An dieser Seite wird gerade gearbeitet.

Die Caesarverschlüsselung als einfache Geheimschrift

	**Die Caesarverschlüsselung als einfache Geheimschrift (Kurzbeschreibung)**
Idee	In dieser Einheit lernen die Kinder mit der Caesarverschlüsselung ein einfaches Verfahren kennen, mit dem man Daten verschlüsseln kann. Sie wenden das Verfahren auf das Morsen an, indem sie verschlüsselte Botschaften verschicken.
Organisatorisches	Schulform: Grundschule Klassenstufe: 3-4 Zeitumfang: ca. 60 Minuten
Curriculares Umfeld	**Bildungsstandards im Primarbereich (GI)** - Die Schüler*innen nutzen und entwickeln Vereinbarungen, um Daten zu verschlüsseln und entschlüsseln (S.21) - Die Schüler*innen nutzen und entwickeln Vereinbarungen zur Übermittlung von Nachrichten (S.13) **Orientierungsrahmen Medienbildung** - Die Schüler:innen entwickeln ein Bewusstsein für Datensicherheit, Datenschutz und Datenmissbrauch, um ihre Privatssphäre durch geeignete Maßnahmen zu schützen (4.2) - Die Schüler:innen beurteilen digitale Werkzeuge im Hinblick auf den Datenschutz und mögliche gesellschaftliche Auswirkungen (5.3)
Voraussetzungen	Lehrer:innen wenden die Begriffe Information, Daten, Codierung und Verschlüsselung sicher an. Schüler:innen können mit einiger Sicherheit einfache Worte lesen und schreiben. Schüler:innen ist die Abhörproblematik unverschlüsselt übertragener Daten bewusst.
Ablauf	Die Schüler:innen verschlüsseln einfache Wörter und Sätze mit der Caesarverschlüsselung. Sie üben das Verschlüsseln und Entschlüsseln in Partnerarbeit. Wörter als einfache Informationen werden danach über eine größere Distanz mit dem Morsealphabet verschlüsselt übertragen.
fachlicher Hintergrund	Die Caesarverschlüsselung ist ein sehr einfaches Verfahren, um Daten so zu übertragen, dass sie nicht auf den ersten Blick man Menschen mitgelesen werden können. Für einen Computer stellt die Caesarverschlüsselung keine Schwierigkeit dar. Verschlüsselte Verbindungen auf hohem Niveau erkennt man im Internet an dem „s“ hinter der Protokollbezeichnung (http**s**, ftp**s**)

	**Die Caesarverschlüsselung als einfache Geheimschrift (Kurzbeschreibung)**
Materialien	- PDF-Export dieser Seite - Webseite zum Verschlüsseln und Entschlüsseln der Caesarverschlüsselung **Zum Ausdrucken:** - Schülermaterial zur Caesarverschlüsselung , Quelle: (it2school) **Hinweis:** Für eine Seite werden pro Schüler:in zusätzlich festes Papier (150-200g/m²) und Paketklammern benötigt!

Ausführliche Beschreibung

	**Die Caesarverschlüsselung als einfache Geheimschrift (Ausführliche Beschreibung)**
Einordnung	Wenn Daten oder Informationen über größere Distanzen übertragen werden, können Dritte diese Daten an verschiedenen Stellen im Internet mitlesen. Dadurch dass z.B. das Morsealphabet weltweit bekannt ist, kann man es aber sehr leicht „abhören“. Mit der Caesarverschlüsselung lernen die Kinder ein einfaches Verfahren zur „Absicherung“ von Daten kennen. Die Caesarverschlüsselung ist extrem unsicher und kann von Computern und geübten Menschen leicht entschlüsselt werden. Das wird anhand einer Webseite gezeigt. In einer Reflexion kann das problematisiert und daraug hingewiesen werden, dass Verschlüsselung im Internet mit viel sicheren Methoden funktioniert.

	**Die Caesarverschlüsselung als einfache Geheimschrift (Ausführliche Beschreibung)**
Spielvoraussetzungen	- ein wenig Platz - eine Paketklammer für jede/n Schüler:in - das ausgedruckte Material zu Vertiefung (die Seite mit der Bastelvorlage auf dickem Papier ausgedruckt) - Gegenstände zum Übertragen (z.B. die weißen und schwarzen Karten aus der Einheit mit den Pixelgrafiken
Ablauf	Als Einleitung wird der Film zum Thema Datenübertragung gezeigt. Als Vertiefung dient das ausgedruckte Material zum Morsealphabet . Es sollten die Begriffe „Information“ (= Wort), „Daten“ (= codierte Worte) und „Codierung“ (= Umwandlungsvorschrift) auf das Morsealphabet übertragen/darauf angewendet werden. Anschließend wird von einer Kleingruppe zu einer Kleingruppe ein Wort „gemorst“. Das kann z.B. durch weiße (kurz) und schwarze Karten (lang) geschehen oder durch andere im Material verwendete Gegenstände oder Verfahren (Fähnchen / Lichtzeichen). Das Morsen kann auch über einen Stromkreis mit Lämpchen und Schalter passieren, sodass in dieser Einheit Querbezüge möglich werden. Einer sendet und alle aus der Gruppe notieren die Nachricht. Dabei kann die angegebene Webseite beim Codieren/Decodieren helfen, wenn die Worte länger werden.
Optionen/Erweiterungen	Beim Morsen sind beliebige „Sender“ möglich. Da das Morsealphabet standardisiert ist, klappt das Aufschreiben der Worte - abgesehen von Übertragungsfehlern - eigentlich immer.
Erfahrungen	Es ist wichtig, zunächst mit Buchstaben zu beginnen und sich dann über einfache Wörter bis hin zu kleinen Sätzen vorzuarbeiten. Für Schüler:innen, die sich mit dem Schreiben und Lesen schwertun, kann eine Codierungs-/Decodierungshilfe in Form der angegebenen Webseite hilfreich sein. Sie schreiben z.B. beim Empfangen nur die Punkte und Striche auf und lassen die dann im Netz „Übersetzen“.
Reflexion	Am Schluss sollte die Verschlüsselungsproblematik erarbeitet werden. Leitfragen könnten sein: - Was ist der Vorteil am Morsen gegenüber unseren eigenen bisherigen Datenübertragungsverfahren?? - Was kann beim Morsen alles schiefgehen? - Welche Informationen kann man morsen und welchen nicht? (Klappt das auch mit Musik?) - Welche Informationen würdet ihr morsen und welche nicht? - Würdet ihr nachts mit einer Taschelampe eurem Freund in der Stadt morsen, was euch heute peinliches passiert ist?

From:
https://wiki.mzclp.de/ - **Fortbildungswiki des Medienzentrums Cloppenburg**

Permanent link:
https://wiki.mzclp.de/doku.php?id=material:infgsnds-caesar&rev=1590483195

Last update: **2020/05/26 10:53**