Kryptografie & Kryptoanalyse

Eine Einführung in die klassische Kryptologie

Ziele

- Anhand historischer Verschlüsselungsverfahren Grundprinzipien der Kryptografie kennen lernen.
- Klassische Analysemethoden anwenden und sich dadurch der trotz Verschlüsselung verbleibenden Restrisiken der Verschlüsselung bewusst werden.

Inhalt

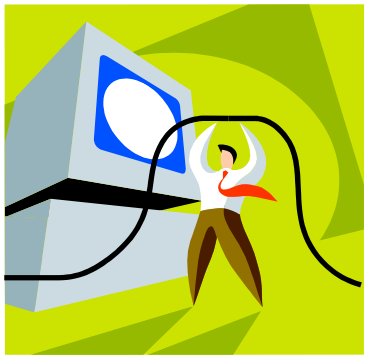
- Übersicht Kryptologie
- Verschlüsselungsverfahren:
  - Caesar
  - Substitution *
  - Vigenère *
  - One-Time-Pad
  - DES / IDEA
- Analysemethoden:
  - Brute-Force *
  - Häufigkeitsverteilung *

* In der Gruppenarbeit

Abbildung: Enigma - Verschlüsselungsmaschine von 1925
(Quelle: http://uboat.net/technical/enigma_breaking.htm

Das Problem

Alice (Sender)



Maloy (Schnüffler)

Bob (Empfänger)

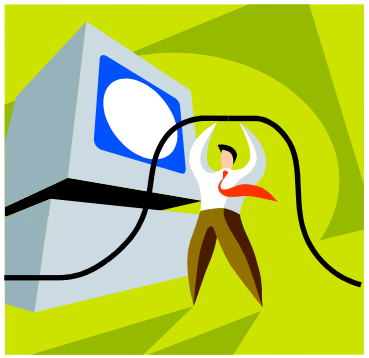
Mithören, Manipulieren

Klartext → Gleicher Klartext?

Nur Bob soll die Nachricht von Alice empfangen können…

Die Lösung

Alice (Sender)



Maloy (Schnüffler)

Bob (Empfänger)

Kein Mithören, kein Manipulieren?

Klartext → Verschlüsseln ⇢ Entschlüsseln → Klartext

Die Nachricht wird verschlüsselt!

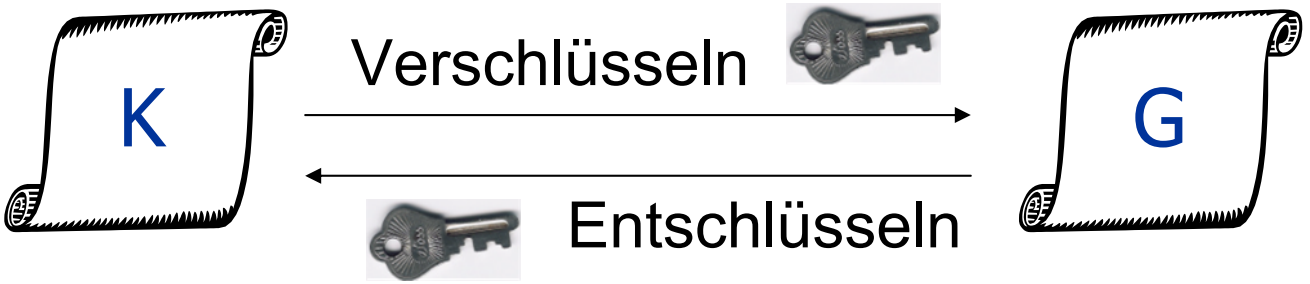
Übersicht

Kryptologie: Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptografischen Verfahren

Kryptografie: Wie kann eine Nachricht ver- und entschlüsselt werden?

Kryptoanalyse: Wie sicher ist ein Ver-schlüsselungsverfahren?

Klassische Kryptografie

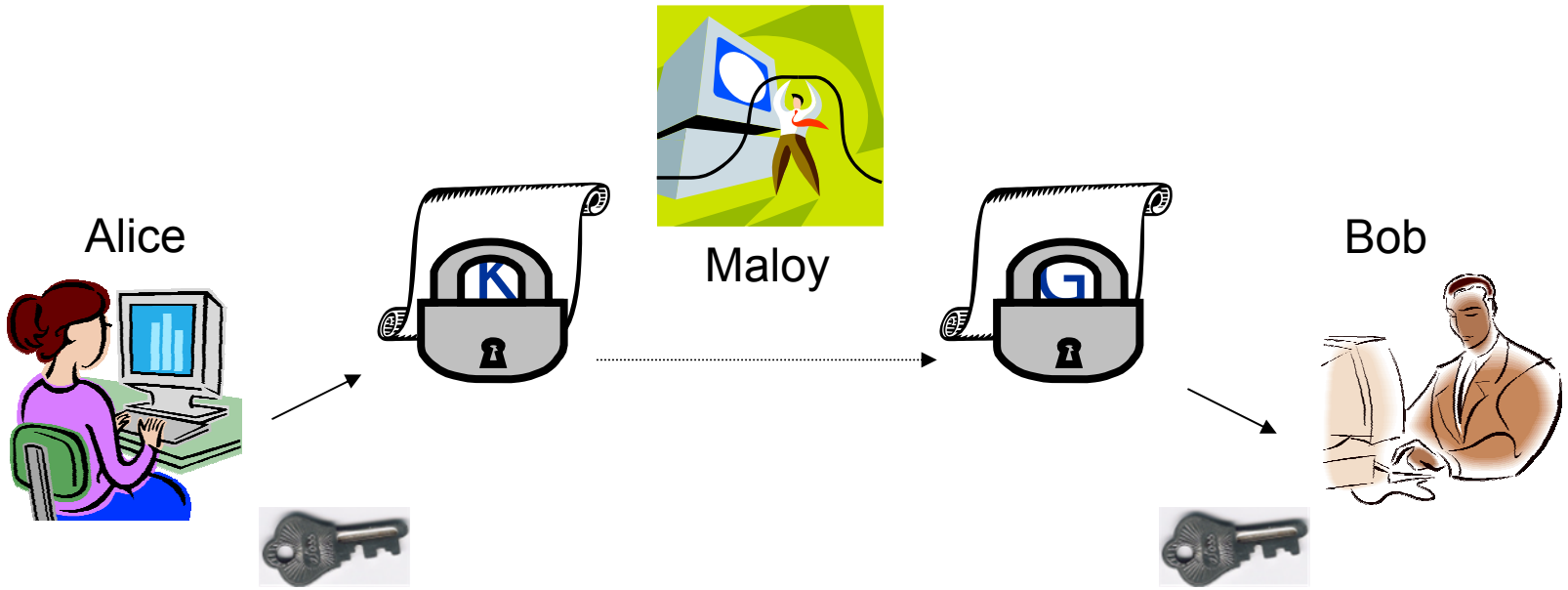


- Der Klartext (K) wird mittels eines Schlüssels verschlüsselt.
- Mit Hilfe des selben Schlüssels kann der Geheimtext (G) wieder entschlüsselt werden.

Geheime Übermittlung

- Voraussetzungen:
  - Der Empfänger kennt den Schlüssel.
  - Aber sonst niemand.
  - Ohne Kenntnis des Schlüssels ist es unmöglich oder sehr schwierig den Klartext herauszufinden.
- Schwierigkeiten:
  - Schlüssel muss vorher vereinbart werden.
  - Schlüssel muss geheim bleiben → „geheimer Kanal“.
  - Das Verschlüsselungsverfahren muss sicher sein.

Vorhängeschloss-Analogie



- Der Klartext ist „eingeschlossen“, und nur Alice und Bob haben den richtigen Schlüssel für das Schloss.

Das Caesar-Verfahren

- Wurde von Julius Caesar 50 Jahre vor Christus benutzt.
- Das Alphabet wird einfach um mehrere Buchstaben verschoben.
- Zum Beispiel um 3 Buchstaben:

  abc**defghijklmnopqrstuvwxyz**

  DEFGHIJKLMNOPQRSTUVWXYZABC
- Damit wird aus dem Klartext „hallo“ der Geheimtext „KDOOR“.

Entschlüsselung

- Die Entschlüsselung ist die Umkehrung der Verschlüsselung (symmetrische Verfahren).
- Das heisst beim Beispiel-Caesar-Verfahren jetzt um 3 Buchstaben zurückverschieben:

  `ABCDEFGHIJKLMNOPQRSTUVW`**`XYZ`**

  `xyz``abcdefghijklmnopqrstuvw`

- So wird aus „KDOOR“ wieder ein „hallo“.

Monoalphabetische Verfahren

- Die Caesar-Verschlüsselung ist ein monoalphabetisches Verfahren
  → Aus einem bestimmten Klartextbuchstaben wird immer derselbe Geheimtextbuchstabe.
- Beispiel:

  abcdefg**h**ijk**l**mn**o**pqrstuvwxyz

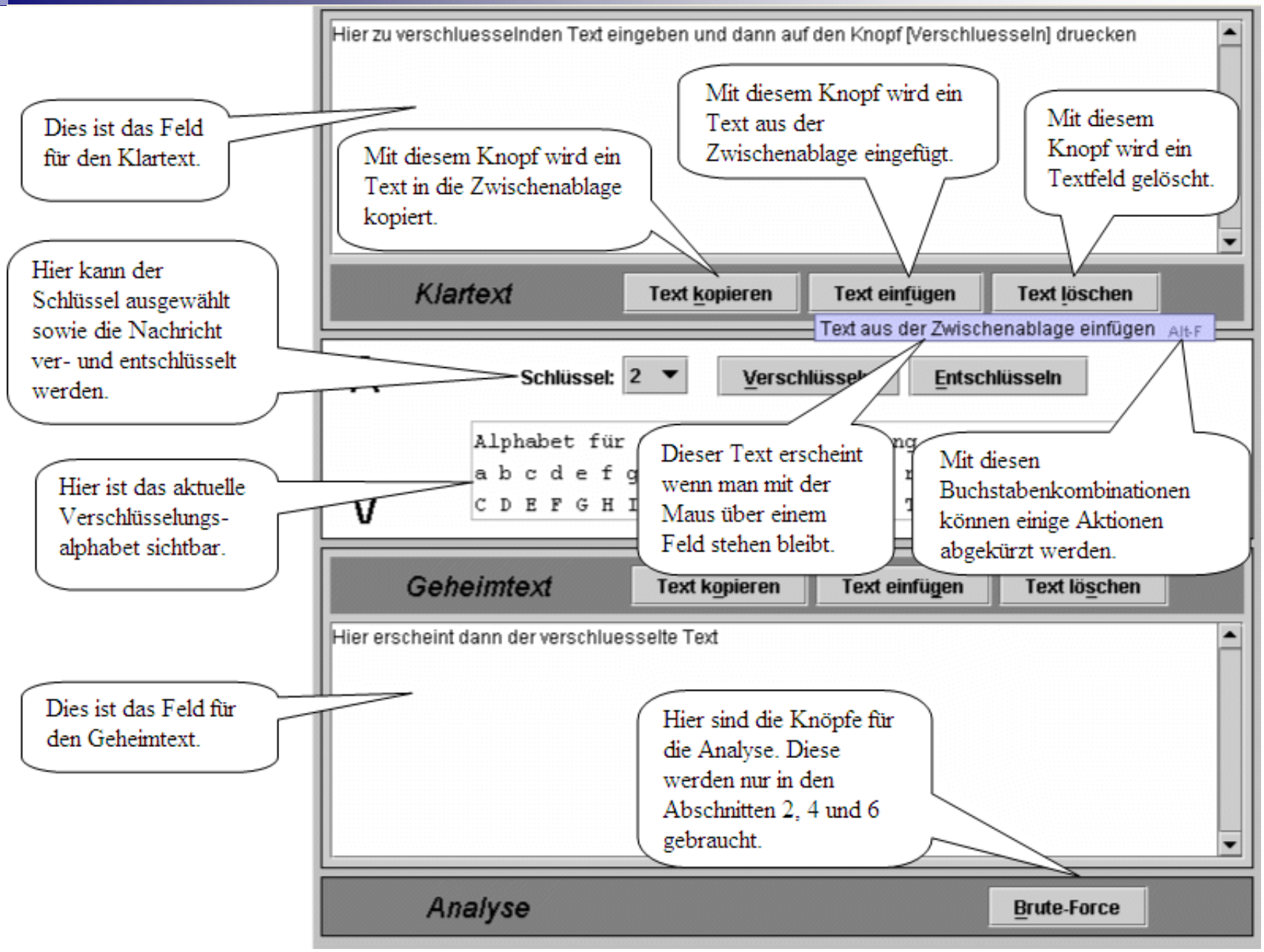
  THEQUIC**K**BRO**W**NF**X**JMPDVLAZYGS
- Damit wird aus dem Klartext „ha**ll**o“ der Geheimtext „KT**WW**X“.
- Aus dem „**l**“ wird beide Male ein „**W**“.

Gruppenarbeit

- Je 2 Zweierteams arbeiten zusammen in einer Vierergruppe.
- Die Zweierteams senden sich gegenseitig Nachrichten.
- Pro Zweierteam steht ein PC zur Verfügung.
- Bevor es losgeht müssen sich die 2 Zweierteams auf einen gemeinsamen Schlüssel für eine Caesar-Verschlüsselung einigen.

Bedienung der Programme

- Während der Gruppenarbeit kommen 3 Programme vor. Die Bedienung sollte kein Problem sein.
- Bei den meisten Knöpfen und Feldern erscheint eine genauere Information, wenn man mit der Maus für kurze Zeit darüber stehen bleibt.


Hier zu verschluesselnden Text eingeben und dann auf den Knopf [Verschluesseln] druecken
Dies ist das Feld für den Klartext.
Mit diesem Knopf wird ein Text in die Zwischenablage kopiert.
Mit diesem Knopf wird ein Text aus der Zwischenablage eingefügt.
Mit diesem Knopf wird ein Textfeld gelöscht.
Klartext
Text kopieren
Text einfügen
Text löschen
Hier kann der Schlüssel ausgewählt sowie die Nachricht ver- und entschlüsselt werden.
Text aus der Zwischenablage einfügen Alt-F
Schlüssel: 2
Verschlüsseln
Entschlüsseln
Alphabet für
a b c d e f g
C D E F G H I
Hier ist das aktuelle Verschlüsselungs-alphabet sichtbar.
Dieser Text erscheint wenn man mit der Maus über einem Feld stehen bleibt.
Mit diesen Buchstabenkombinationen können einige Aktionen abgekürzt werden.
Geheimtext
Text kopieren
Text einfügen
Text löschen
Hier erscheint dann der verschluesselte Text
Dies ist das Feld für den Geheimtext.
Hier sind die Knöpfe für die Analyse. Diese werden nur in den Abschnitten 2, 4 und 6 gebraucht.
Analyse
Brute-Force

Während der Gruppenarbeit

- Wenn ein Zweierteam auf das andere warten muss, hat es in der Anleitung diverse Links um ein Thema zu vertiefen.
- Bei Fragen oder Problemen aufstrecken → ich komme vorbei.
- Viel Spass!