Eine Einführung in die klassische Kryptologie

Kryptografie & Kryptoanalyse

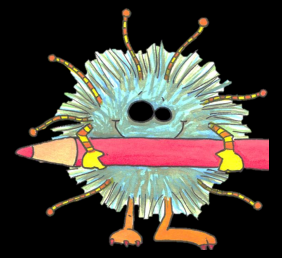
© Jana Rau, 02/2021

Ziele des Kurses

Anhand historischer und moderner **Verschlüsselungsverfahren** werden die Grundprinzipien der Kryptografie kennen gelernt.

Klassische **Analysemethoden** werden verstanden und die verbleibenden **Restrisiken jeder Verschlüsselung** sind bewusst.

Ewas bedeutet Kryptologie?



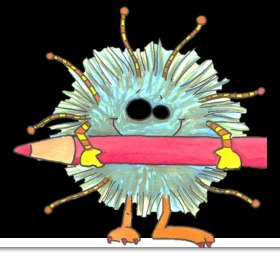
Kryptologie:

Kryptografie

Kryptoanalyse

Steganografie

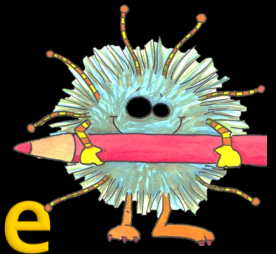
Definition der Verschlüsselung



Eine Verschlüsselung ist eine **eindeutige**[!1] Zuordnung, eines Zeichens aus der Menge des Klartextalphabets zu einem Zeichen aus Menge des Verschlüsselungsalphabets[!2].

[!1] Nicht eineindeutig!
[!2] Klartext -und Verschlüsselungsalphabet müssen nicht gleich sein.

Kryptographie und Kryptoanalyse



Kryptographie und Kryptoanalyse sind harte Gegenspieler im Kampf um Integrität und Vertraulichkeit.

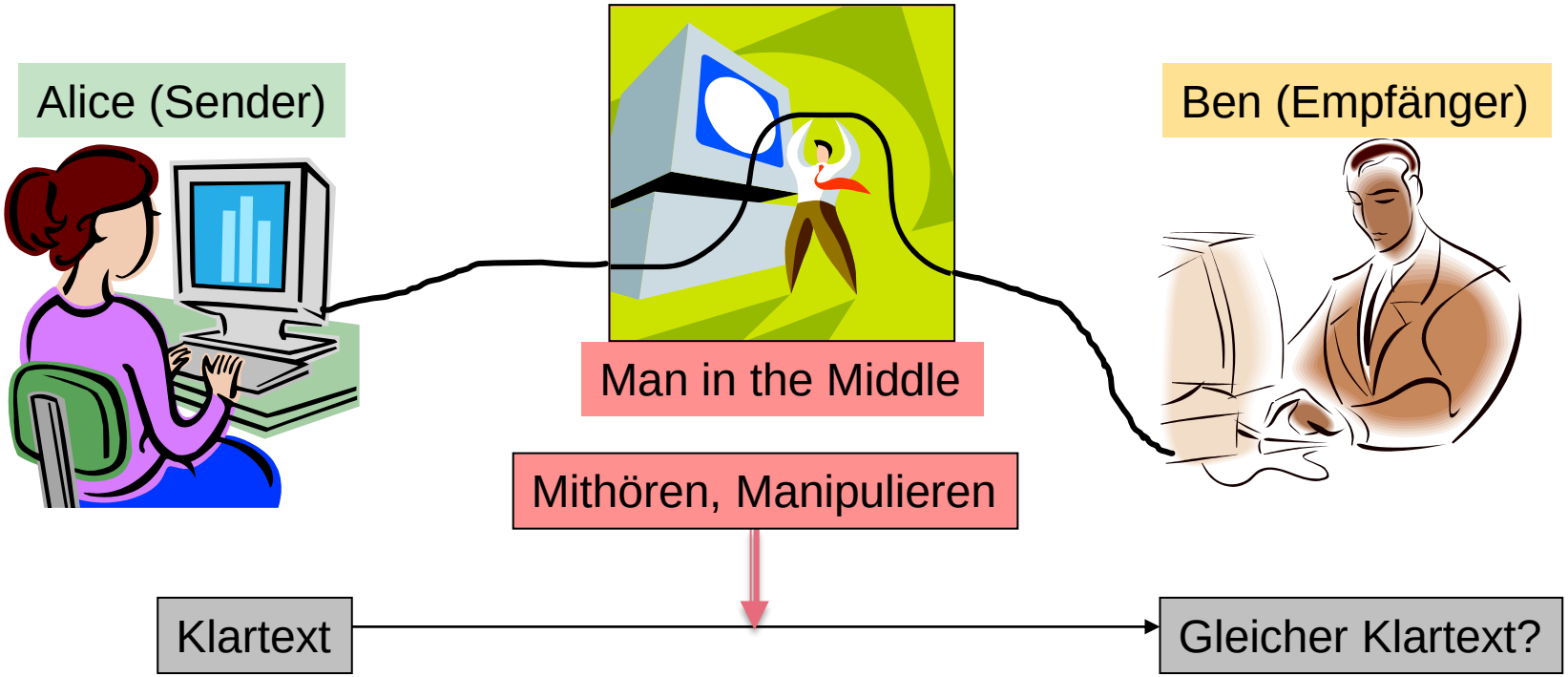
also

Es findet ein permanenter Wettkampf zwischen den Schutzmechanismen und den Hackern statt!

Die klassische Kryptografie

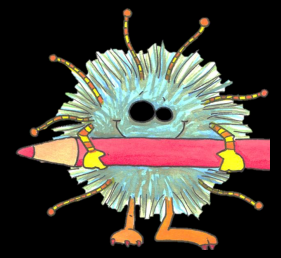
Der Klartext (K) wird mittels eines Schlüssels verschlüsselt.
Mit Hilfe des selben Schlüssels kann der Geheimtext (G) entschlüsselt werden.

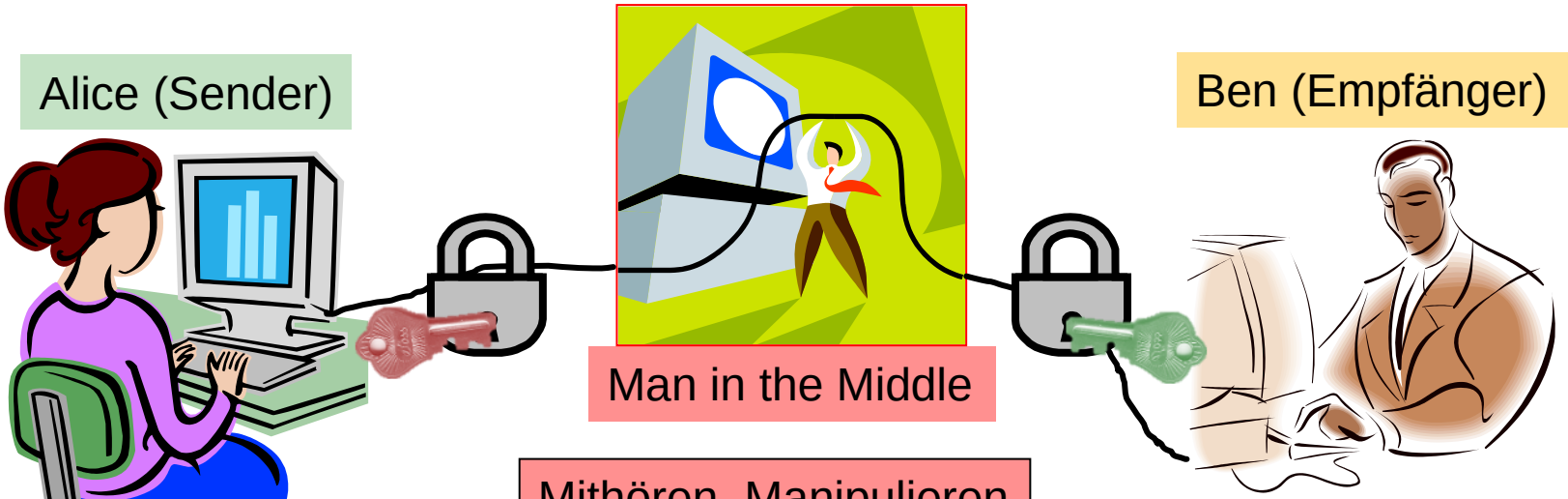
Das Problem – Vertraulichkeit & Integrität schützen



Nur Bob soll die unverfälschte Nachricht von Alice lesen können…

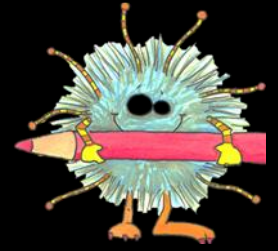
Die Lösung...





Die Nachricht wird verschlüsselt!

Schlüsselübergabe



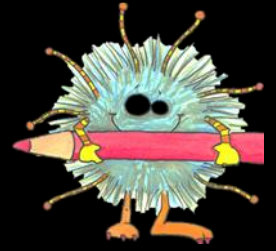
Voraussetzungen: -->Vertraulichkeit

- Der Empfänger kennt den Schlüssel, sonst niemand.
- Ohne Kenntnis des Schlüssels ist es zeitaufwändig den Klartext herauszufinden.

Schwachstellen:

-
-
-

Verschlüsselungen ‘knacken’



(1) Brute - Force-Verfahren:

- Dieses Verfahren ist immer erfolgreich, aber nicht immer sinnvoll., z.B. wenn es bis zum Erfolg mehrere Jahre dauert.
- kann mit modernen Computern sehr schnell erfolgreich sein.
- Gegenmaßnahmen:
  sehr lange, komplizierte Schlüssel
  Beschränkung der Anzahl der Versuche

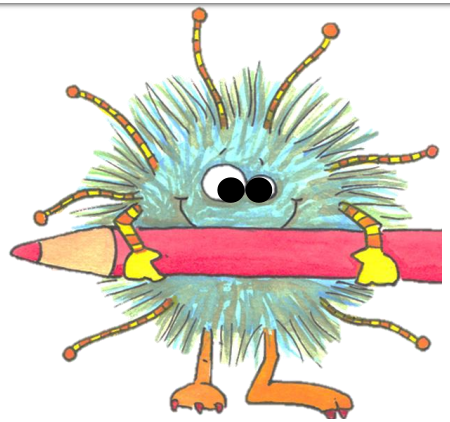
Verschlüsselungen 'knacken'

(2) Statistische Analyse der Zeichenhäufigkeit

Wird jedem Buchstaben eines Alphabets eineindeutig einem anderen zugeordnet, bleibt die Häufigkeit der Buchstaben.

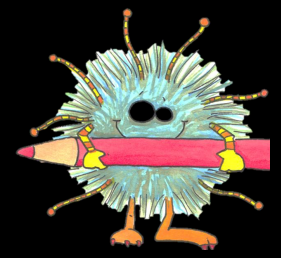
Bsp.: In deutschen Texten tritt "e" mit einer mittleren Wahrscheinlichkeit von 17,4% am häufigsten auf. Findet man also ein Zeichen, dessen Häufigkeit die der anderen deutlich übersteigt, handelt es sich sehr wahrscheinlich im Klartext um das "e". Auch Buchstabenpaare (Bigramme) treten mit unterschiedlichen Häufigkeiten auf: "en" ist beispielsweise mit 3,9 Prozent das häufigste Bigramm.

Die Einteilung der Verschlüsselungsverfahren



Ergänzen Sie jeweils Beispiele,
während des Durcharbeitens der weiteren Materialien!

Die Einteilung der Verschlüsselungsverfahren



1. Art der Verschlüsselung

Umordnung (Transposition)

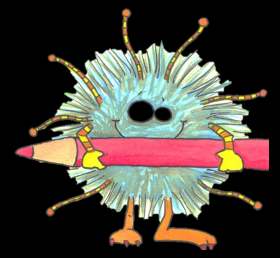
☠ die Häufigkeitsverteilung der Zeichen bleibt gleich.

Permutation (Umordnung /Durchschütteln) der Zeichen des Klartextalphabets. (keine neuen Symbole)

H	A	S	E	N	O	H	R	E	N
N	S	A	O	R	H	E	N	H	E

Beispiele:

Die Einteilung der Verschlüsselungsverfahren



1. Art der Verschlüsselung (1)

Ersetzung (Substitution)

☠ die Häufigkeitsverteilung der Zeichen bleibt gleich.

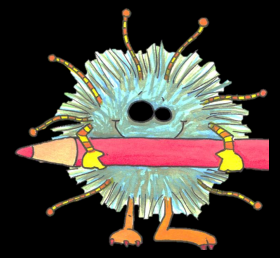
Nicht die Anordnung wird verändert, sondern die Elemente des Klartextalphabets werden durch die Elemente eines Verschlüsselungsalphabets ersetzt.

H	A	S	E	N	O	H	R	E	N
I	B	T	F	O	P	I	S	F	O

H	A	S	E	N	O	H	R	E	N
👆	✌	💧	👈	☠	⚑	👆	☼	👈	☠

Beispiele:

Die Einteilung der Verschlüsselungsverfahren



2. Art der Zuordnung

Monoalphabetisch

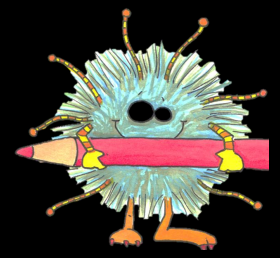
Eineindeutige Zuordnung des Verschlüsselungsalphabets zum Klartextalphabet

☠ die Häufigkeitsverteilung der Zeichen bleibt gleich.

H	A	S	E	N	O	H	R	E	N
I	B	T	F	O	P	I	S	F	O

Beispiele:

Die Einteilung der Verschlüsselungsverfahren



2. Art der Zuordnung

Polyalphabetisch

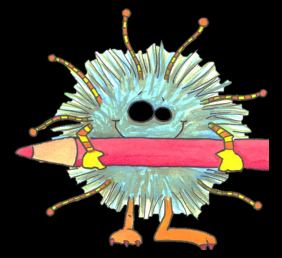
Eindeutige Zuordnung des Verschlüsselungsalphabets zum Klartextalphabet, d. b. eine mehrdeutige Zuordnung des Klartextbuchstabens zum Verschlüsselungsalphabet

☺ Verschleierung der Buchstabenhäufigkeit

H	A	S	E	N	O	H	R	E	N
T	A	W	Y	F	S	G	R	L	A

Beispiele:

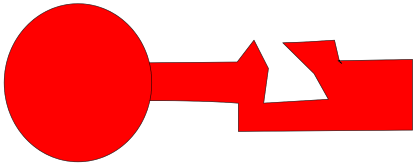
Die Einteilung der Verschlüsselungsverfahren

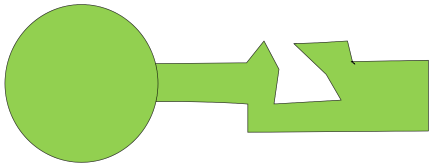


3. Art der Schlüsselverteilung

Symmetrische Verschlüsselung

symmetrisch: nur ein Schlüssel – gleiche Schlüssel für das Ver- und Entschlüsseln

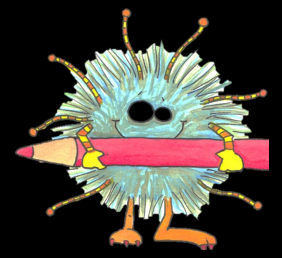




Kopien verteilen: Gefahr der unbefugten Benutzung oder Weitergabe des Schlüssels
Einzelexemplar: Gefahr des Verlustes bzw. ständige Übergabe zwischen Sender und Empfänger notwendig.

Beispiele:

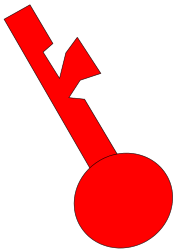
Die Einteilung der Verschlüsselungsverfahren

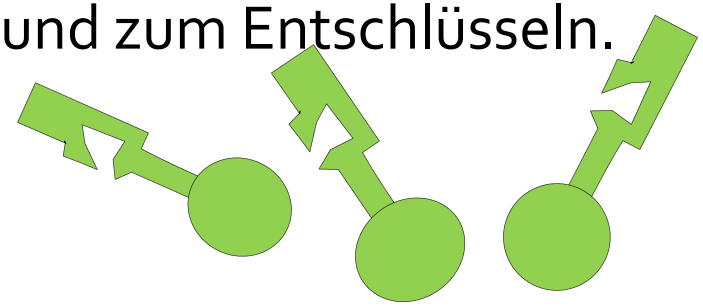


3. Art der Schlüsselverteilung

Asymmetrische Verschlüsselung

asymmetrisch: ein zusammenpassendes Schlüsselpaar - je ein Schlüssel zum Ver – und zum Entschlüsseln.





Vorteil: Es ist keine Schlüsselweitergabe notwendig, weil der „Ver-Schlüssel', kopiert und verteilt wird, den ‚Ent-Schlüssel' hat nur der Empfänger.

Beispiele:

:Ein Schlüssel ist natürlich meist ein Passwort!