**UV 6.1: Detektivarbeit – Auseinandersetzung mit verschiedenen Verfahren zur Codierung und Verschlüsselung sowie deren Anwendung (ca. 6 - 7 Ustd.)**

|  |  |
| --- | --- |
| **Inhaltsfeld**  **Inhaltliche Schwerpunkte** | **Übergeordnete Kompetenzerwartungen** |
| * Information und Daten * Daten und ihre Codierung * Verschlüsselungsverfahren * Algorithmen * Algorithmen und algorithmische Grundkonzepte * Informatik Mensch und Gesellschaft * Datensicherheit und Sicherheitsregeln | * Argumentieren (A) * formulieren Fragen zu einfachen informatischen Sachverhalten * äußern Vermutungen zu informatischen Sachverhalten auf der Basis von Alltagsvorstellungen oder Vorwissen * Modellieren und Implementieren (MI) * erstellen informatische Modelle zu gegebenen Sachverhalten * Darstellen und Interpretieren (DI) * beschreiben einfache Darstellungen von informatischen Sachverhalten * stellen informatische Sachverhalte in geeigneter Form dar * interpretieren informatische Darstellungen * Kommunizieren und Kooperieren (KK) * beschreiben einfache informatische Sachverhalte unter Verwendung von Fachbegriffen sachgerecht * *anstelle der vorherigen KE: erläutern informatische Sachverhalte unter Verwendung von Fachbegriffen sachgerecht* * strukturieren gemeinsam eine Lösung für ein informatisches Problem * dokumentieren gemeinsam ihren Arbeitsprozess und ihre Ergebnisse auch mithilfe digitaler Werkzeuge |
| **Weitere Hinweise, Vereinbarungen und Absprachen:**  … zur Vernetzung:   * Informationen aus Daten zu erhalten und diese zu entschlüsseln, spielt im Unterrichtsverlauf in Informatik immer wieder eine Rolle, z. B. in dem Unterrichtsvorhaben „*Codierungen zum Austausch und zur Verarbeitung von Nachrichten“* (UV 5.3)   … zu Synergien:   * Zusammenarbeit mit dem Fach Deutsch, Lesen des Buches Kalle Blomquist (Räubersprache); Geschichte, Mathematik | |

**Vorhabenbezogenen Konkretisierung:**

Das Unterrichtsvorhaben steht am Anfang der Klasse 6 und nutzt das Unterrichtsvorhaben „Information und Daten“ als Grundlage. Angelegt ist das Unterrichtsvorhaben im Sinne eines Leitprogramms, in dem an das Binärsystem als Codierung angeknüpft wird und verschiedene Arten der Verschlüsselung erarbeitet werden. Die Verfahren sind z.T. dem Spioncamp der Uni-Wuppertal entnommen und sind Teil eines Stationenlernens.

Der Einstieg in die Reihe kann durch ein kurzes Warm-up zum Binärsystem erfolgen. Daran anknüpfend kann die Übersicht der geplanten Stunden transparent gemacht werden und der Bezug zum Binärsystem als Codierung thematisiert werden.

**Fokussierung der inhaltlichen Schwerpunkte:**

* Die „Räubersprache“ zu Kalle Blomquist, in der in einem Wort nach dem Konsonanten der Buchstabe o eingesetzt und der Konsonant selbst wiederholt wird. Aus z.B. Schule wird dann Soscochohulole. Dies wird in der Informatik als Steganographie bezeichnet (die Buchstaben bleiben was sie sind, man erkennt aber die nicht, wo die Nachricht ist).
* Die Gartenzaun-Verschlüsselung und das Pflügen, bei denen zuerst durch Anordnen und dann durch Neuordnen eine Nachricht verschlüsseln werden kann, welche im Bereich der Transposition (die Buchstaben bleiben was sie sind, aber nicht wo sie sind, siehe Abb1) zu verorten sind.
* Optional: Die Caesar-Verschlüsselung als Beispiel aus dem Bereich der Substitution (die Buchstaben bleiben, wo sie sind, aber nicht was sie sind, vgl. weitere Ausführungen)

| **Sequenzierung:**  ***Fragestellungen*** | **Kompetenzerwartungen des Kernlehrplans**  Die Schülerinnen und Schüler können | **Didaktisch-methodische Anmerkungen und Empfehlungen** |
| --- | --- | --- |
| *Wer kann das lesen? Einführung in die Steganografie am Beispiel der „Räubersprache“ und der Wiederholung der Codierung*  (ca. 2 Ustd.) | * nennen Beispiele für die Codierung von Daten aus ihrer Erfahrungswelt (DI) * codieren und decodieren Daten unter Verwendung des Binärsystems (MI) * erläutern Einheiten von Datenmengen (A/KK) * führen Handlungsvorschriften schrittweise aus (MI) | Visualisierung durch die PPP S 1 bis 7 (Seite 6 mögliche Differenzierung) zur Wiederholung und als Impuls zur Themenfindung der kommenden Reihe  Bearbeitung AB 1 „Noch fit?“  Abschließende Fragestellung:  Reicht das Binärsystem aus, um „vertraute“ Nachrichten zu verschicken.  Klärung der Begriffe:  Sender, Empfänger, Klartext, Geheimtext  Einstieg in die Steganografie mit Textausschnitt zu Kalle Blomquist (s.PPP S. 8 bis 11)  Ein Bild, das Text enthält.  Automatisch generierte Beschreibung  Bearbeitung AB 2 „Werde zum Meisterdetektiv“  Abspielen des Films von INF-schule bis ca. 01:40 min  Ein Bild, das drinnen enthält.  Automatisch generierte Beschreibung  bei Bedarf auch länger |
| *Was bringt der Einsatz eines Schlüssels? – Erkundung des Transpositionverfahrens am Beispiel der Gartenzaunmethode (und/oder des Pflügens)*  (ca. 3 Ustd.) | * erläutern ein einfaches Transpositionsverfahren als Möglichkeit der Verschlüsselung (DI) (MKR 1.4) * führen Handlungsvorschriften schrittweise aus (MI) * beschreiben Maßnahmen zum Schutz von Daten mithilfe von Informatiksystemen (A) * *vergleichen verschiedene Verschlüsselungsverfahren unter Berücksichtigung von Sicherheitsaspekten (DI)* (MKR 1.4) | Eines der beiden Verfahren kennenlernen und anwenden  Teil 1: Die Gartenzaun - Verschlüsselung  Material: AB 3 und PPP S. 13 bis 15  Teil 2: Pflügen  Material AB 4 und PPP S. 16 bis 18  *Vergleichen beider Verfahren* |
|  |  |  |
| Zusatzmaterial zur Substitution  Wie überbrachte Caesar seine geheimen Nachrichten?  (ca. 2 Ustd.) | * führen Handlungsvorschriften schrittweise aus (MI) * beschreiben Maßnahmen zum Schutz von Daten mithilfe von Informatiksystemen (A) * *vergleichen verschiedene Verschlüsselungsverfahren unter Berücksichtigung von Sicherheitsaspekten (DI)* | Die Caesar - Verschlüsselung  (Substitutionsverfahren)  Verfahren kennenlernen und anwenden  Vergleichen der Verfahren (siehe AB 5)  Material PPP S. 19 bis 20  Hinweis: AB muss je nach behandelten Verfahren bei Aufgabe 3 angepasst werden |

**Material:**

| **Nr.** | **URL / Quellenangabe** | **Kurzbeschreibung des Inhalts / der Quelle** |
| --- | --- | --- |
| 1 | https://inf-schule.de/kryptologie | Video zum Einstieg in das Unterrichtsvorhaben |
| 2 | https://ddi.uni-wuppertal.de/www-madin//material/spioncamp.html | Material zu den Inhalten zur Transposition und Substitution.  Wenn möglich sollte die Caesar-Scheibe von den SuS selbst hergestellt werden |
| 3 | https://schuelerlabor.informatik.rwth-aachen.de/module/schatzsuche | Alternative zum UV, der PC ist hier ein Voraussetzung |

letzter Zugriff auf die URL: 15.01.2022

*[Diese Liste/Diese Veröffentlichung/Dieses Angebot enthält Links zu externen Websites Dritter, auf deren Inhalte QUA-LiS NRW keinen Einfluss hat. Dementsprechend obliegt die Einhaltung der datenschutzrechtlichen Regelungen dem jeweiligen Anbieter bzw. Betreiber. Im Sinne der gesetzlichen Gesamtverantwortung für den Datenschutz an Schulen prüfen Schulleitungen daher vor einem Einsatz der genannten Quellen eigenverantwortlich, inwieweit und unter welchen Bedingungen die Nutzung der genannten Quellen für den beabsichtigten Zweck datenschutzrechtskonform möglich ist. Ggf. resultiert aus einer solchen Prüfung im konkreten Fall, dass die allgemeine Nutzung weitestgehend nur auf freiwilliger Basis möglich ist, d.h. Schülerinnen und Schüler (oder deren Erziehungsberechtige) bzw. Lehrerinnen und Lehrer nicht oder nur eingeschränkt zur Nutzung verpflichtet werden können.]*

**Kryptologie – Noch fit? AB1**

Aufgabe 1: Bits und Bytes



Info:

Informatiksysteme speichern und verarbeiten alle Daten in Bits. Dies ist die kleinste Speichereinheit. Größere Einheiten sind z.B. Megabyte oder auch Gigabyte.

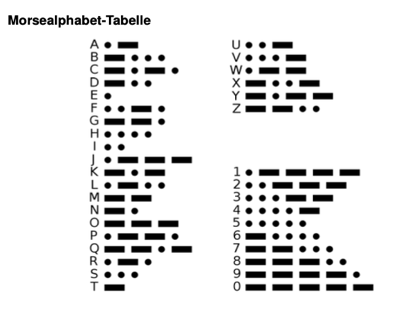
Gib die nächstkleinere Einheit an.

1 Byte (B) = 8 \_\_\_\_\_\_\_\_\_\_

1 Kilobyte (KB) =

1 Megabyte (MB) =

1 Gigabyte (GB) =



https://ddi.uni-wuppertal.de/www-madin/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf

CC BY-NC-SA

Aufgabe 2: Das Morsealphabet

Info:

1832 erfand Samuel Morse einen Apparat, mit dem Nachrichten über große Entfernungen übermittelt werden konnten. Es konnten allerdings keine gesprochenen Nachrichten übertragen werden, sondern nur lange oder kurze Signaltöne.

1. Schreibe deinen Namen im Morsecode.
2. Notiere, was die folgenden Zeichen bedeuten:

\_ . \_ . \_ . \_ . \_ \_ . \_ \_ . \_ \_ \_ \_ . \_ . . \_ \_ \_ \_ \_ . . . .

Aufgabe 3: Binärzahlen codieren und decodieren

Info:

Das Binärsystem ist ein Zahlsystem mit genau zwei Ziffern 0 und 1.   
Jede Zahl hat im Binärsystem eine eindeutige Codierung.

Die folgende Tabelle kann dir beim Codieren und Decodieren helfen.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|  |  |  |  |  |  |  |  |

1. Wie sehen die folgenden Zahlen im Binärcode aus?

32, 78, 129 und 256

1. Decodiere die folgenden Binärzahlen.

11001, 110100, 01001100 und 111111

1. Sprinteraufgabe:   
   Beschreibe die Gemeinsamkeit aller „durch 2 teilbaren“ Binärzahlen.

**Kryptologie – Aus dem Leben eines Meisterdetektivs! – AB 2**

Klassenfahrt oder 5 Tage ohne das Smartphone

Für Lea, Emre und Paul geht es in wenigen Wochen auf Klassenfahrt an die Ostsee. Alle drei freuen sich schon sehr auf die „elternfreie Zeit“. Leider teilt die Klassenlehrerin Frau Wagner kurz vor der Abfahrt der Klasse mit, dass die Klassenfahrt nicht nur elternfrei, sondern auch handyfrei sein wird. Smartphones und ähnliche elektrischen Geräte müssen zu Hause bleiben.

Das Problem:   
Wie tauschen die drei auf der Klassenfahrt vertrauliche Mitteilungen aus, die nicht jeder lesen kann?

Emre schlägt folgendes vor:

„Wir machen es wie der Meisterdetektiv Kalle Blomquist aus Astrid Lindgrens Romanen!   
In der „Räubersprache“ zu Kalle Blomquist wird in einem Wort nach einem Konsonanten der Buchstabe o eingesetzt und der Konsonant selbst wiederholt. So können wir unsere geheimen Nachrichten einfach auf kleine Zettel aufschreiben, diese austauschen und nur wir drei können sie lesen. Frau Wagner versteht diese dann bestimmt nicht. “

Emre schreibt für alle das folgende Beispiel auf:

So wird aus Kalle »Kok a lol lol e«

und aus

Emre »E mom ror e «.

Aufgabe 1: Wandle das Wort Schule in die Räubersprache um.

Wichtig: Jeder Konsonant wird verdoppelt und ein o dazwischen eingefügt.

S \_ \_ C \_ \_ H \_ \_ \_ L \_ \_ \_



Info:

Dieses Verfahren wird in der Informatik als **Steganographie** bezeichnet.

Die Buchstaben bleiben was sie sind, man erkennt aber nicht, wo die Nachricht ist.

Aufgabe 2: a) Wie sehen die Vornamen von Paul und Lea in der Räubersprache aus.

Paul: \_ \_ \_ \_ \_ \_ \_ \_

Lea: **\_ \_ \_ \_ \_**

b) Wende das Verfahren auf deinen Vornamen an.

Aufgabe 3: Decodiere die folgende Nachricht, die Paul an Emre schreibt.

ToT rer e fef fef e non u non sos hoh e u tot e A bob e non dod a non dod e ror a lol tot e non E i coc hoh e

Aufgabe 4: Beantworte folgende Fragen zuerst in Einzelarbeit und stelle diese dann im Plenum vor.

Mach dir dazu Notizen.

1. Ist das Verfahren des Meisterdetektives ein sicheres Verfahren?   
   Begründe deine Antwort.
2. Kennst du Verfahren zur sicheren Übermittlung von (geheimen) Nachrichten aus deinem Alltag?
3. Sprinteraufgabe:  
   Hast du eine Idee, das Verfahren sicherer zu machen?

**Kryptologie – Der Blick über den Gartenzaun – AB 3**

Kannst du den folgenden Geheimtext entschlüsseln?

GEUATNANRZ

Verschlüsselt wurde er mit der Gartenzaun-Verschlüsselung.

Dies bedeutet, dass der Klartext in eine Tabelle mit einer bestimmten Anzahl an Zeilen und Spalten im „Zick-Zack“ eingetragen wird.

Unten siehst du, wie das Wort „INFORMATIK“ verschlüsselt wird.

Die Anzahl der Spalten ist die Anzahl der Buchstaben des Klartextes.

Die Anzahl der Zeilen ist der sogenannte Schlüssel.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I |  |  |  |  |  | A |  |  |  |
|  | N |  |  |  | M |  | T |  |  |
|  |  | F |  | R |  |  |  | I |  |
|  |  |  | O |  |  |  |  |  | K |

Aus dem Wort „INFORMATIK“ wird der Geheimtext „IANMTFRIOK“.

Der Schlüssel ist 4, da die Tabelle aus 4 Zeilen besteht.



Info:

Dieses Verfahren wird in der Informatik als **Transposition** bezeichnet.

Die Buchstaben bleiben was sie sind, aber nicht wo sie sind.

Aufgabe 1: Verschlüssel das Wort DETEKTIV mit der Gartenzaun-Verschlüsselung. Der Schlüssel ist 2.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Aufgabe 2: Entschlüssel den o.g. Geheimtext „GEUATNANRZ“. Der Schlüssel ist 3.

Tipp:

Zähle zuerst die Buchstaben, die im Geheimtext vorhanden sind und zeichne dann die Tabelle mit zehn Spalten und 3 Zeilen.

Aufgabe 3: Verschlüssel eine kurze Nachricht (max. 12 Buchstaben) mithilfe der Gartenzaun-Verschlüsselung in Einzelarbeit. Tausche dann den Geheimtext mit deinem Partner aus.

Könnt ihr die Nachrichten entschlüsseln?

Ein Bild, das draußen, Feld enthält.

Automatisch generierte Beschreibung**Kryptologie – Ab auf das Feld -Pflügen – AB 4**

Ein weiteres Transpositionsverfahren ist das Pflügen.

Dies erinnert an die Entstehung von Pflugfurchen auf einem Feld.

Bild: https://pixabay.com/de/

Das Pflügen zeigt dir, wie man durch Anordnen und Neuordnen von Buchstaben eine Nachricht verschlüsseln kann. Auch bei diesem Verfahren nutzt du einen Schlüssel.   
Dieser ist beim Pflügen die Anzahl der Spalten.



Bei der **Transposition** bleiben die Buchstaben bleiben was sie sind, aber nicht wo sie sind.

Der Algorithmus zum Verschlüsseln funktioniert wie folgt:

1. Schreibe zuerst deinen Text auf:   
   DIES IST EINE GEHEIME NACHRICHT
2. Lege jetzt den Schlüssel fest:  
   Der Schlüssel ist 5, also brauchst du eine Tabelle mit 5 Spalten.
3. Zeichne die Tabelle mit 5 Spalten.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| D | I | E | S | I |
| S | T | E | I | N |
| E | G | E | H | E |
| I | M | E | N | A |
| C | H | R | I | C |
| H | T | X | X | X |

1. Trage deine Nachricht in die Tabelle ein.
2. Fülle die nicht ausgefüllten Felder mit X auf. Hier sind es drei zusätzliche Xe.
3. Der verschlüsselte Text entsteht, indem du nun die letzte Spalte von unten nach oben aufschreibst, danach die vorletzte Spalte von oben nach unten und so weiter.   
   Ein Bild, das Text, Kreuzworträtsel enthält.

   Automatisch generierte Beschreibung  
   XCAENISIHNIXXREEEEITGMHTHCIESD

Aufgabe 1: a) Verschlüssel das Wort DETEKTIVARBEIT mit der Pflügen-Verschlüsselung.   
Der Schlüssel ist 3.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

b) Sprinteraufgabe:

In der vorgegebenen Tabelle ist eine Zeile zu viel gezeichnet worden. Wie kannst du das verhindern? Formuliere dazu einen Tipp für deine Mitschülerinnen und Mitschüler!

Aufgabe 2: Entschlüssel den Geheimtext „(hier den Namen der eigenen Schule eintragen)“.

Der Schlüssel ist 6.

(Beispiel hier AlbertEinsteinGesamtschule

also: XUAETRTSHXXCESEBNGSXETNILAEIML)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Sprinteraufgabe:

Kannst du den folgenden Text ohne bekannten Schlüssel entschlüsseln?

EETEENZßHNILITIEAEIMLWHKM  
  
Du weißt nur, dass das „Pflügen“ als Verschlüsselungsverfahren benutzt wurde.

Tipp:Die Anzahl der Buchstaben ist hier durch die zuvor festgelegte Anzahl von Buchstaben pro Zeile teilbar.

**Kryptologie – Zu Gast bei Julius Caesar\* – AB 5 (Optional) Differenzierung**

Der römische Feldherr Julius Caesar (100 bis 44 v.Chr.) verschlüsselte seine geheimen Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte.   
Dabei werden die Buchstaben im Klartext immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt.   
Diese Anzahl der Stellen heißt **Caesar-Schlüssel**.

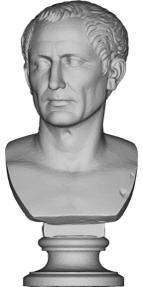


Bild: https://pixabay.com/de/



Info:

Dieses Verfahren wird in der Informatik als **Substitution** bezeichnet.

Die Buchstaben bleiben wo sie sind, aber nicht was sie sind.

Bei dem Caesar-Schlüssel 2 nimmt man immer den Buchstaben, der im Alphabet zwei Stellen weiter rechts steht.

Verschlüsselt man das Wort „Informatik“ kommt also folgender Geheimtext heraus:

KPHQTOCVKM

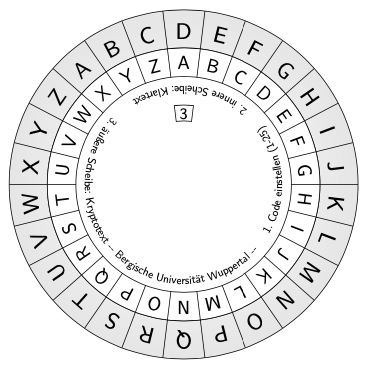
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Klartext | A | B | C | D | E | F | G | H | I | J | K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

Hinweis: aus I wird K, aus N wird P, aus F wird H, usw.

Damit nicht immer die beiden gegeneinander verschobenen Alphabete aufgeschrieben werden müssen, kann auch eine sogenannte Chiffrierscheibe benutzt werden.

In der Abbildung ist wie im Beispiel der Schlüssel 3 eingestellt.

Mit der Scheibe kannst du nun sowohl Texte verschlüsseln als auch entschlüsseln.   
Möchtest du verschlüsseln, dann suchst du den Buchstaben auf der inneren Scheibe und schreibst den entsprechenden Buchstaben auf der äußeren Scheibe auf.   
Entschlüsseln geht entsprechend umgekehrt: Hier suchst du den Buchstaben außen und schreibst den entsprechenden Buchstaben auf der inneren Scheibe auf.



https://ddi.uni-wuppertal.de/www-madin/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf

CC BY-NC-SA

Aufgabe 1: Verschlüssel den Text mit dem Caesar-Schlüssel 7.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Entsperren mit einfarbiger Füllung | S | C | H | U | L | E | M | A | C | H | T | S | P | A | S | S |
| Sperren mit einfarbiger Füllung |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Aufgabe 2: Lea schreibt an Emre eine Test-Nachricht mit folgendem Text:

**AIVOERRHEWPIWIR ?**

Emre weiß nur, dass der Schlüssel 4 ist. Der Klartext wurde mit der Caesar-Verschlüsselung verschlüsselt. Entschlüssel die folgende Nachricht.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sperren mit einfarbiger Füllung | A | I | V | O | E | R | R | H | E | W | P | I | W | I | R | ? |
| Entsperren mit einfarbiger Füllung |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Sprinteraufgabe: a) Inzwischen kennst du verschieden Verfahren zur Codierung und Verschlüsselung.

Die folgende Tabelle gibt dir einen Überblick.

Trage den passenden Fachbegriff -wie im ersten Beispiel- für das entsprechende

Verfahren ein.



Tipp: Alle Informationen dazu findest du auf den Arbeitsblättern 1 bis 4 unter Info

|  |  |  |  |
| --- | --- | --- | --- |
| Verfahren | Fachbegriff | mit Schlüssel? | Sicherheit |
| Morsealphabet | Codierung | ohne | Stern SilhouetteStern SilhouetteStern SilhouetteStern Silhouette |
| Räubersprache |  |  | Stern SilhouetteStern SilhouetteStern SilhouetteStern Silhouette |
| Gartenzaun |  |  | Stern SilhouetteStern SilhouetteStern SilhouetteStern Silhouette |
| Pflügen |  |  | Stern SilhouetteStern SilhouetteStern SilhouetteStern Silhouette |
| Caesar |  |  | Stern SilhouetteStern SilhouetteStern SilhouetteStern Silhouette |

Schätze in der Spalte „Sicherheit“ ein, wie schwer es ist, das Verfahren zu „knacken“.

Male die Sterne entsprechend aus:

: sehr leicht  : eher schwer

: eher leicht  : sehr schwer

1. Bergründe deine Antwort:

|  |  |
| --- | --- |
| Morsealphabet: |  |
|  |  |
| Räubersprache: |  |
|  |  |
| Gartenzaunverschlüsselung: |  |
|  |  |
| Pflügen: |  |
|  |  |
| Caesarverschlüsselung: |  |
|  |  |

1. Schon fertig? Dann tausche dich mit deinem Partner aus?

**Kryptologie –Lösungen**

AB1: A1: 8 Bit, 1000 Byte, 1000 Kilobyte, 1000 Megabyte

A2: a. individuelle Lsg.

b. Kryptologie

A3: a. 100000 / 1001110 / 10000001 / 100000000

b. 25 / 52 / 76 / 63

c. 0 die letzte Ziffer

AB2: A1: SOS COC HOH U LOL E

A2: a. POP A U LOL / LOL E A

b. individuelle Lsg.

A3: Treffen uns heute Abend an der alten Eiche

A4: a. unsicher, Begründung individuell

b. individuelle Lsg.

c. individuelle Lsg., ggf abwechselnder Tausch der Vokale, …

AB3: A1: DTKIEETV

A2: Gartenzaun

A3: individuelle Lsg.

AB4: A1: a. XEATTEKVBTIRIED

b. Anzahl der Buchstaben geteilt durch den Schlüssel = Anzahl der Zeilen (falls Dezimalzahl, runden auf die nächstgrößere ganze Zahl)

A2: individuelle Lsg

A3: Meine Katze heißt Wilhelmine

AB5: A1: ZJOBSLTHJOAZWHZZ

A2: Wer kann das lesen

A3: Codierung/ohne, Codierung/ohne, Transposition/mit, Transposition/mit, Substitution/mit

Vergleich: individuelle Lsg. Ergebnis sollte sein: alle unsicher und (sehr) leicht zu knacken