zum Dechiffrieren kann von Schülern und Schülerinnen einer 6. Klasse angewandt werden. Für die Kasiski-Methode zur Ermittlung der Länge des Schlüsselwortes muss lediglich der Geheimtext auf gleiche Buchstabenfolgen untersucht werden, der Abstand zwischen zwei Folgen ermittelt werden und der größte gemeinsame Teiler dieser Abstände bestimmt werden. Bezeichnungen wie „absolute Häufigkeit“ und „Rangfolge“ sind in der Klassenstufe 5/6 ebenfalls bekannt.

Niveaustufen:

Innerhalb der Bereiche gibt es drei unterschiedliche Niveaustufen, die mit ● (leicht), ! (mittel) oder ★ (schwer) markiert sind. Die mit einem Stern gekennzeichneten Stationen sind für Experten, die mit ● gekennzeichneten Stationen sollen von allen Schülern bearbeitet werden. Die Expertenaufgaben enthalten vertiefende oder weiterführende Inhalte. Selbstverständlich können Sie je nach Leistungsstand Ihrer Klasse problemlos Stationen anders kennzeichnen, indem Sie ●, ! oder ★ übermalen und anders kennzeichnen.

Lösungen:

Wer die Aufgaben der Schüler korrigiert, hängt zum einen von der Lerngruppe und zum anderen von den Vorlieben des unterrichtenden Lehrers ab. So können Sie die Verbesserung der Schüleraufgaben selbst übernehmen, oder diese Aufgabe in die Verantwortung der Kinder übergeben. In diesem Fall haben Sie die Möglichkeit, die Karten einfach auszuschneiden und zu laminieren. Es befindet sich dann direkt auf der Rückseite der Aufgabe die passende Lösung zur einfachen Selbstkontrolle (Ausnahmen: Stationen 17, 18, 23, 26, 27, 29, 30). Alternativ können Sie die Seiten jedoch auch kopieren und die Lösungen, für die Schüler erkenntlich markiert, an einem passenden Ort positionieren.

Stationen-Laufzettel:

Der Stationen-Laufzettel ist so konzipiert, dass die Lehrkraft oder die Schüler die Stationsnummer (alternativ den Bereich) sowie den Stationsnamen eintragen. Die Kinder haken dann ab, wenn sie eine Station erledigt haben. Ein weiterer Haken wird gesetzt, wenn die Station korrigiert wurde. Dies geschieht entweder durch den Lehrer oder die Schüler selbst.

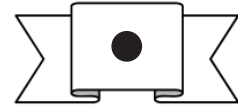
ANLEITUNG

Symbole:

Heft



Niveaustufe: leicht



Stift/Bleistift/
Buntstift



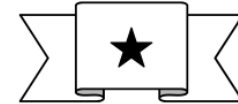
Niveaustufe: mittel



Kleber



Niveaustufe: schwer



Blatt Papier



Einzelaufgabe



Schere/
Cuttermesser



Partneraufgabe



Nach dieser kurzen Einführung wünschen Ihnen viel Spaß beim Einsatz der Materialien

Ihr Kohl-Verlag und *Hans J. Schmidt*

Weiterführende Literatur:

Simon Singh, Geheime Botschaften, München 2001

Simon Singh, Codes, München, 2004

Albrecht Beutelspacher, Geheimsprachen: Geschichte und Techniken, München, 2013

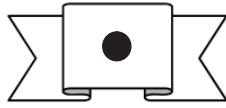
Rudolf Kippenhahn, Verschlüsselte Botschaften, Reinbek bei Hamburg, 1999

ANLEITUNG

Name: _____

Datum: _____

Niveaustufe: leicht



Station	Stationsname	erledigt ✓	korrigiert ✓

Niveaustufe: mittel



Station	Stationsname	erledigt ✓	korrigiert ✓

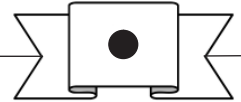
Niveaustufe: schwer



Station	Stationsname	erledigt ✓	korrigiert ✓



Station 1



Rund um Geheimschriften - ein Puzzle

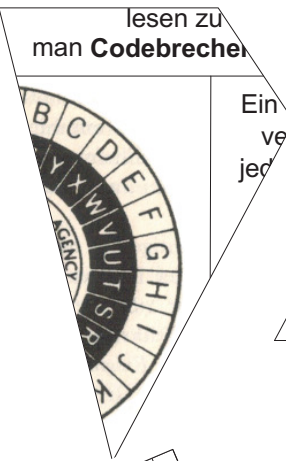
Schneidet die einzelnen Puzzleteile aus, setzt sie zusammen und klebt sie ins Heft. Es ergeben sich Begriffe, die ihr euch merken solltet.

Die Wissenschaft von der einer Mitteilung nennt man **Kryptologie** ist die Wissenschaft der Verschlüsselung in all **kryptos** (griech. geheime) **graphein** (griech. schreiben) **logos** (griech. Wort) der Sprache

Die Vorschrift „Ersetze den Buchstaben der an einer bestimmten Stelle durch den Buchstaben der an einer bestimmten Stelle“ nennt man auch **Substitution**. Lässt man die Buchstaben an den Stellen 26 • 25 • 24 • ...

Menschen, denen daran gelegen ist, geheime Nachrichten anderer ebenfalls - aus welchen Gründen auch immer - zu erhalten, nennt man **Codeknacker**. Jeder hat schon einmal versucht, eine geheime Nachricht zu knacken. Man verwendet z. B. Wörterbücher oder versteckt eine Nachricht in harmlosen Nachrichten. Es geht es darum, wie sie entschlüsselt werden kann.

Verschlüsselungsverfahren, bei dem jeder Buchstabe durch einen anderen Buchstaben oder ein Zeichen ersetzt wird, nennt man **Substitutionsverfahren**. Dabei behält die Botschaft ihre ursprüngliche Bedeutung bei.



Substitution. Dabei werden die Buchstaben an ihre jeweilige Position verschieben.

44 v. Chr.), der auch bekannt sein als **Cäsar**, Feldherr und Schriftsteller, Verschlüsselung mittels Substitution. In jeder Buchstaben seiner Nachrichten, der im Alphabet drei Stellen weiter folgte, selbst aber unverändert bleibt, nennt man **Caesarschlüssel**.

Schon im Altertum wurde eine Methode zur Versteckung von Nachrichten verwendet. In der **Steganographie** wird eine Mitteilung versteckt, indem sie in einer harmlosen Mitteilung zu halten. Das heißt, die Botschaft ist in einer harmlosen Mitteilung zu halten. Das heißt, die Botschaft ist in einer harmlosen Mitteilung zu halten.

Die Mitteilung, die zu verschlüsseln ist, nennt man **Klartext**. Er wird mit **klare** Buchstaben geschrieben. **Geheimschrift** (oder **Chiffre**) ist die verschlüsselte Mitteilung. **Entschlüsselung** (oder **Dechiffrierung**) ist die Umkehrung der Verschlüsselung. **Geheimschrift** (oder **Chiffre**) ist die verschlüsselte Mitteilung. **Entschlüsselung** (oder **Dechiffrierung**) ist die Umkehrung der Verschlüsselung.

Die Ziffern 3 • 2 • 1 = 4, 032914611 • 10²⁶ unterschiedliche Möglichkeiten. **Caesarschlüssel** (oder **Caesarschlüssel**) ist eine Methode zur Verschlüsselung von Nachrichten. Dabei werden die Buchstaben an ihre jeweilige Position verschieben. **Caesarschlüssel** (oder **Caesarschlüssel**) ist eine Methode zur Verschlüsselung von Nachrichten. Dabei werden die Buchstaben an ihre jeweilige Position verschieben.

Buchstaben (oder **Alphabet**) sind die Zeichen, die zur Verschlüsselung verwendet werden. **Geheimschrift** (oder **Chiffre**) ist die verschlüsselte Mitteilung. **Entschlüsselung** (oder **Dechiffrierung**) ist die Umkehrung der Verschlüsselung.

Verschlüsselung (oder **Kryptographie**) ist die Umkehrung der Entschlüsselung. **Geheimschrift** (oder **Chiffre**) ist die verschlüsselte Mitteilung. **Entschlüsselung** (oder **Dechiffrierung**) ist die Umkehrung der Verschlüsselung.

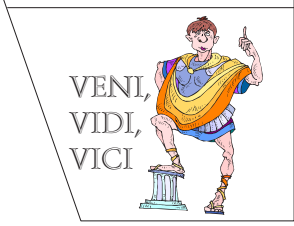
Ein **Geheimschrift** (oder **Chiffre**) ist eine Methode zur Verschlüsselung von Nachrichten. Dabei werden die Buchstaben an ihre jeweilige Position verschieben.



Die **Alphabet** (oder **Alphabet**) sind die Zeichen, die zur Verschlüsselung verwendet werden. **Geheimschrift** (oder **Chiffre**) ist die verschlüsselte Mitteilung. **Entschlüsselung** (oder **Dechiffrierung**) ist die Umkehrung der Verschlüsselung.

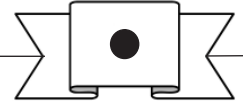
Ein Verschlüsselungsverfahren, bei dem jeder Buchstabe innerhalb der geheimen Mitteilung den Platz wechselt, nennt man **Transposition**.

Ein Verschlüsselungsverfahren, bei dem jeder Buchstabe innerhalb der geheimen Mitteilung den Platz wechselt, nennt man **Transposition**. **Geheimschrift** (oder **Chiffre**) ist die verschlüsselte Mitteilung. **Entschlüsselung** (oder **Dechiffrierung**) ist die Umkehrung der Verschlüsselung.





Station 1



Rund um Geheimschriften - ein Puzzle

Schneidet die einzelnen Puzzleteile aus, setzt sie zusammen und klebt sie ins Heft. Es ergeben sich Begriffe, die ihr euch merken solltet.

<p>Schon immer haben Menschen versucht, Mitteilungen an eine zweite Person geheim zu halten. Das kann auf unterschiedliche Weise erfolgen. Man verwendet z. B. unsichtbare Tinte oder versteckt eine Botschaft in einer harmlosen Nachricht. In der Steganographie geht es darum, wie eine Mitteilung versteckt werden kann.</p>	<p>Die Wissenschaft von der Verschlüsselung einer Mitteilung nennt man Kryptographie. Kryptologie ist die Wissenschaft von der Verschlüsselung in all ihren Formen. kryptos (griech. geheim), graphein (griech. schreiben), logos (griech. das Wort, der Sinn).</p>	
<p>Die Mitteilung, die zu verschlüsseln ist, nennt man Klartext. Er wird mit kleinen Buchstaben geschrieben. Den verschlüsselten Text schreibt man mit großen Buchstaben.</p>	<p>Menschen, denen daran gelegen ist, geheime Nachrichten anderer ebenfalls - aus welchen Gründen auch immer - lesen zu können, nennt man Codebrecher oder Codeknacker.</p>	
<p>Zu einer geheimen Mitteilung gehören mindestens zwei Personen: der Verschicker (Sender), der seine Nachricht verschlüsselt (chiffriert) und der Empfänger, der sie wieder entschlüsselt (dechiffriert).</p>		<p>Ein Verschlüsselungsverfahren, bei dem jeder Buchstabe durch einen anderen Buchstaben oder ein Zeichen ersetzt wird, nennt man Substitutionsverfahren. Dabei behalten die Buchstaben ihre jeweilige Position bei.</p>
<p>Ein Verschlüsselungsverfahren, bei dem jeder Buchstabe innerhalb der geheimen Mitteilung den Platz wechselt, selbst aber unverändert bleibt, nennt man Transposition.</p>		
<p>Gajus Julius Cäsar (100 - 44 v. Chr.), der euch bekannt sein dürfte als römischer Staatsmann, Feldherr und Schriftsteller, benutzte als Erster die Verschlüsselung mittels Substitution. Er ersetzte einfach jeden Buchstaben seiner Nachricht durch den Buchstaben, der im Alphabet drei Stellen weiter folgte</p>		
<p>Die Vorschrift „Ersetze den Buchstaben, der an einer bestimmten Stelle im Alphabet steht, durch den, der eine bestimmte Anzahl von Buchstaben später kommt“ nennt man auch Algorithmus.</p>	<p>Die Zahl, um die man die Buchstaben verschob, nennt man auch den Schlüssel. Cäsar benutzte den Schlüssel 3. Möglich sind bei der Methode des Cäsar aber 25 Schlüssel.</p>	
<p>Lässt man beliebige Umstellungen des Alphabets zu, dann ergeben sich $26 \cdot 25 \cdot 24 \cdot \dots \cdot 3 \cdot 2 \cdot 1 = 4,032914611 \cdot 10^{26}$ unterschiedliche Geheimschriften.</p>		

Stationenlernen Geheimschriften

Top Secret!

5. Digitalauflage 2023

© Kohl-Verlag, Kerpen 2015
Alle Rechte vorbehalten.

Inhalt: Hans-J. Schmidt
Umschlagbild: Sergey Nivens - fotolia.com
Grafik & Satz: Kohl-Verlag

Bestell-Nr. P11 752

ISBN: 978-3-95686-258-8

© Kohl-Verlag, Kerpen 2020. Alle Rechte vorbehalten.

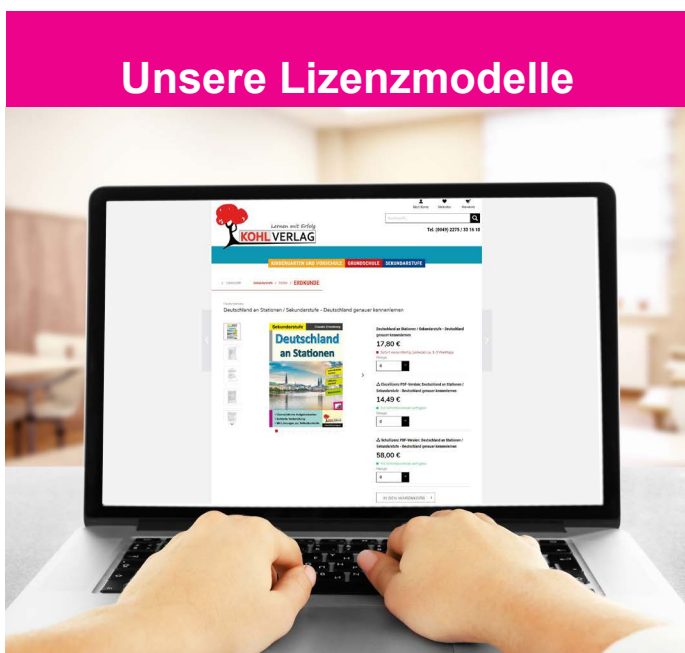
Das Werk und seine Teile sind urheberrechtlich geschützt und unterliegen dem deutschen Urheberrecht. Jede Nutzung in anderen als den gesetzlich zugelassenen Fällen bedarf der vorherigen schriftlichen Einwilligung des Verlages (§ 52 a Urhg). Weder das Werk als Ganzes noch seine Teile dürfen ohne Einwilligung des Verlages an Dritte weitergeleitet, in ein Netzwerk wie Internet oder Intranet eingestellt oder öffentlich zugänglich gemacht werden. Dies gilt auch bei einer entsprechenden Nutzung in Schulen, Hochschulen, Universitäten, Seminaren und sonstigen Einrichtungen für Lehr- und Unterrichtszwecke. Der Erwerber dieses Werkes in PDF-Format ist berechtigt, das Werk als Ganzes oder in seinen Teilen für den Gebrauch und den Einsatz zur Verwendung im eigenen Unterricht wie folgt zu nutzen:

- Die einzelnen Seiten des Werkes dürfen als Arbeitsblätter oder Folien lediglich in Klassenstärke vervielfältigt werden zur Verwendung im Einsatz des selbst gehaltenen Unterrichts.
- Einzelne Arbeitsblätter dürfen Schülern für Referate zur Verfügung gestellt und im eigenen Unterricht zu Vortragszwecken verwendet werden.
- Während des eigenen Unterrichts gemeinsam mit den Schülern mit verschiedenen Medien, z.B. am Computer, Tablet via Beamer, Whiteboard o.a. das Werk in nicht veränderter PDF-Form zu zeigen bzw. zu erarbeiten.

Jeder weitere kommerzielle Gebrauch oder die Weitergabe an Dritte, auch an andere Lehrpersonen oder pädagogische Fachkräfte mit eigenem Unterrichts- bzw. Lehrauftrag ist nicht gestattet. Jede Verwertung außerhalb des eigenen Unterrichts und der Grenzen des Urheberrechts bedarf der vorherigen schriftlichen Zustimmung des Verlages. Der Kohl-Verlag übernimmt keine Verantwortung für die Inhalte externer Links oder fremder Homepages. Jegliche Haftung für direkte oder indirekte Schäden aus Informationen dieser Quellen wird nicht übernommen.

Kohl-Verlag, Kerpen 2020

Unsere Lizenzmodelle



Der vorliegende Band ist eine PDF-Einzellizenz

Sie wollen unsere Kopiervorlagen auch digital nutzen? Kein Problem – fast das gesamte KOHL-Sortiment ist auch sofort als PDF-Download erhältlich! Wir haben verschiedene Lizenzmodelle zur Auswahl:



	Print-Version	PDF-Einzellizenz	PDF-Schullizenz	Kombipaket Print & PDF-Einzellizenz	Kombipaket Print & PDF-Schullizenz
Unbefristete Nutzung der Materialien	X	X	X	X	X
Vervielfältigung, Weitergabe und Einsatz der Materialien im eigenen Unterricht	X	X	X	X	X
Nutzung der Materialien durch alle Lehrkräfte des Kollegiums an der lizenzierten Schule			X		X
Einstellen des Materials im Intranet oder Schulserver der Institution			X		X

Die erweiterten Lizenzmodelle zu diesem Titel sind jederzeit im Online-Shop unter www.kohlverlag.de erhältlich.

SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Stationenlernen Geheimschriften - TOP SECRET

Das komplette Material finden Sie hier:

School-Scout.de

