WERNER WINKELMANN

KRYPTOLOGIE

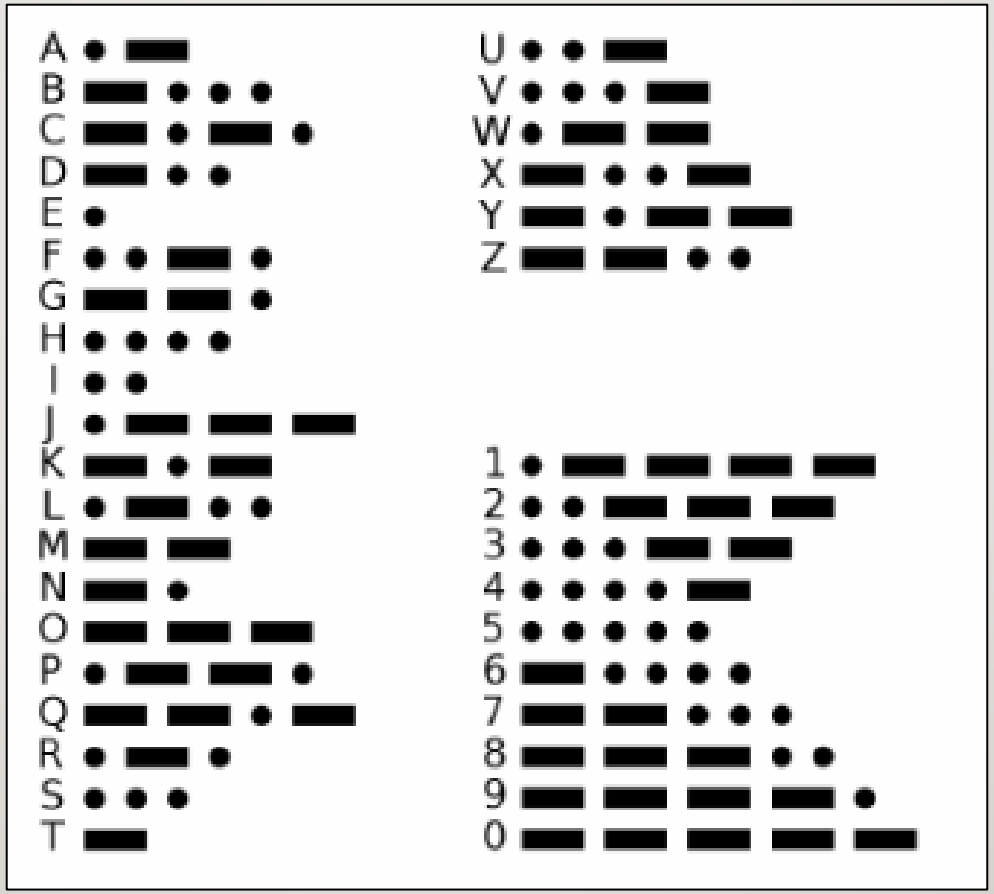
Basierend auf

- https://ddi.uni-wuppertal.de/www-madin/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf
- https://lehrerfortbildung-bw.de/u_matnatech/informatik/gym/bp2016/fb1/3_rechner_netze/1_hintergrund/9_krypto/07_run_hintergrund_kryptografie.pdf
- https://www.oszhandel.de/gymnasium/faecher/informatik/krypto/index.htm
- https://oinf.ch/kurs/informationsgesellschaft/verschluesselung/
- Unterlagen von Timon Ruther

KRYPTOLOGIE

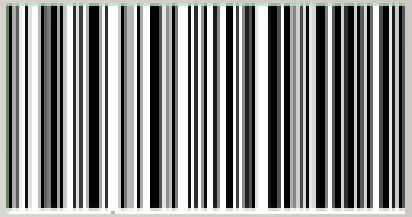
- Kryptographie — Verschlüsseln von Informationen
- Kryptoanalyse — Entschlüsseln von Informationen
- Steganographie — Verstecken von Information

Beispiel: Morse-Code

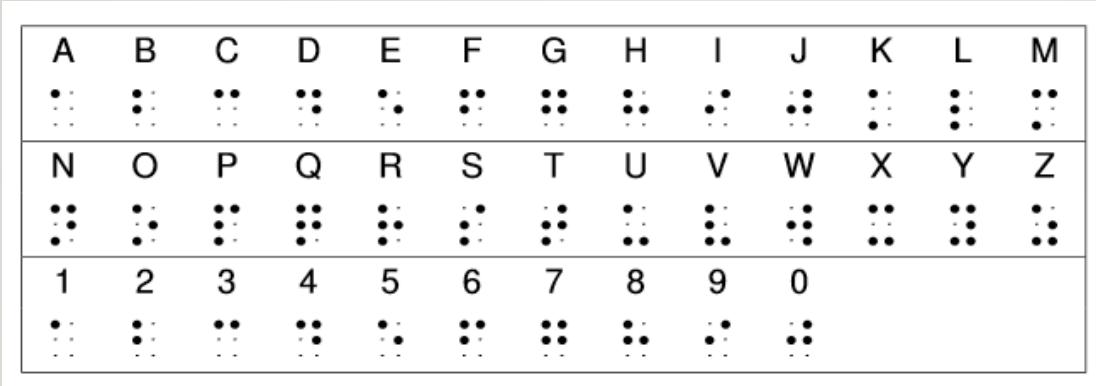


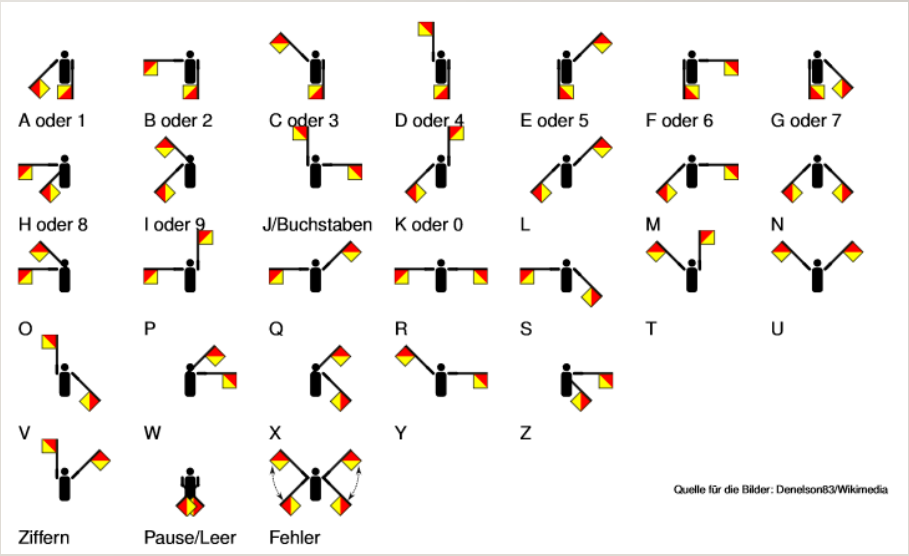
Codierung

- Mit einem Code soll nichts geheim gehalten werden.



- *Die Buchstaben bleiben wo sie sind, aber nicht was sie sind. Jeder kann nachschlagen, was sie bedeuten, man nennt so etwas einen Code.*





Aufgabe: Finden Sie die versteckte Botschaft

Lieber Chef
Mein Mitarbeiter, Herr X, ist immer dabei,
seine Arbeit zu tun, und das sehr eifrig, ohne jemals
seine Zeit mit Schwätzchen zu verplempern. Nie
lehnt er es ab, anderen zu helfen, und trotzdem
schafft er sein Arbeitspensum; oft bleibt er länger
im Büro, um seine Arbeit zu beenden. Er arbeitet sogar
in der Mittagspause. Mein Mitarbeiter ist jemand ohne
Überheblichkeit in Bezug auf seine überragenden
Fachkenntnisse. Er ist einer der Kollegen auf die man
stolz sein kann und auf deren Arbeitskraft man nicht
gern verzichtet. Ich denke, dass es Zeit wird für ihn,
befördert zu werden, damit er nicht auf den Gedanken kommt,
zu gehen. Die Firma kann davon nur profitieren.

Steganographie

- Verbergen von Nachrichten (Häufig in anderen Informationen wie Bild- oder Musikdateien.)
- *Die Buchstaben bleiben was sie sind, aber man erkennt nicht, wo die Nachricht ist.*
- Texte oder Bilder, in denen Nachrichten versteckt wurden, heißen Semagramme.

Bonus: Kannst du die Nachricht in dem folgenden Semagramm lesen?

Es ist nicht ganz einfach, da die Nachricht vor dem Verstecken codiert wurde.

Bild: Emma, 3 Jahre (dem Bild wurde dann die (codierte) Nachricht hinzugefügt)

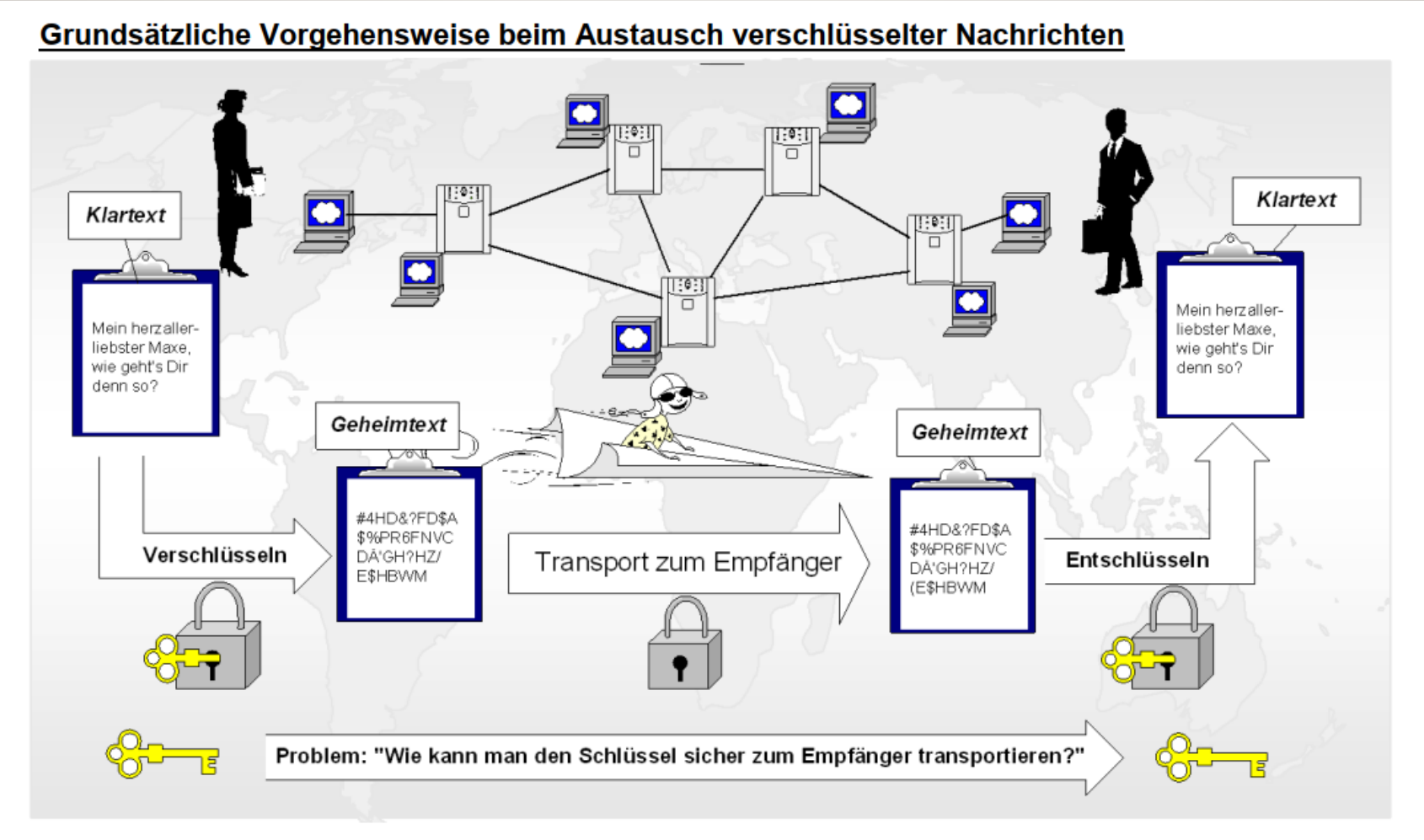
SYMMETRISCHE VERSCHLÜSSELUNG

1. Transposition: Skytale
2. Substitution
   - Monoalphabetisch: Cäsar
   - Polyalphabetisch: Vigenère, One-Time-Pad

– Geschichtlicher Rückblick

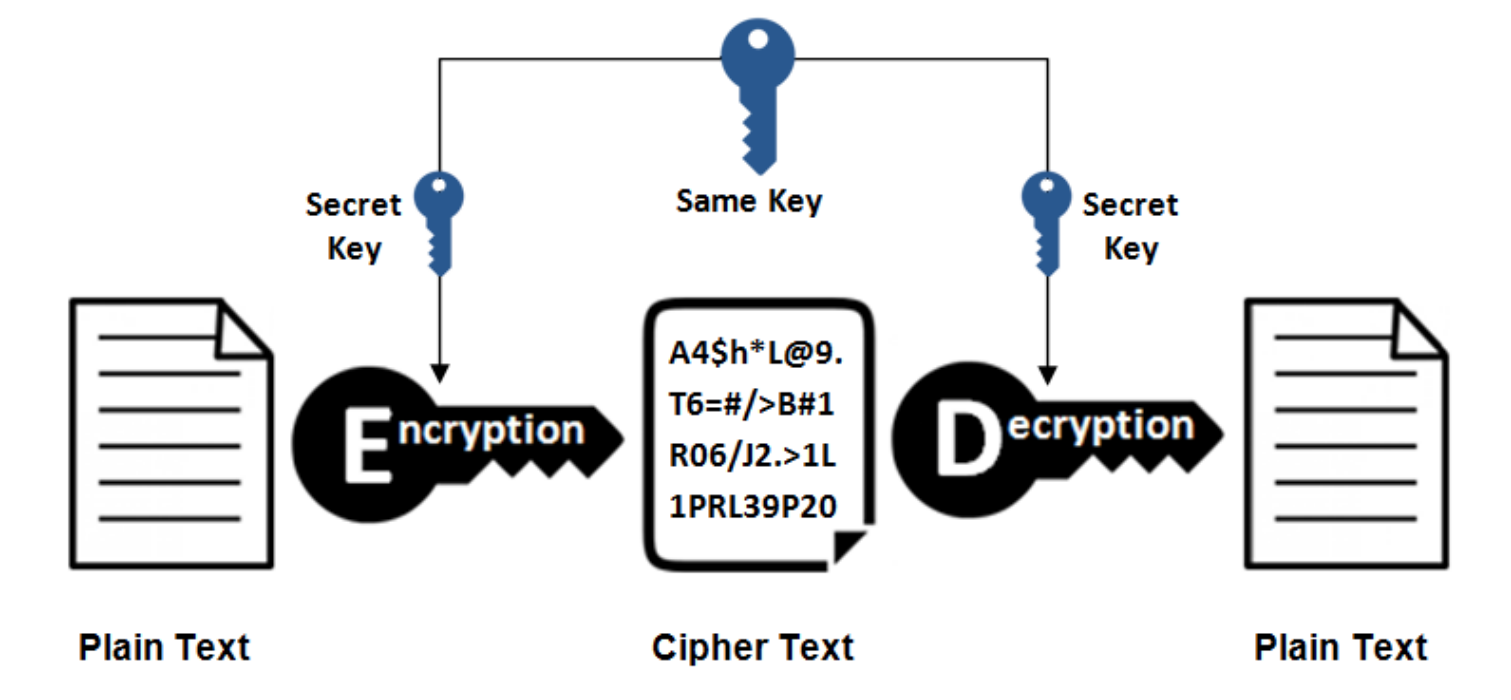
- **600 v. Chr.** benutzen hebräische Gelehrte einfache Zeichenaustauschalgorithmen.
- **405 v. Chr.**: Eine verschlüsselte Botschaft auf der Innenseite eines Gürtels wird lesbar, wenn man den Gürtel um einen Holzstab wickelt.
- **50 v. Chr.** entwickelt der römische Feldherr Julius Cäsar das heute als Caesar-Verschlüsselung bekannte Verfahren.
- **Im 16. Jahrhundert** entwickelt Blaise de Vigenère die nach ihm benannte polyalphabetische Verschlüsselungstechnik. Sie wurde für unknackbar gehalten, bis Charles Babbage 1854 eben doch einen Weg zur Entzifferung fand.
- **Ende des 19. Jahrhunderts** werden durch die Einführung des Telegrafen neue Überlegungen in der Kryptographie angeregt. Durch das relativ einfache Abhören von Telegrafen wächst auch das Bedürfnis nach einer verschlüsselten Übertragung.
- **Während des 2. Weltkriegs** gilt die Enigma zunächst als absolut sichere Chiffriermaschine, wird jedoch von polnischen und englischen Kryptoanalytikern (insb. Alan Turing) geknackt – unter Zuhilfenahme eines eigens dafür entwickelten Vorläufers moderner Computer.

Grundlagen


Grundsätzliche Vorgehensweise beim Austausch verschlüsselter Nachrichten
Klartext
Mein herzaller-liebster Maxe, wie geht's Dir denn so?
Verschlüsseln
Geheimtext
#4HD&?FD$A $%PR6FNVC DÄ'GH?HZ/ E$HBWM
Transport zum Empfänger
Geheimtext
#4HD&?FD$A $%PR6FNVC DÄ'GH?HZ/ (E$HBWM
Entschlüsseln
Klartext
Mein herzaller-liebster Maxe, wie geht's Dir denn so?
Problem: "Wie kann man den Schlüssel sicher zum Empfänger transportieren?"

Symmetrische Verschlüsselung

- Derselbe Schlüssel dient dem Ver- und Entschlüsseln der Nachricht

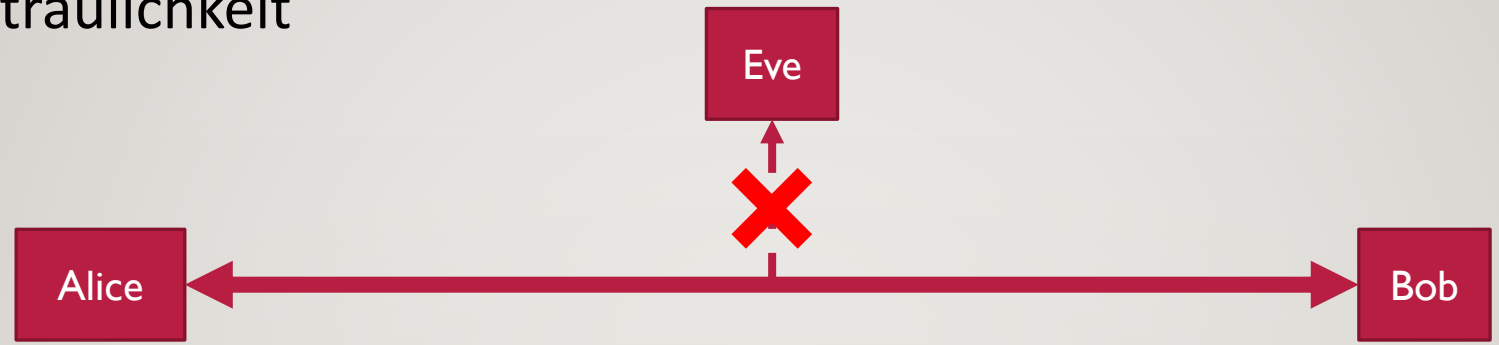


Grafik von: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

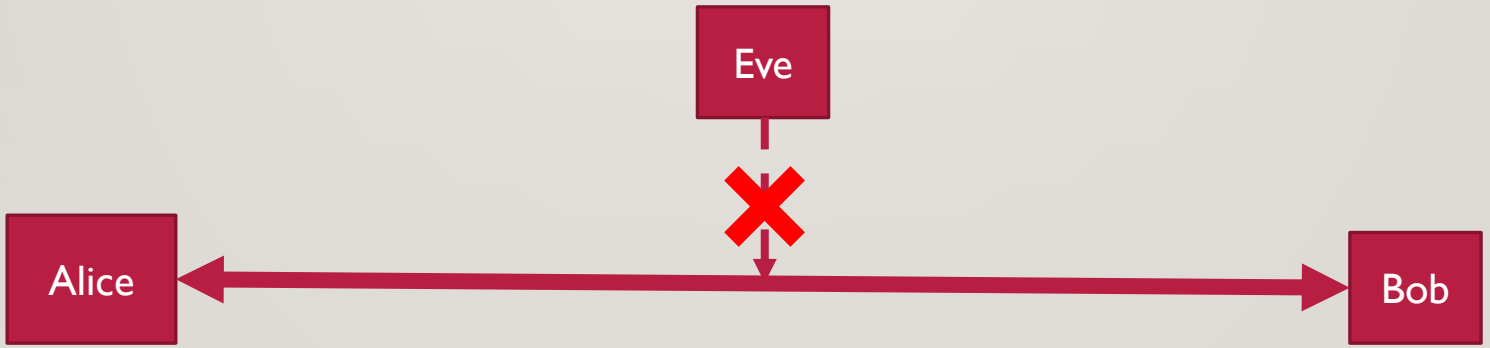
Welche Ziele verfolgt die Kryptographie?

Welche Ziele verfolgt die Kryptographie?

1. Vertraulichkeit



2. Integrität



Welche Ziele verfolgt die Kryptographie?

3. Authentizität

4. Verbindlichkeit

Kryptographie

Beim Chiffrieren von Klartexten in Geheimtexte gibt prinzipiell es nur zwei Methoden:

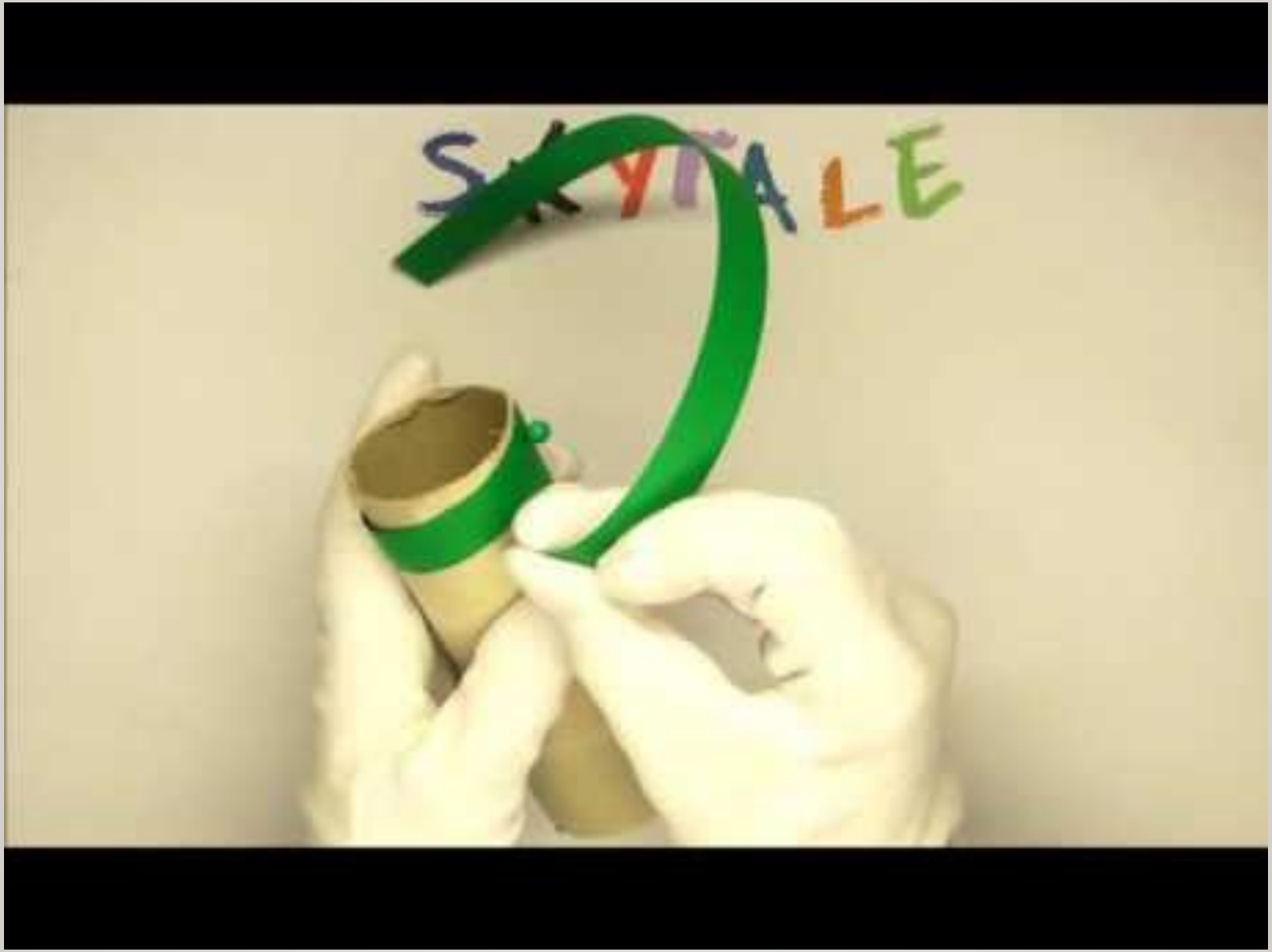
1. **Transposition**
   Die Zeichen des Klartextes bleiben im Geheimtext dieselben, ihre Anordnung im Text wird jedoch verändert.

2. **Substitution**
   Jedes Zeichen des Klartextes wird durch ein anderes ersetzt. A ==> D, B ==> E, C ==> F oder ähnlich. Am Ende besteht der Geheimtext aus anderen Zeichen als der Klartext.

Symmetrische Verschlüsselung

1. **Transposition:** **Skytale**
2. Substitution
   - Monoalphabetisch: Cäsar
   - Polyalphabetisch: Vigenère, One-Time-Pad

SKYTALE



SKYTALE

- Der Durchmesser des Stabes ist von grosser Bedeutung und entspricht dem ***Versatz***, also dem Schlüssel dieser ***Transpositions***-Verschlüsselung.
- Leerzeichen werden mitcodiert oder weggelassen
- Zum **Entschlüsseln** des Geheimtextes ist dieser in ***n*** Spalten der *richtigen Länge* einzutragen und zeilenweise ab zu lesen.
- Die richtige Länge erhält man durch eine Division mit Rest.

Beispiel einer Transposition

D	I	E	S	E	R
T	E	X	T	I	S
T	G	A	N	Z	G
E	H	E	I	M	

Skytale (Transposition)

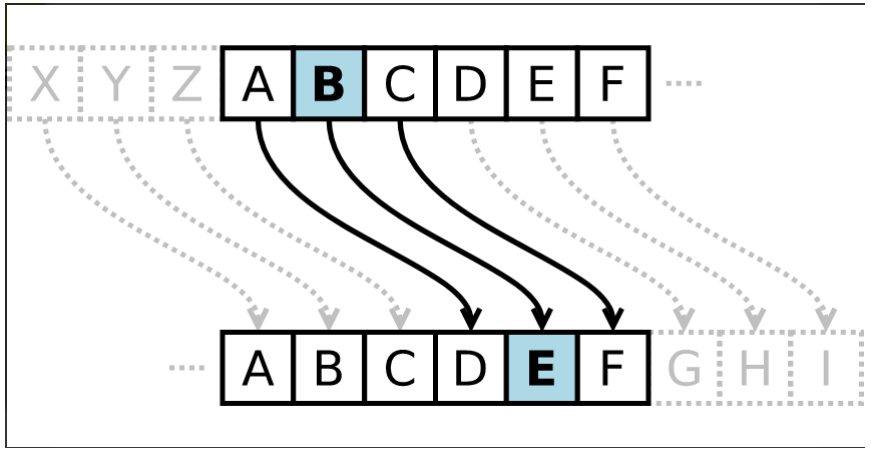
Aufgabe 1: Kannst du folgende Nachricht ohne Skytale »knacken«?

K R C I O G H N M E B X M N E D M N R K O A L P

Aufgabe 2: Warum ist das »knacken« und nicht »entschlüsseln«?

Symmetrische Verschlüsselung

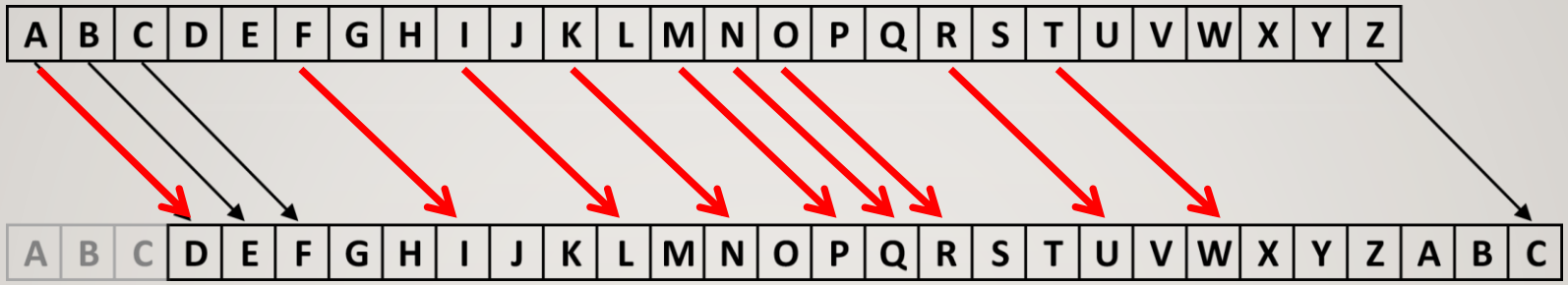
1. Transposition — Skytale
2. **Substitution**
   - **Monoalphabetisch: Cäsar**
   - Polyalphabetisch: Vigenère, One-Time-Pad



Die CAESAR- Verschlüsselung

Monoalphabetische Substitution

Beispiel Cäsar-Chiffre



«informatik» nach Caesar → «lqirupdwln»

Monoalphabetische Verschlüsselung

- bei monoalphabetischen Verschlüsselungen wird für den gesamten Text jedes Klartextzeichen immer durch dasselbe Geheimtextzeichen ersetzt

- es muss aber nicht zwingend einer festen Verschiebung im Alphabet folgen, sondern kann:
  - zufällig sein
  - ein anderes Alphabet verwenden

=> Als Beispiel: Jedes "E" durch ein "A" ersetzen und jedes "R" durch ein "B" usw.

Symmetrische Verschlüsselung

1. Transposition: Skytale
2. Substitution
   - Monoalphabetisch: **Cäsar**
   - Polyalphabetisch: Vigenère, One-Time-Pad

Angriffsstellen der Monoalphabetischen Verschlüsselung

1. Schlüssel abfangen (bei der Übergabe)
2. Alles ausprobieren (z.B. die 26 möglichen Verschiebungen des Alphabets durchprobieren)

3. Ohne Schlüssel geschickt raten, aufgrund bekannter Eigenschaften der Zielsprache, z.B.
    - Häufigkeitsverteilung von Buchstaben
    - Übliche Buchstabenkombinationen oder Wortendungen
    - Kurze Wörter erraten (gibt nicht viele)
    - ...

Häufigkeitsanalyse (Histogramme)

Platz	*Buch-stabe*	*relative Häufig-keit*
1.	E	17,40 %
2.	N	9,78 %
3.	I	7,55 %
4.	S	7,27 %
5.	R	7,00 %
6.	A	6,51 %
7.	T	6,15 %
8.	D	5,08 %
9.	H	4,76 %

Platz	*Buch-stabe*	*relative Häufig-keit*
10.	U	4,35 %
11.	L	3,44 %
12.	C	3,06 %
13.	G	3,01 %
14.	M	2,53 %
15.	O	2,51 %
16.	B	1,89 %
17.	W	1,89 %
18.	F	1,66 %

Platz	*Buch-stabe*	*relative Häufig-keit*
19.	K	1,21 %
20.	Z	1,13 %
21.	P	0,79 %
22.	V	0,67 %
23.	J	0,27 %
24.	Y	0,04 %
25.	X	0,03 %
26.	Q	0,02 %

Bigramme & Trigramme

Bigramm	ER	EN	CH	TE	ND	EI	DE
Häufigkeit	9,9%	3,7%	3%	2,2%	2,1%	2,1%	2,1%

Trigramm	EIN	ICH	DER	SCH	UND	DIE	NDE
Häufigkeit	1,1%	1,1%	0,9%	0,8%	0,8%	0,7%	0,7%

Weitere Ansätze (Deutscher Klartext)

- Der erste Buchstabe in drei-Zeichen-Worten ist wahrscheinlich ein D (der, die, das, den,…).
- Ein Zeichen, das fast nur in Begleitung eines bestimmten anderen Zeichens vorkommt, ist ziemlich sicher ein C (gefolgt von H).
- Ein Zeichen, das nur in Begleitung eines bestimmten anderen Zeichens vorkommt, ist sehr sicher ein Q (gefolgt von U).
- Das E ist am Wortende sehr häufig gefolgt von N (üblichster Plural), innerhalb von Wörtern oft in Kombination mit I (ei, ie).
- Nur wenige Buchstaben können doppelt vorkommen, im Deutschen verdoppelt man zumeist N, M oder T.
- Vokale und Konsonanten können zumeist aufgrund ihrer Verteilung in Wörtern voneinander unterschieden werden.

Kryptoanalyse

Wissenschaft, um Informationen aus verschlüsselten Texten zu gewinnen

Krypotools:

- https://studio.code.org/s/frequency_analysis/stage/1/puzzle/1
- http://mgje.github.io/Interaktive_Experimente/Interaktiv_verschluesseln/exp6/index.html

Symmetrische Verschlüsselung

1. Transposition: Skytale
2. Substitution
   - Monoalphabetisch: Cäsar
   - **Polyalphabetisch:** **Vigenère,** One-Time-Pad

Polyalphabetische Verschlüsselung

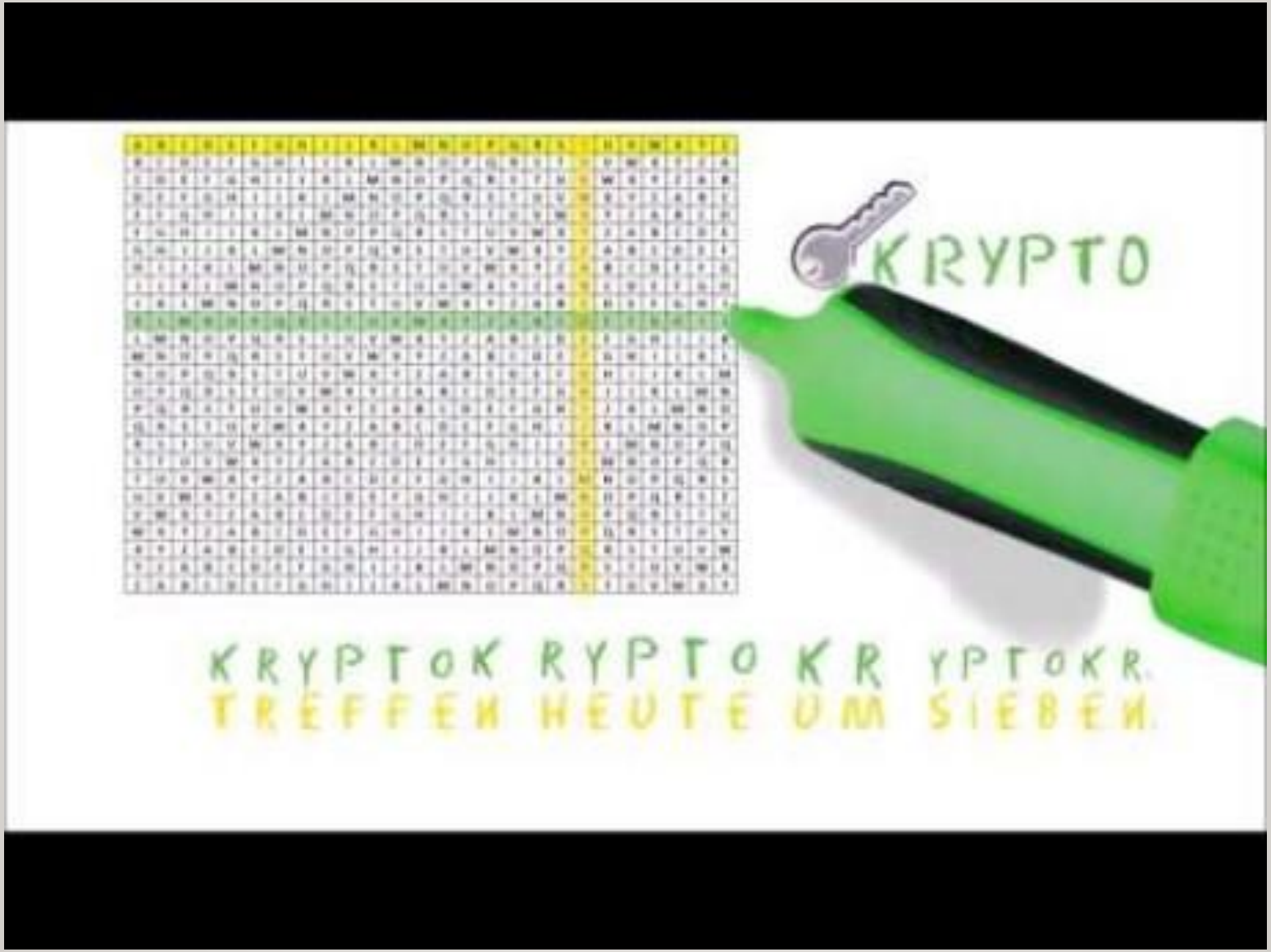
- bei der polyalphabetischen Verschlüsselung werden mehrere Geheimtextalphabete eingesetzt, um eine Häufigkeitsanalyse zu erschweren bzw. zu verunmöglichen.

  => gleiche Klartextbuchstaben werden damit immer wieder zu anderen Geheimtextbuchstaben

```
Klartext:              RITTER
Geheimtext (Mono):     XMSSQR
Geheimtext (Poly):     AXTEWR
```

- bereits 1460 wurde diese Weiterentwicklung mit 2 alternierenden Geheimtextalphabeten vorgeschlagen
- Vigenère griff 1585 die Grundidee auf und verwendete nicht nur 2 sondern 26 Geheimtextalphabete

Vigènere (3min)



Kryptologie/Kryptographie

- **Transposition**: *Bei der Transposition bleiben die Buchstaben, was sie sind, aber nicht wo sie sind.*

Skytale (405 v. Chr.)

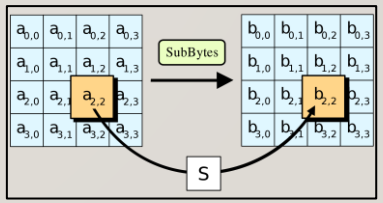
- **Substitution**: *Die Buchstaben bleiben wo sie sind, aber nicht was sie sind*.
  - Monoalphabetische

Cäsar (50 v. Chr)

  - Polyalphabetische

Vigènere (1585 n. Chr)

- Raffinierte Kombination von beiden Verfahren



AES (2000 n. Chr)

Symmetrische Verschlüsselung

1. Transposition: Skytale
2. Substitution
   - Monoalphabetisch: Cäsar
   - Polyalphabetisch: **Vigenère**, One-Time-Pad

Angriffsstellen der Polyalphabetischen Verschlüsselung

- Schlüssel abfangen (bei der Übergabe)

- Kennen (oder erraten) wir die Länge des Schlüssels, wissen wir auch, welche Buchstaben mit demselben Alphabet verschlüsselt wurden → dann kann wieder mit der Häufigkeitsanalyse gearbeitet werden

Knacken der Vigenère-Verschlüsselung

- Charles Babbage gelang es Mitte des 19. Jahrhunderts, die Schwäche von polyalphabetischen Verschlüsselungsverfahren aufzudecken. Diese liegt insbesondere bei zu kurz gewählten Schlüsseln.
- Zum Knacken der Vigenère-Verschlüsselung wird im Geheimtext nach mehrfach vorkommenden Buchstabenfolgen gesucht.
- So kann in einem ersten Schritt auf die Länge des Schlüssels und in einem zweiten Schritt auf das Schlüsselwort selbst geschlossen werden.

Knacken der Vigenère-Verschlüsselung

Gleiche Buchstabenfolgen im Geheimtext können auf zwei Arten entstehen:

1. Das gleiche Klartextwort wurde mit der gleichen Stelle des Schlüsselwortes codiert

Schlüssel	n	k	s	a	n	k	s	a	n	k	s	a	n	k	s	a	n	k	s	a	n	k	s	a	n	k	s	a	n	k
Klartext	j	a	i	m	e	l	e	n	n	i	s	t	e	r	i	s	t	d	e	r	k	o	e	n	i	g	s	m	o	e	r	d	e	r
Geheimtext	w	k	a	m	r	v	w	n	a	s	k	t	r	b	a	s	g	n	w	r	x	y	w	n	v	q	k	m	b	o	j	d	r	b

2. Gleiche Folgen sind zufällig entstanden? Bei einer Buchstabenfolge der Länge n≥3 eine sehr geringe Wahrscheinlichkeit

Knacken der Vigenère-Verschlüsselung

Um auf die Schlüssellänge zu schliessen, halten wir mehrfach vorkommenden Folgen mit ihrem jeweiligen Abstand zum nächsten Vorkommen fest:

Bsp: `ls`**`kdwv`**`rvsre`**`kdwv`**`sn`**`kdwv`**`ts` → Abstände 9 und 6

9 6

(Anzahl Buchstaben vom einen Beginn zum nächsten Beginn)

Die logische Schlussfolgerung daraus ist, dass jeder der Abstände das Schlüsselwort eine ganzzahlige Anzahl Mal enthalten muss. Es muss also die Länge des Schlüsselwortes ein Teiler aller aufgelisteten Abstände sein!

In der Regel versucht man es zunächst mit dem grössten gemeinsamen Teiler (ggT); im Bsp. also mit 3.

Symmetrische Verschlüsselung

1. Transposition: Skytale
2. Substitution
   - Monoalphabetisch: Cäsar
   - Polyalphabetisch: Vigenère, **One-Time-Pad**

One-Time-Pad

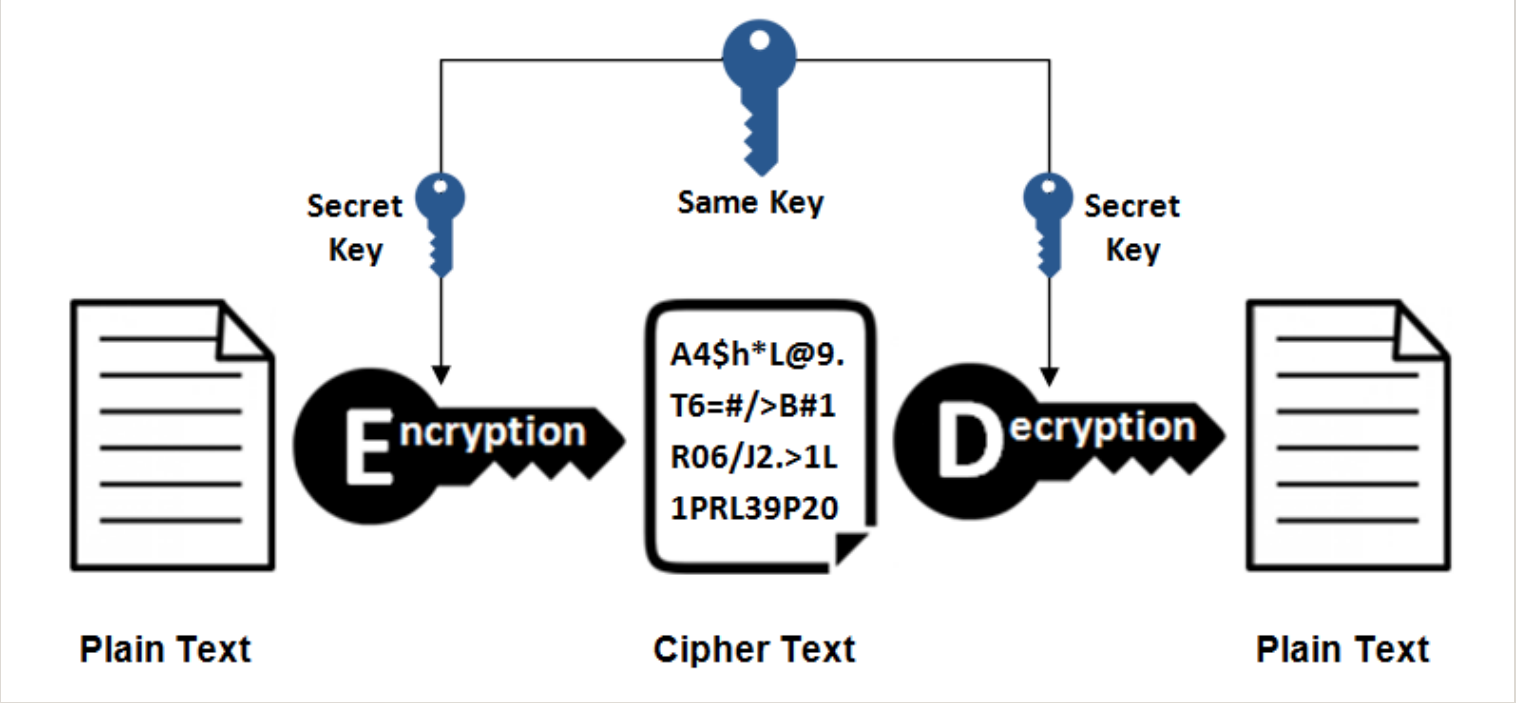
- Schlüsselcode zufällig
- nur einmal benutzt
- der Schlüssel ist genau so lang sein muss wie der zu verschlüsselnde Text.

Symmetrische Verschlüsselung

1. Transposition: Skytale
2. Substitution
   - Monoalphabetisch: Cäsar
   - Polyalphabetisch: Vigenère, One-Time-Pad

Symmetrische Verschlüsselung

- Derselbe Schlüssel dient dem Ver- und Entschlüsseln der Nachricht



Grafik von: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Probleme von symmetrischen Verschlüsselungen

- Der (eine) Schlüssel muss irgendwie zwischen Sender und Empfänger ausgetauscht werden

- Viele symmetrische Verfahren können mit statistischen Methoden geknackt werden

  - Das hat allerdings weniger mit der Symmetrie des Verfahrens zu tun, sondern damit, dass einzelne Zeichen ersetzt werden. In der modernen Kryptographie gibt es symmetrische Verfahren (z.B. AES), die diese Schwäche nicht aufweisen.

Geschichte der Kryptographie (8min)