Einführung in die Kryptologie

Die Skytale

Schon vor 2500 Jahren wurden im militärischen Umfeld geheime Botschaften übermittelt, beispielsweise in Form der Skytale - die Verschlüsselung beruht auf einem **Transpositionsverfahren**.

1)

(A1)

(A) Recherchiere zur **Skytale** und notiere den historischen Kontext.

(B) Beschreibe das Verschlüsselungsverfahren: Was muss der Absender tun, um eine Nachricht zu **verschlüsseln**, was muss der Empfänger tun, um die Nachricht zu **entschlüsseln**? Nenne den **Schlüssel**, den Sender und Empfänger kennen müssen.

(C) Bewerte die Sicherheit des Verfahrens.

(D) Wie könnte die Verschlüsselung sicherer gemacht werden? Mache Vorschläge.

Grundbegriffe

Die folgende Grafik ist eine Darstellung einer Miniwelt, welche die Situation zur Untersuchung verschlüsselter Kommunikation gut darstellt. Alice möchte mit Bob über einen unsicheren Kanal (z.B. das Internet) kommunizieren, ohne dass Eve (Eavesdropping, „abhören“, manchmal auch Mallory) diese Kommunikation verstehen kann.

Die Nachricht liegt beim Sender zunächst als **Klartext** vor und wird von diesem mit Hilfe eines **Schlüssels verschlüsselt** und damit in einen **Geheimtext** umgewandelt. Dieser Geheimtext lässt sich nur von einer Person zurück in den Klartext **entschlüsseln**, die ihrerseits über einen passenden **Schlüssel** verfügt.

Wenn Eve in den Besitz des Geheimtexts kommt, kann sie versuchen, durch **Kryptoanalyse** den Klartext – oder zunächst den Schlüssel – zu ermitteln. Außerdem könnte Sie versuchen, die übermittelten Informationen zu manipulieren.

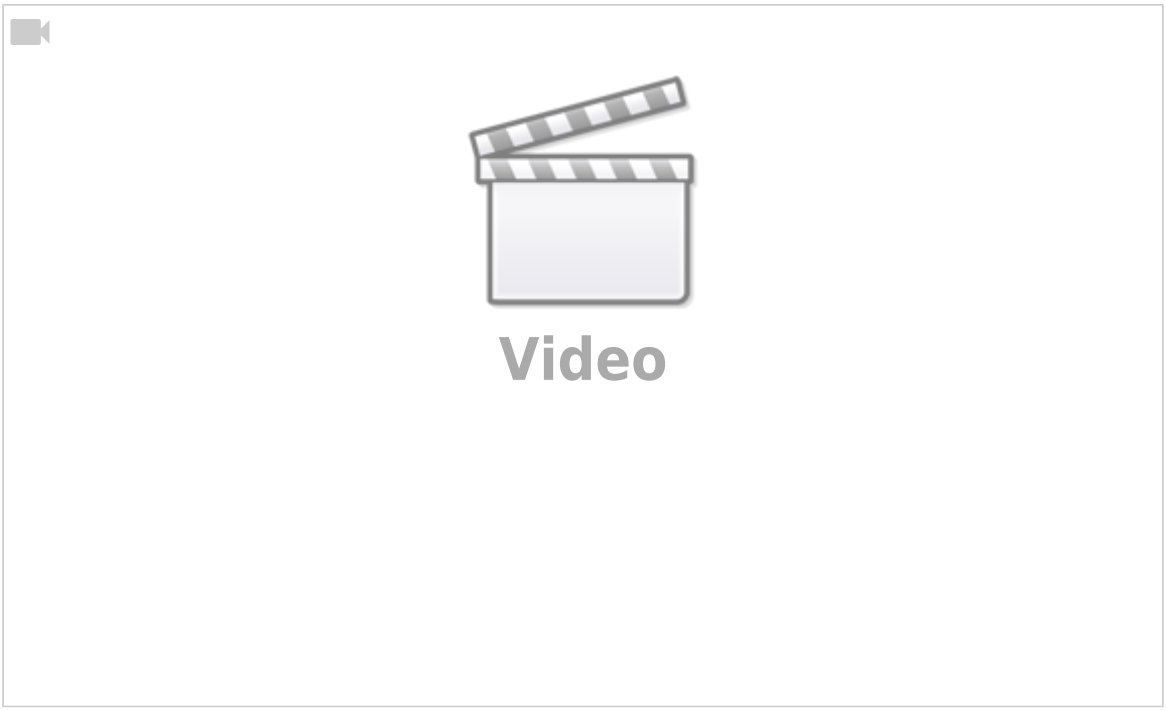
Da Bob über den korrekten **Schlüssel** zur **Dechiffrierung** des **Geheimtexts** verfügt, kann er den Geheimtext entschlüsseln, um den Klartext zu erhalten. So kann er die Nachricht lesen, die Alice ihm geschickt hat.

(A2)

Analysiere die Grafik und erstelle einen Heftaufschrieb mit allen **Fachbegriffen**, denen du in der Grafik begegnest. Es reicht aus, eine Liste mit den Fachbegriffen und kurzen Erklärungen zu haben.

Die Cäsar Verschlüsselung

Jahrhunderte später vertraute Julius Cäsar keinem der Boten, die Nachrichten an seine Generäle überbrachten. Er ersetzte deshalb in seinen Nachrichten jedes A durch ein D, jedes B durch ein E usw. So verfuhr er mit dem ganzen Alphabet. Nur jemand, der die Regel des Vertauschens durch den drittnächsten Buchstaben kannte, konnte die Nachrichten entschlüsseln - er wandte das erste **Substitutionsverfahren** zur Verschlüsselung an.



https://www.youtube.com/watch?v=VeH0KnZtljY

(A3)

(A) Die Cäsar-Chiffre ist ein **monoalphabetisches Substitutionsverfahren**. Erkläre den Begriff.

(B) Grenze Substitutions- von Transpositionsverfahren gegeneinander ab.

(C) Nenne den **Schlüssel**, den Sender und Empfänger bei der Cäsar Chiffre kennen müssen.

(D) Monoalphabetische Chiffren sind für die Kryptoanalyse keine Herausforderung - sie können leicht durch eine **Häufigkeitsanalyse** angegriffen werden. Beschreibe dieses Verfahren.

(E) Benutze die Informationen und Werkzeuge auf https://www.cryptogram.org/resource-area/solve-a-cipher/ um den folgenden Geheimtext in Cäsar-Chiffre zu entschlüsseln, Was ist der Schlüssel für diese Chiffre? Weitere Werkzeuge:

- Häufigkeitsanalyse: https://www.cryptool.org/de/cto/frequency-analysis
- Buchstabenhäufigkeit in der deutschen Sprache: https://www.startpage.com/do/search?query=Buchstabenh%C3%A4ufigkeit+Deutsch&cat=web

```
Iwjydan cexp oeyd reaha Iqad’
Iep zai heaxaj Bazanread;
Aejaopaeho zan Aean sacaj,
Sahyda zeaoa Rkacah hacaj;
Vsaepajo: Saeh iwj zwjj qjz swjj
Aejaj Xnwpaj aooaj gwjj;
Zneppajo wxan jeiip iwj wqyd
Edna Bazanj vqi Caxnwqyd
Ej zea Geooaj qjz zea Lbqadha,
Zajj iwj heacp jeydp canja gqadha.
Oadp, zw eop zea Sepsa Xkhpa,
Zea zwo wqyd jeydp canja skhhpa.
Ednan Dqadjan swnaj znae
Qjz aej opkhvan Dwdj zwxae.
Iwt qjz Iknepv zwydpaj jqj:
Swo eop dean fapvp skdh vq pqj?
Cwjv caoydsejza, aejo, vsae, znae,
Oydjaezaj oea oeyd Xnkp ajpvsae,
Ej rean Paeha, fazao Opqayg
Sea aej ghaejan Bejcan zeyg.
Zeaoa xejzaj oea wj Bwazaj,
Qxano Gnaqv, aej Opqayg wj fazaj,
Qjz ranhacaj oea, cajwq
Ej zaj Dkb zan cqpaj Bnwq.
Gwqi dwp zeao zan Dwdj caoadaj,
Bwjcp an wqyd oydkj wj vq gnwadaj:
Geganege! Gegeganeged!!
```

Verschlüsselung und Entschlüsselung

Daten, die ohne besondere Entschlüsselungsmethoden gelesen werden können, werden *Klartext* genannt. Das Verfahren zum Chiffrieren von Klartext, so dass dessen Inhalt unerkannt bleibt, wird Verschlüsselung (= **Kryptographie**) genannt.

Verschlüsseln von Klartext ergibt ein unleserliches Zeichengewirr, das dann Verschlüsselungstext oder *Chiffrat*, manchmal auch *Geheimtext* genannt wird. Mit der Verschlüsselung bleiben Informationen unbefugten Personen verborgen, selbst wenn ihnen die Daten im verschlüsselten Zustand vorliegen. Das Verfahren des Zurückführens von chiffriertem Text in den ursprünglichen Klartext wird als Entschlüsselung (= **Kryptoanalyse**) bezeichnet.

Aufgaben

1. Übernimm das Schema oben auf dieser Seite in dein Heft und ergänze an passender Stelle die kryptologischen Fachbegriffe, die du bis jetzt gelernt hast.
2. Erläutere die drei Ziele der Kryptographie (**Vertraulichkeit, Authentizität, Integrität**).
3. Bewerte die beiden dir bisher bekannten kryptographischen Verfahren im Hinblick auf die drei Ziele.

1)

Bildquelle: https://commons.wikimedia.org/wiki/File:Skytale.png, Lizenz: Creative Commons Attribution-Share Alike 3.0 Unported

From:
https://wiki.qg-moessingen.de/ - **QG Wiki**

Permanent link:
https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:kryptographie:einfuehrung:substitution:start?rev=1645466894

Last update: **21.02.2022 19:08**