Transportverschlüsselung

Caesarverschlüsselung als ein symmetrisches Verschlüsselungsverfahren

Bei einer bekannten Codierung können Daten sehr leicht auf dem Transportweg abgehört werden. So könnten Morsezeichen, die nachts per Licht übertragen werden z.B. von Feinden sehr leicht mitgehört werden. Man kann die Daten durch eine Verschlüsselung schützen. Eine sehr einfache (und unsichere Methode) zur Verschlüsselung ist die

Caesarverschlüsselung

.



Aufgabe 1 (Partnerarbeit) - Mit der Caesar-Verschlüsselung üben
Erledigt zusammen die Aufgaben in dem Material zur

Caesarverschlüsselung

. Eine große Hilfe kann dabei eine Textverarbeitung sein, mit der ihr Klaralphabet und Geheimalphabet wie im Material untereinanderschreibt. Die Größe der Verschiebung dürft ihr selbst bestimmen.



Aufgabe 2 (Partnerarbeit) - Verschlüsselte Nachrichten morsen
Überlege dir einen kurzen Satz aus drei kurzen Worten. Übertrage diesen diesmal verschlüsselt an deine(n) Partner/in. Es ist sehr wichtig, dass du diesem die von dir gewählte Verschiebung mitteilst.

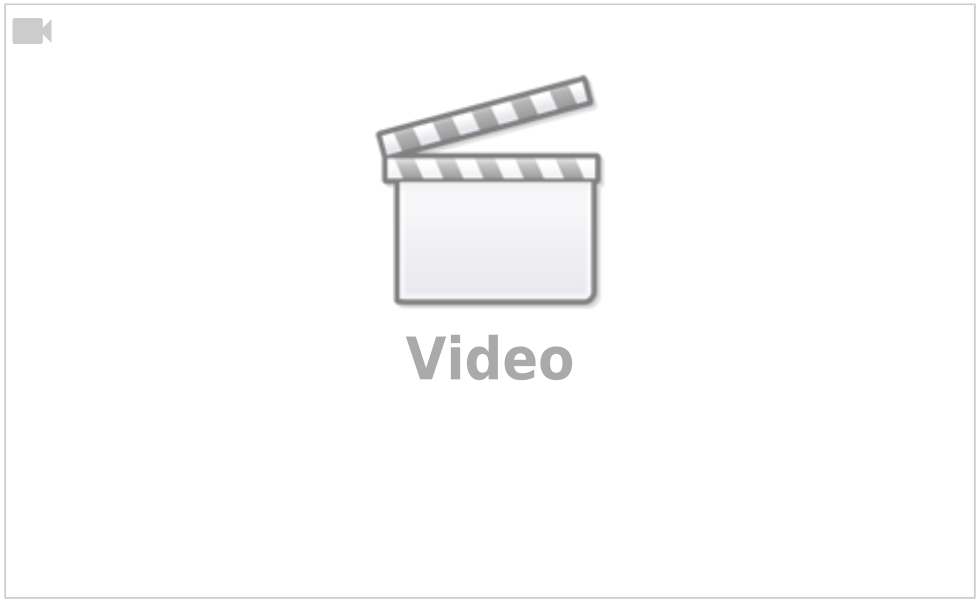
Die Caesarverschlüsselung ist sehr leicht zu knacken. Diese Material zeigt, wie es geht.



Aufgabe 3 (Gruppenarbeit - Angriffsprinzip auf die Caesarverschlüsselung erklären
Erlärt mit einer kleinen Präsentation, wie der Angriff auf die Caesarverschlüsselung funktioniert.

Die asymmetrische Verschlüsselung

Schaue dir dieses Video an:



Aufgabe 4 (Partnerarbeit) - Fragen zum Video beantworten

1. Was ist das Problem an der symmetrischen Verschlüsselung?
2. Was ist der Unterschied zwischen einem öffentlichen und einem privaten Schlüssel?
3. Wann verschlüsselt man mit dem öffentlichen und wann mit dem privaten Schlüssel?
4. Warum stellt die asymmetrische Verschlüsselung einen sicheren Weg zur Übertragung eines symmetrischen Schlüssels dar?

Aufgabe 5 (Partnerarbeit) - Fragen zum Video beantworten
Erstelle eine Grafik, die das Prinzip der asymmetrischen Verschlüsselung verdeutlicht.

From:
https://schule.riecken.de/ - **Unterrichtswiki**

Permanent link:
https://schule.riecken.de/doku.php?id=informatik:datenspuren:verschluesselung

Last update: **2024/07/15 15:31**