Symmetrische Verschluesselung

Eine Einführung

Max (nopx) - max@noppelmax.online

August 22, 2018

Übersicht

Geschichte

- Die Nutzung von Chiffren reicht zurück bis 3000 v.Chr..
- Sie wurde hauptsächlich zu militärischen also auch diplomatischen Zwecken verwendet.[1]

Ziele

Bob möchte Alice über einen *unsicheren* Kanal *sicher* eine Nachricht übermitteln.

Statt der Nachricht M wird das Chiffrat C übermittelt.

$$\texttt{Alice} \xleftarrow{C} \texttt{Bob}$$

Anforderungen:

- Bob muss Chiffrat berechnen
- Alice muss Nachricht aus Chiffrat berechnen
- Chiffrat soll *Angreifer keine Informationen* über die Nachricht liefern.

Übersicht

Geheime Verfahren

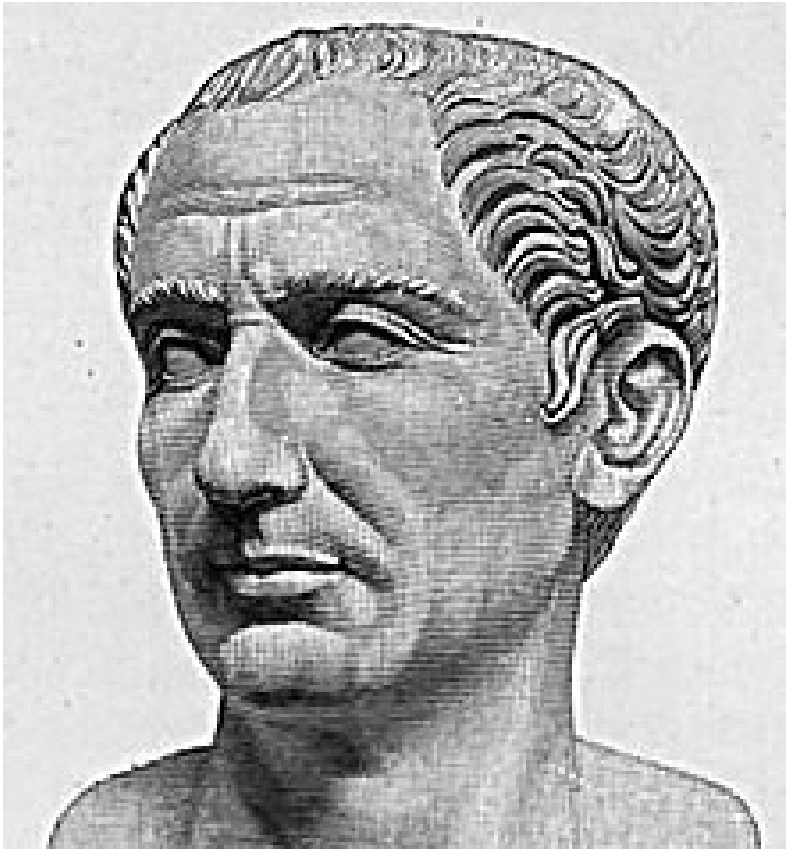
$C := Enc(M)$ und $M = Dec(C)$

Die beiden Funktionen *Enc* und *Dec* werden geheimgehalten.

$$\texttt{Alice} \xleftarrow{C:=Enc(M)} \texttt{Bob}$$

Nur Alice und Bob kennen *Enc* und *Dec*!

Cäsar



Julius Cäsar. Quelle: https://en.wikipedia.org/wiki/Caesar_cipher

Beispiel - Caesar3

`ABCDEFGHIJKLMNOPQRSTUVWXYZ` (plain)

`DEFGHIJKLMNOPQRSTUVWXYZABC` (cipher)

$$C_i = M_i + 3 \pmod{26}$$

Solche Verfahren werden **Substitutionsverfahren** genannt.

Beispiel - Caesar3

`ABCDEFGHIJKLMNOPQRSTUVWXYZ` (plain)

`DEFGHIJKLMNOPQRSTUVWXYZABC` (cipher)

Beispiel:

```
Plain:  THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
```

```
Cipher:  QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
```

Fun Fact: Wird immer noch verwendet!

Kerckhoffs's principle

Nachteile von Geheimen Verfahren

- Für jede Kommunikation eigenes Verfahren
- Wenn Verfahren bekannt, neues Verfahren. Aufwendig
- Geheime Algorithmen können rekonstruiert werden
- Fehler in öffentlichen Verfahren werden leichter entdeckt

Kerckhoffs's principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.[1]

[1] https://en.wikipedia.org/wiki/Kerckhoffs's_principle

Übersicht

1 Einführung

2 Geheime Verfahren

3 Substitution

4 Permutation

5 Stromchiffren

6 Blockchiffren

7 DES

8 Abschluss

Substitionsverfahren

- $C := Enc(K, M)$ und $M = Dec(K, C)$
- Die beiden Funktionen *Enc* und *Dec* sind öffentlich.
- Alice und Bob besitzen gemeinsames Geheimnis K.

$$\texttt{Alice} \xleftarrow{C:=Enc(K,M)} \texttt{Bob}$$

Monoalphabetische Substitution

Es wird nur ein Schlüsselalphabet verwendet.

Klartextalphabet:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimalphabet:	U	F	L	P	W	D	R	A	S	J	M	C	O	N	Q	Y	B	V	T	E	X	H	Z	K	G	I

Ein Monoalphabet. Quelle: https://de.wikipedia.org/wiki/Monoalphabetische_Substitution

Alphabeterzeugnung

- Es gibt mehrer Möglichkeiten ein Alphabet zu erzeugen.
- Caesar-Verschlüsselung (siehe später)
- Kennwort:

  `abcdefghijklmnopqrstuvwxyz`

  `REGNSCHIMABDFJKLOPQTUVWXYZ`

- Zufällig

  Das ergibt $26 * 25 * 24... = 26!$ viele mögliche Alphabete!
  Das entspricht 88 Bit!

Caesar

$$C_i = M_i + K \ (mod\ 26)$$

```
VSPACE

VSPACE (K=A)

WTQBDF (K=B)

XURCEG (K=C)

...
```

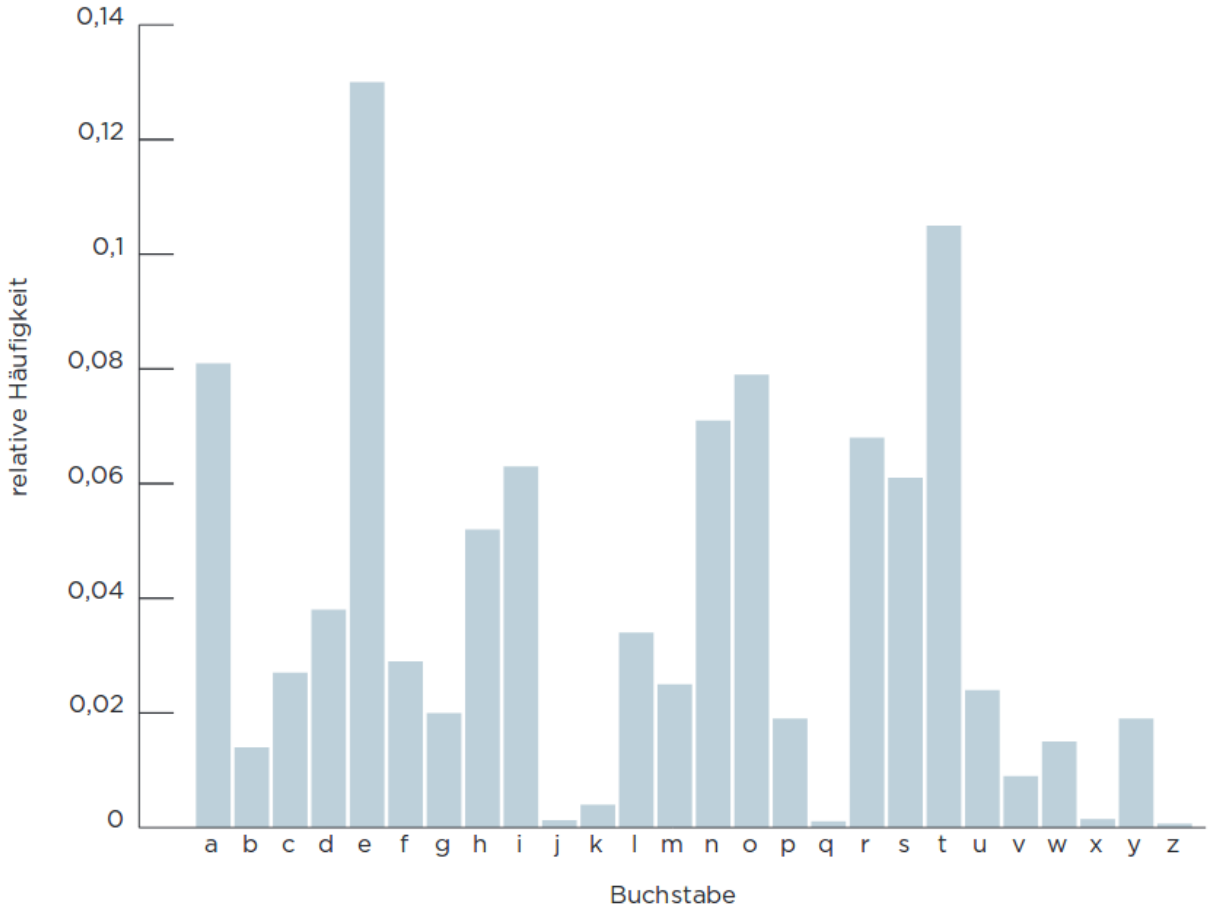
Caesar - Unsicherheit

- Annahme: *M sinnvoller* Text.
- Kleiner Schlüsselraum ($K \in \{0, ...25\}$)
- Häufigkeitsanalyse
- Bekannte Teiltexte

Häufigkeitsanalyse

- Ausnutzen linguistischer Besonderheiten der Klartextsprache
- Im Deutschen kommen die Buchstaben `e` und `n` am häufigsten vor.
- `c` folgt im Deutschen wie im Englischen häufig auf `h`. `h` jedoch äußerst selten auf `c`.
- Wörter wie `die`, `der`, `und`, `in`, `am`, `zu`, `den`, `das` und `nicht` kommen sehr häufig vor.[1]

Häufigkeitsanalyse



Rel. Häufigkeit von Buchstaben im Englischen. Quelle: [1]

Vigenère - le chiffre indéchiffrable

Blaise de Vigenère. Quelle: https://en.wikipedia.org/wiki/Vigenère_cipher

Vigenère - le chiffre indéchiffrable

- Wurde bis zur Mitte des letzten Jahrhunderts für unbrechbar gehalten.
- Der Schlüssel besteht jetzt aus mehr als einem Zeichen. Zum Beispiel `LEMON`.
- Das Schlüsselwort wird solange wiederholt bis es der Länge der Nachricht M entspricht.
- $M =$ `ATTACKATDAWN` dann wird $K =$ `LEMONLEMONLE`.

Vigenère - le chiffre indéchiffrable

- Wurde bis zur Mitte des letzten Jahrhunderts für unbrechbar gehalten.
- Der Schlüssel besteht jetzt aus mehr als einem Zeichen. Zum Beispiel `LEMON`.
- Das Schlüsselwort wird solange wiederholt bis es der Länge der Nachricht M entspricht.
- $M =$ `ATTACKATDAWN` dann wird $K =$ `LEMONLEMONLE`.

`ATTACKATDAWN` (M)

`LEMONLEMONLE` (K)

`LXFOPVEFRNHR` (C)

Vigenère - le chiffre indéchiffrable

Vigenère-Verschlüsselungen verwenden quasi mehrere Caesar-Verschlüsselungen.

Sie ist damit eine **polyalpabetische Substitution**.

Vigenère - le chiffre indéchiffrable

Schlüssel \ Klartext-Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Geheimtext

Schlüssel:	A	K	E	Y					
Klartext:	G	E	H	E	I	M	N	I	S
Schlüssel:	A	K	E	Y	A	K	E	Y	A
Geheimtext:	G	O	L	C	I	W	R	G	S

Vigenère Quadrat Quelle:
https://de.wikipedia.org/wiki/Polyalphabetische_Substitution

Vigenère - Kryptoanalyse

Was tun wir jetzt damit?

Vigenère - Kryptoanalyse

$$\begin{aligned}(C_1, C_2, ...) &= (M_1, M_2, ..., M_m, M_{m+1}, ...) \\ &+ (K_1, K_2, ..., K_m, K_1, ...)\ (mod\ 26)\end{aligned}$$

$$(C_1, C_{m+1}, ...) = (M_1 + K_1, M_{m+1} + K_1, ...)\ (mod\ 26)$$

Unterfolge $(C_1, C_{m+1}, C_{2m+1}, ...)$ Cäsar verschlüsslt mit K_1.

$\rightarrow$ Rate m und find $K_1, K_2, ...$ mit Häufigkeitsanalyse. (Kreuzkorrelation)

Vigenère - Kryptoanalyse

ATTACKATDAWN (M)

LEMONLEMONLE (K)

LXFOPVEFRNHR (C)

Vigenère - Kryptoanalyse ZUSATZ

Zusatz für CTF später.

Kreuzkorrelation für Schlüsselbuchstabe k:

$$K(k) = \sum_{i=0}^{25} < P_i, H_{i+k \ mod \ 26} >$$

mit $< a, b >= (a, b)^2$.

P_i sind die Häufigkeiten in der jeweiligen Sprache, H_i die gezählten der einzelnen Cäsarchiffren.

Vigenère - Kryptoanalyse

- Wie kommen wir an m?

Vigenère - Kryptoanalyse

- Wie kommen wir an m?
- Eine Möglichkeit ist die Autokorrelation mit Metrik $< \cdot, \cdot >$ und Periode d:

$$K(d) = \int_x < f(x), f(x+d) > dx$$

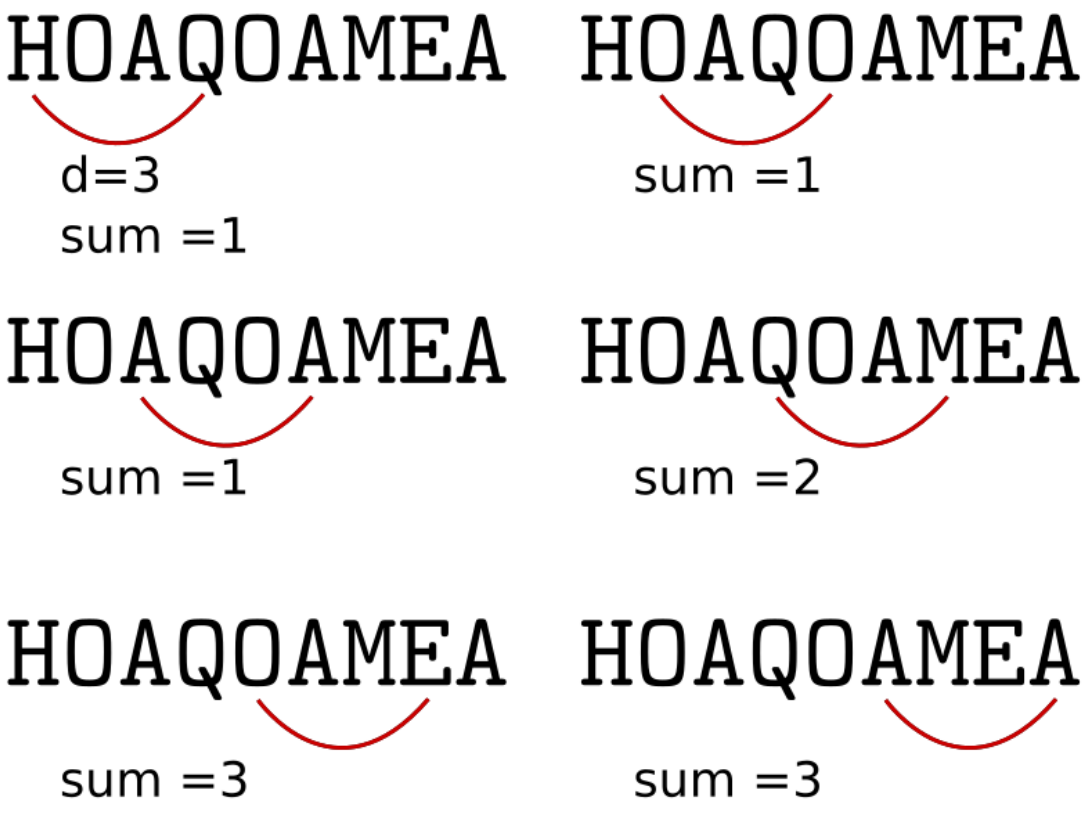
- Bei uns im diskreten Definitionsbereich also:

$$K(d) = \sum_{i=0}^{l-d} < a_i, a_{i+d} >$$

Vigenère - Kryptoanalyse

- Also auf Deutsch:
- Als Metrik verwenden wir Folgende: `0` falls beide Zeichen gleich sind, sonst `1`.
- Vergleich immer den aktuellen Buchstaben und den um die Periode verschobenen.

Vigenère - Kryptoanalyse



AutoCorrelation

Vigenère - Kryptoanalyse

Tragen wir verschiedene Perioden auf einem Diagram aus sehen wird die Periodenlänge:

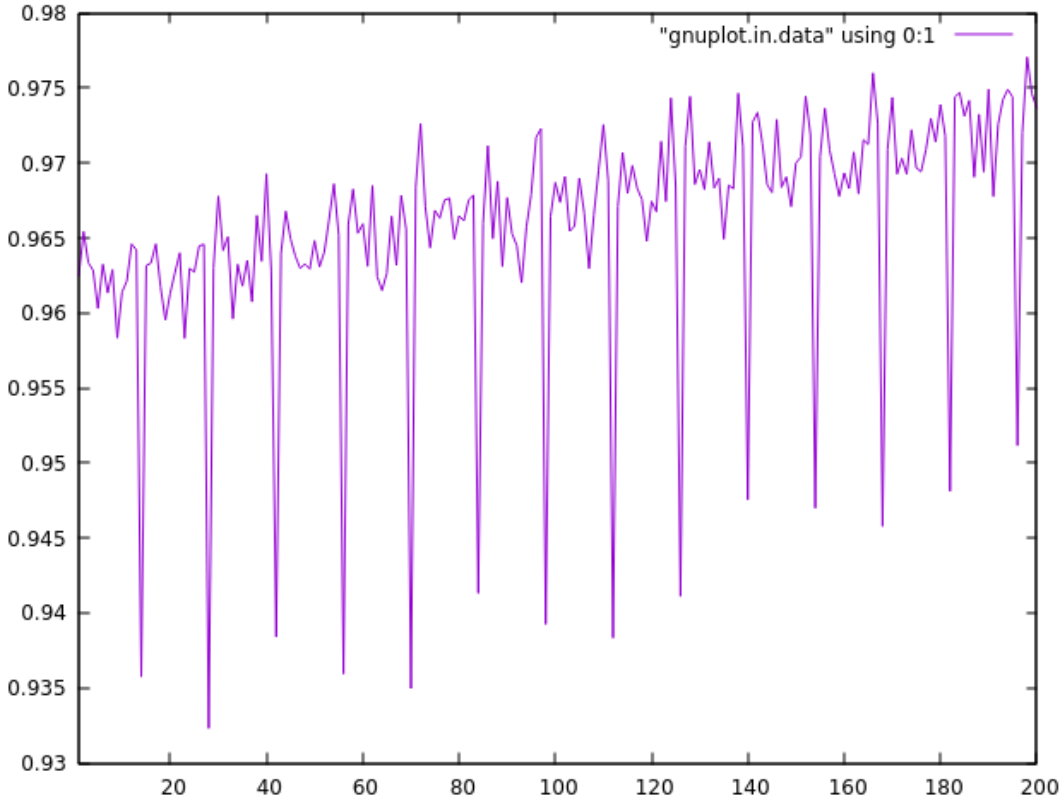


Diagramm mit Perioden 1 - 200

Vigenère - Kryptoanalyse

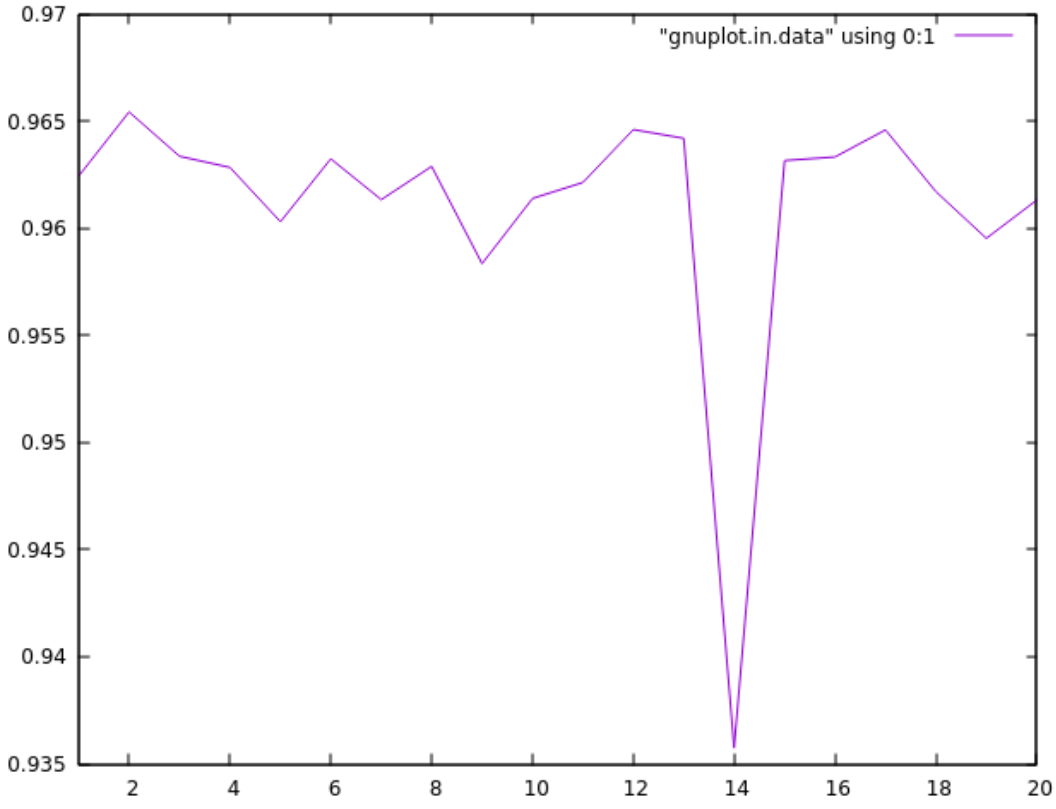


Diagramm mit Perioden 1 - 20

One-Time-Pad

- Wenn die Schlüssellänge der Länge der Nachricht entspricht $m = |M|$ wird es schwierig.
- Wir sprechen dann von einem **One-Time-Pad**!
- Das One-Time-Pad ist sicher!

  $C = M \oplus K$

One-Time-Pad - Nachteile

- Der Schlüssel ist so lang wie Nachricht
- Der Schlüssel darf nur einmal verwendet werden
- Wie Schlüssel übertragen?

Übersicht

Skytale

- 600 v.Chr wurden in Sparta Skytale zur Verschlüsselung verwendet.
- Pergament wurde um Stäbe gewickelt und beschrieben.
- Nur mit dem richtigen Stab konnte es wieder entschlüsselt werden.

Quelle: https://en.wikipedia.org/wiki/Scytale

Skytale

Solche Verfahren, die die Reihenfolge der Buchstaben vertauschen wurden **Transpositionsverfahren** oder **Permutationsverfahren** genannt.

Übersicht

Stromchiffren

- Die Nachteile des One-Time-Pads lassen sich umgehen
- Pseudozufall statt echten teurem Zufall
- Seed als Key
- Der Pseudozufallsgenerator spuckt immer neue Bits aus mit denen verschlüsselt wird.
- Schnell
- Stichwort: LFSRs

Übersicht

1 Einführung

2 Geheime Verfahren

3 Substitution

4 Permutation

5 Stromchiffren

6 Blockchiffren

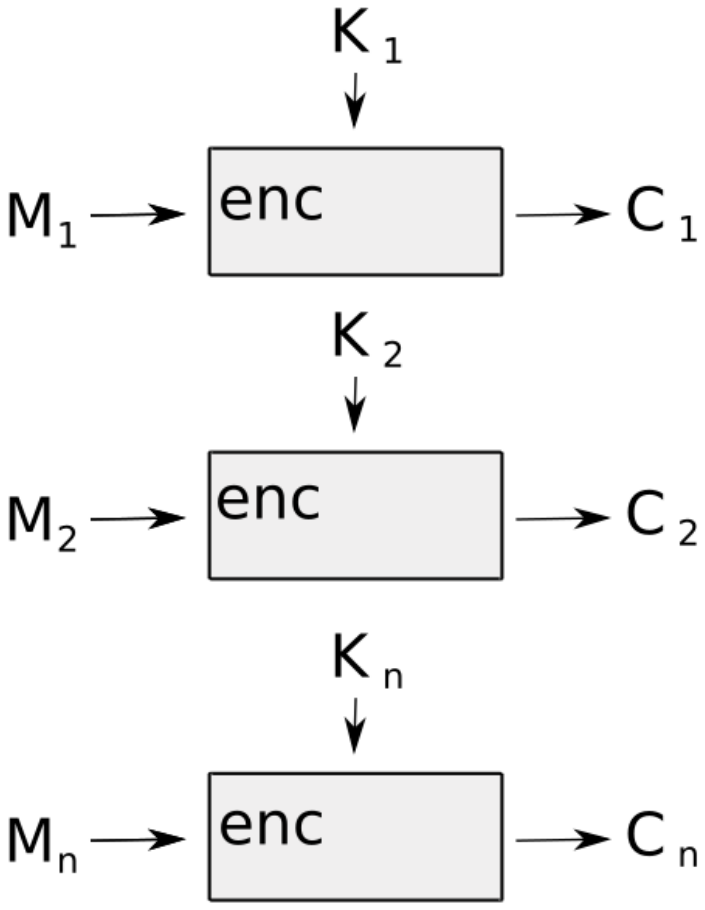
7 DES

8 Abschluss

Blockchiffren

- Arbeitet blockweise, Nachricht wird in Blöcke eingeteilt
- Jeder Block wird einzeln verschlüsselt
- Es gibt verschiedene Betriebsmodi für Blockchiffren mit unterschiedlichen Eigenschaften

Electronic Code Book Betriebsmodus



ECB Betriebsmodus

Electronic Code Book Betriebsmodus

Vorteile:

- einfach zu implementieren
- kein Zustands-Update, keine Synchronisation nötig

Nachteile

Electronic Code Book Betriebsmodus

Vorteile:

- einfach zu implementieren
- kein Zustands-Update, keine Synchronisation nötig

Nachteile

- Gleiche Nachricht $\Rightarrow$ Gleiches Chiffrat
- Einfügen und umsortieren von Chiffratblöcken möglich

Electronic Code Book Betriebsmodus

Vorteile:

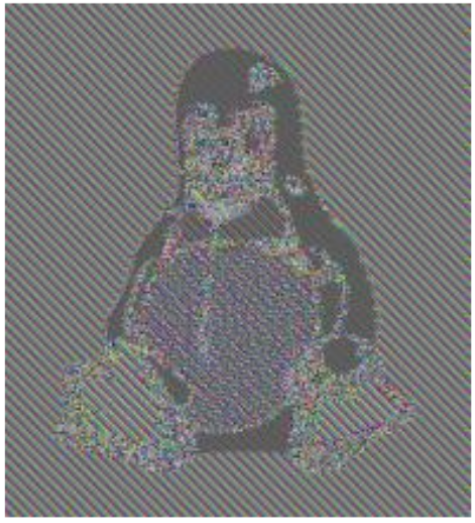
- einfach zu implementieren
- kein Zustands-Update, keine Synchronisation nötig

Nachteile

- Gleiche Nachricht $\Rightarrow$ Gleiches Chiffrat
- Einfügen und umsortieren von Chiffratblöcken möglich

Fun Fact: Bundestrojaner nutzt AES (gängige Blockchiffre) im ECB Modus (mit hartkodiertem Schlüssel)[2]

Electronic Code Book Betriebsmodus



ECB Betriebsmodus, Links Nachricht, Rechts Chiffrat [2]

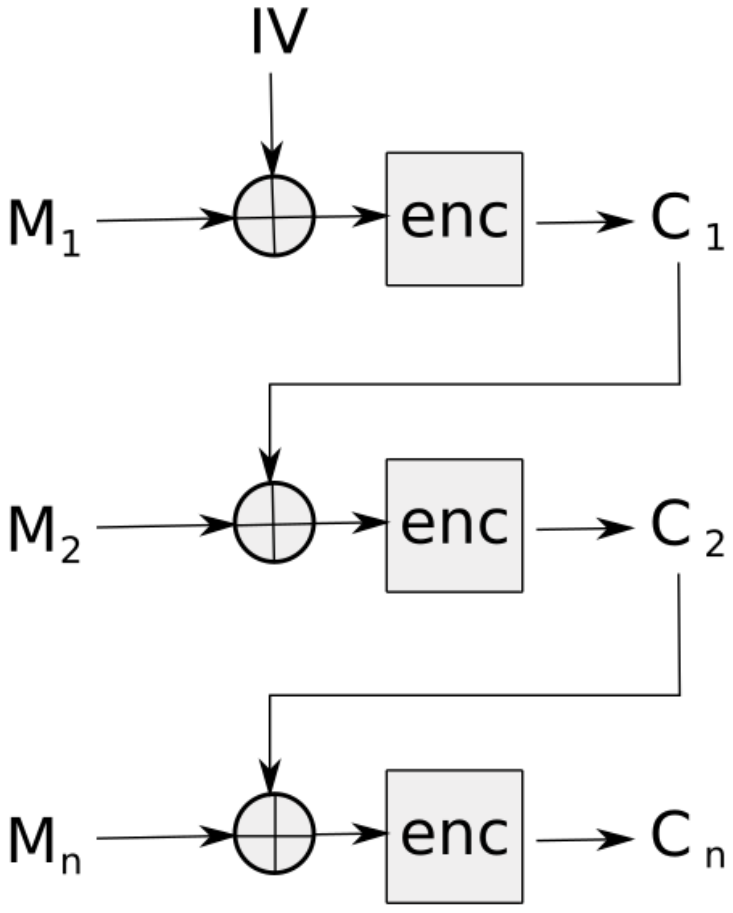
Cipher Block Chaining Betriebsmodus

- Problem des ECB: Chiffratblöcke 'unabhängig'

Cipher Block Chaining Betriebsmodus

- Problem des ECB: Chiffratblöcke 'unabhängig'
- Idee: Chiffratblöcke verketten

Cipher Block Chaining Betriebsmodus



CBC Modus

Cipher Block Chaining Betriebsmodus

- IV muss übertragen werden oder konstant sein
- IV ist nicht kritisch, kann also auch öffentlich sein.
- Vor und Nachteile?

Cipher Block Chaining Betriebsmodus

Vorteile

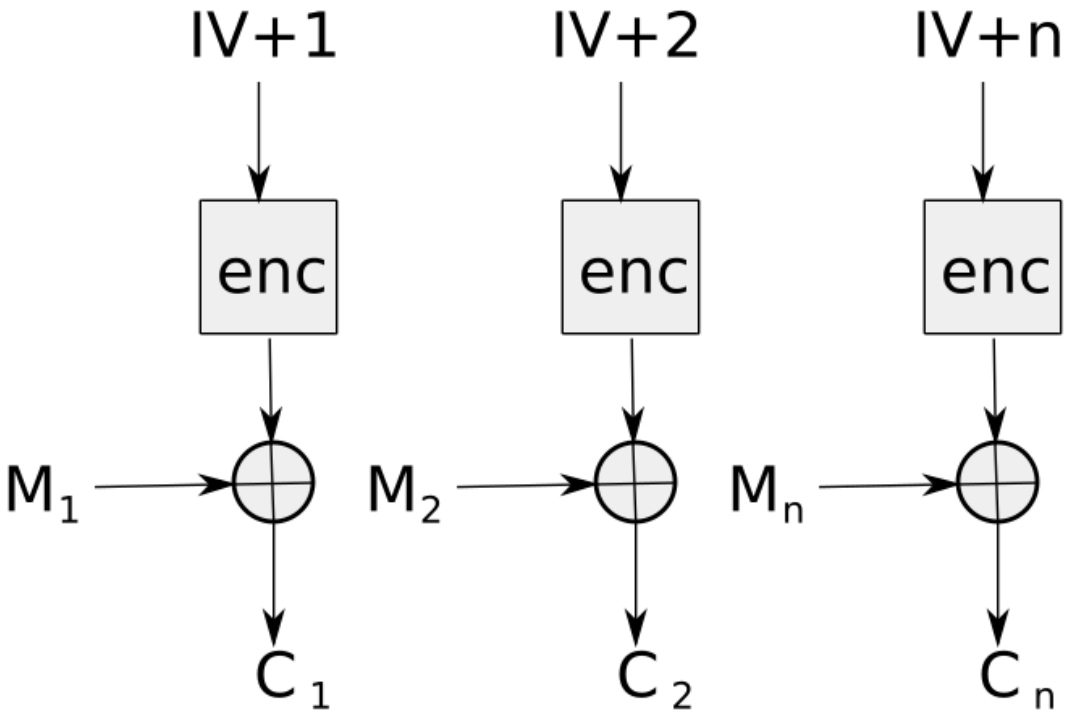
- Gleich Nachricht $\Rightarrow$ unterschiedliches Chiffrat (bei unterschiedl. vorherigen Chiffraten)
- Umsortierung führt zu fehlerhaften Blöcken

Nachteile

- Verschlüsselung nicht parallelisierbar
- Veränderbar (ändern von C_i ändert entschlüsselted M_i.), annähernde XOR Homomorphie
  - Angriffe auf TLS
  - Angriffe auf Linux Festplattenverschlüsselung[2]

[2] http://www.jakoblell.com/blog/2013/12/22/practical-malleability-attack-against-cbc-encrypted-luks-partitions/

Counter (CTR) Mode (ähnlich Stromchiffre)



CTR Modus

Counter (CTR) Mode

- Ähnlich wie eine Stromchiffre
- Auch homomorph veränderbar
- **Deshalb:** Galois Counter Mode (GCM)!
- Authentifizierter CTR Mode mit Prüfsumme
- Schützt gegen Manipulation der Chiffrate

Zusammenfassung Betriebsmodi

- ECB: "rohe" Funktion **nicht benutzen!**
- CBC, CTR: besser, schützt aber nur gegen Lauschangriffe
- GCM: Betriebsmodus der Wahl! Leider nicht überall unterstützt.

Übersicht

Geschichte DES

- 1973: National Bureau of Standards (NBS) der USA gab eine öffentliche Anfrage nach einem Algo- rithmus zum sicheren Verschlüsseln sensitiver Regierungsinformationen ab.
- 1974 entwarf IBM einen Kandidaten
- NSA überprüft und verändert den Algorithmus.
- Schlüssel wir von 128 auf 56 Bits verkürzt. Außerdem unkommentierte Änderungen an S-Boxen
- Befürchtung um Hintertür!

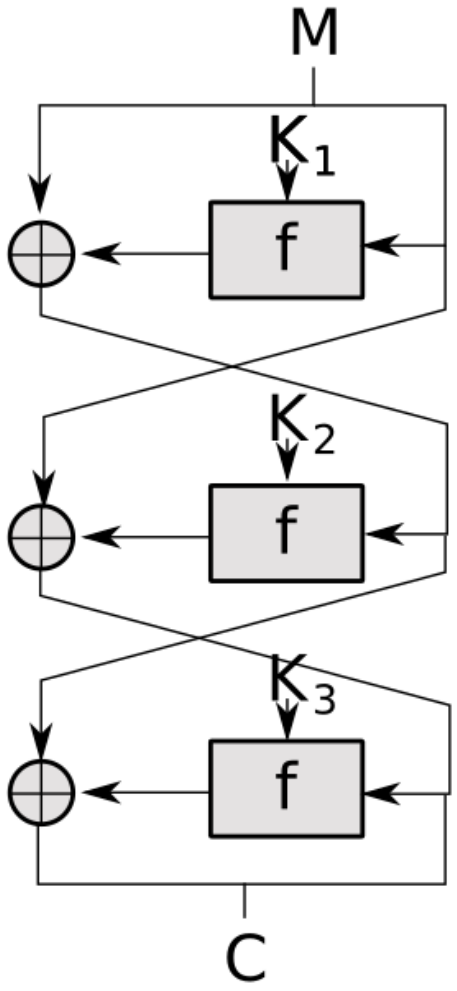
Geschichte DES

- Der Data Encryption Standard (DES) wird 1977 veröffentlicht und standardisiert.
- Schnell und weltweite Verbreitung
- 1994: Design Kriterien für S-Boxen von IBM veröffentlich.
- S-Boxen besonders resistent gegen 1990 veröffentlichte differentielle Kryptoanalyse
- Verdächtigung der NSA an dieser Stelle unberechtigt.

DES

- 16 Runden Feistel
- Verschlüsselt 64-Bit Blöcke, die je in zwei 32-Bit Blöcke aufgeteilt werden.
- Rundenfunktion F
- 56-Bit Schlüssel wir auf 16 Rundenschlüssel mit je 48 Bit *erweitert*.

Feistel-Netzwerk DES

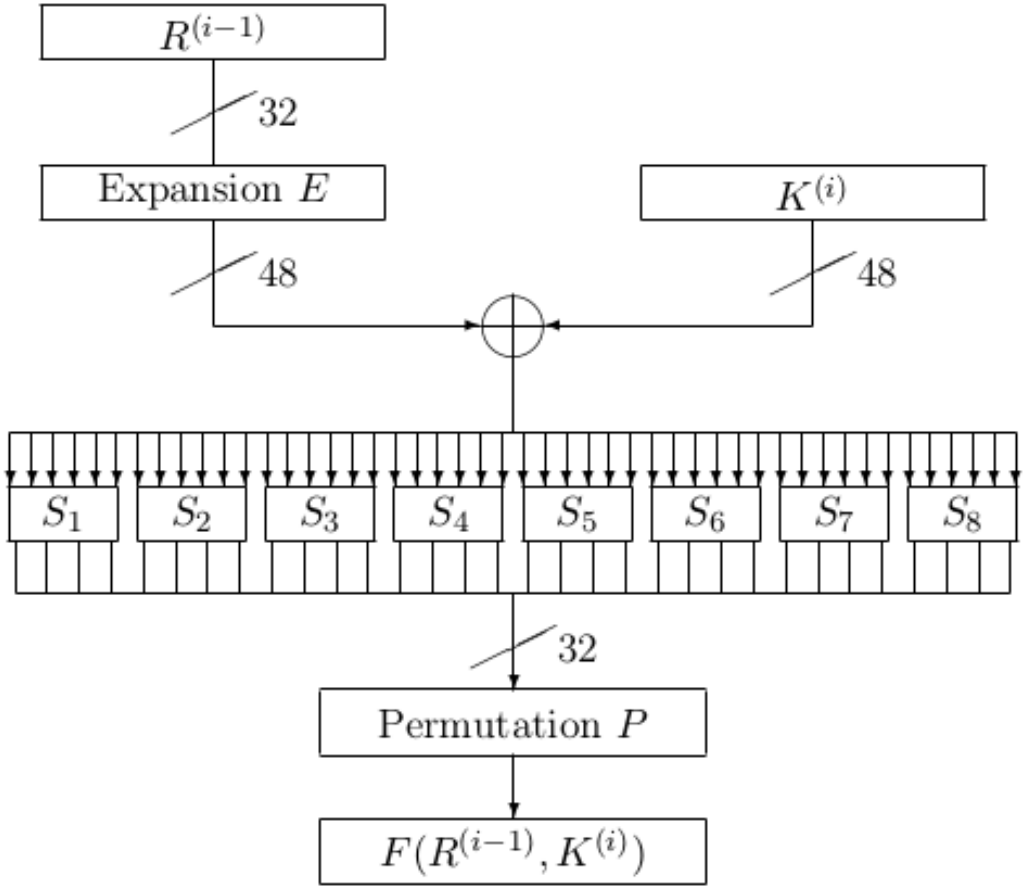


3-Runden Feistelstruktur des DES[2]

Feistel-Netzwerk DES

- F muss nicht invertierbar sein!
- Entschlüsselung wie Verschlüsselung nur mit Teilschlüsseln in umgekehrter Reihenfolge!

F Funktion DES



F Funktion des DES[2]

Fazit DES

- Der DES ist strukturell ungebrochen
- Es gibt Angriffe durch lineare Kryptoanalyse die besser als vollständige Suche sind.
- Brute-Force bricht die 56 Bit Schlüssel aber in akzeptabler Zeit (90er Jahre: innerhalb eines Tages!)
- **Reinen DES nicht mehr verwenden!**
- **Besser:** 3DES und AES

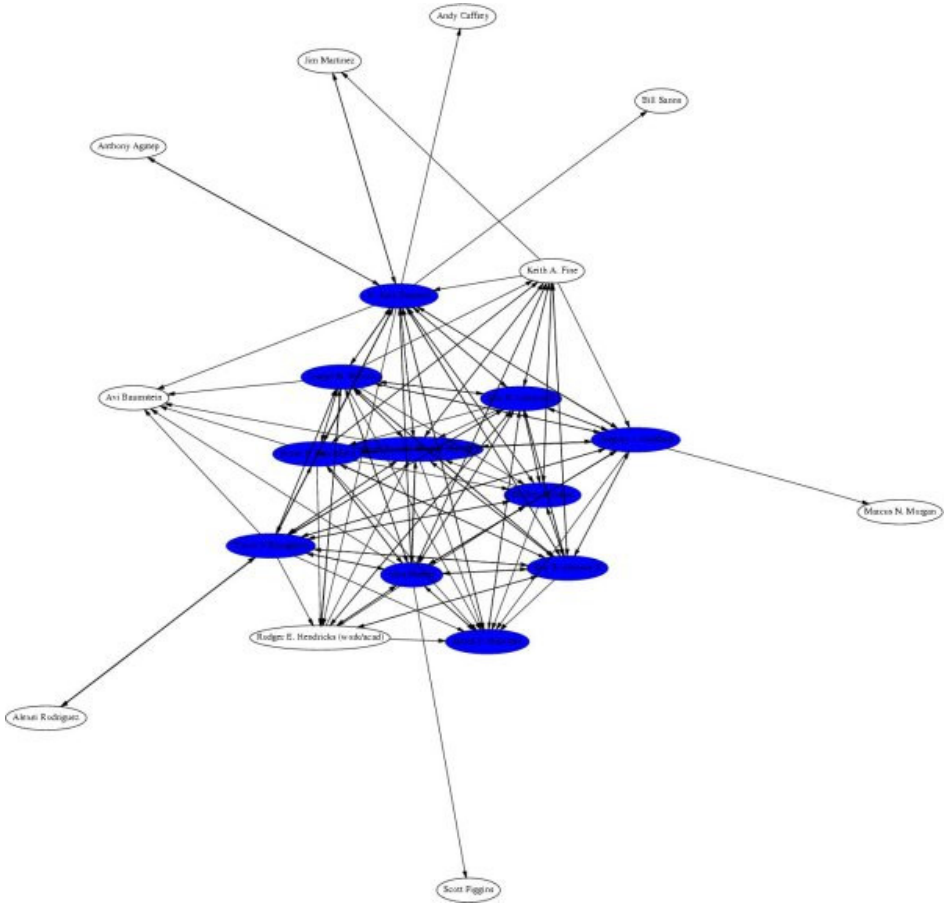
Übersicht

Buchtipps

- Simon Singh; Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.

KeySigning

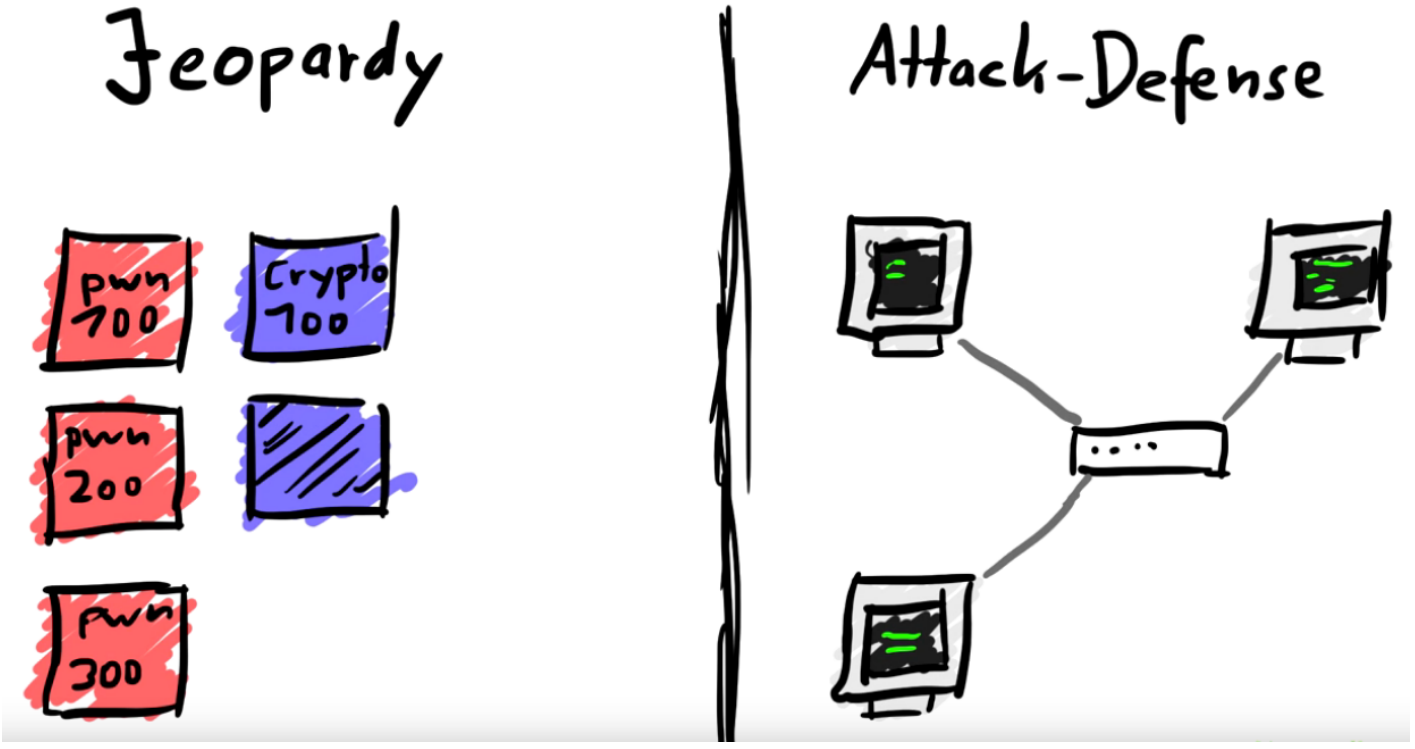
Wir treffen uns nachher noch zum PGP-KeySigning, wer Lust hat!



Security-CTF

- Hacking Wettbewerb
- Online oder Vor-Ort
- In Team oder Alleine
- Zwei Spielarten

Security-CTF



Quelle: https://www.youtube.com/watch?v=8ev9ZX9J45A

Security-CTF - Jeopardy

- In einem bestimmten Zeitraum werden Punkte gesammelt.
- Wer die meisten hat gewinnt.
- Aufgaben werden gelöst in dem man ein Flag findet.
- Flags sind oft in Dateien auf Servern, die man knacken muss
- Oder eben verschlüsselt wie in unserem Fall

Security-CTF - Jeopardy

- Ich habe einen kleinen CTF angelegt für uns.
- Jeder ist herzlich eingeladen mitzumachen, gerne auch in Teams!
- Die Aufgaben beginnen ganz einfach mit Caesar3
- Los gehts auf: http://10.10.0.21:4000

Literatur I

 Thawte Inc., “Die Geschichte der Chiffren,” 2013.

 Prof. Dennis Hofheinz, “Sicherheit,” 2018.