Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

SECURITY

Einführung Kryptographie

May 18, 2024

Marc Stöttinger

> Don't roll your own Crypto!
>
> Anonymous

WAS VERSTEHEN WIR UNTER KRYPTOLOGIE?

Kryptologie

Wissenschaft der Verfahren zur Geheimhaltung von Nachrichten, aber auch zu deren Berechnung. Kryptologie vereinigt Kryptographie und Kryptanalyse.

- **Kryptographie:**
  - Geheimschriftkunde – offen versendete Nachrichten sollen durch Verschlüsselung bzw. Chiffrierung für Unbefugte nicht lesbar sein.
- **Kryptanalyse:**
  - Meist mathematische und statistische Methoden zur Entzifferung von Geheimtexten, d.h. Informationen unbefugt erlangen.

WOZU BRAUCHEN WIR KRYPTOLOGIE?

- → Kryptologie ist als mathematische Disziplin wissenschaftlich fundiert und anerkannt.
- → Mathematik liefert – jedenfalls im Prinzip – Rechtfertigung für die „Stärke“ einer Sicherheitsmaßnahme.
- → Im Idealfall lässt sich beweisen, dass ein kryptographischer Algorithmus ein gewisses Sicherheitsniveau hat (oder eben nicht).
- → Damit kann der Nachweis erbracht werden, dass für eine bestimmte Anwendung der beanspruchte Sicherheitswert tatsächlich erreicht wird.

Achtung! Nachweis für benötigten Sicherheitswert

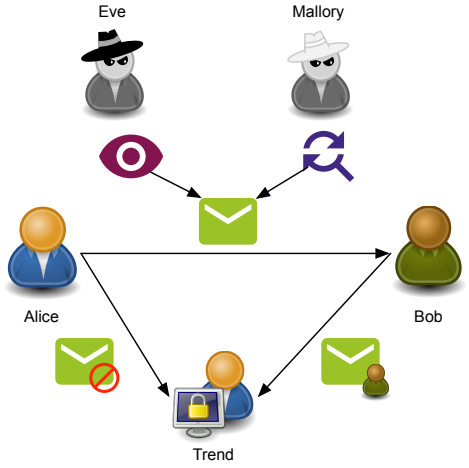
Design und Entwurf von Kryptographischen Algorithmen und Protokollen, benötigte Jahre Erfahrung in Zahlentheorie und Statistik, sowie der Implementierung!

WARUM MACHEN WIR DANN KRYPTOGRAPHIE HIER?!

- → Verstehen funktionaler Anforderungen an die Sicherheit von Verschlüsselungsverfahren
- → Anhand der Berechnungskomplexität sichere von unsicheren Verfahren unterscheiden können
- → Den Verwendungszweck von Betriebsmodi für Blockchiffren verstehen
- → Passende Betriebsmodi für einen einfachen Anwendungsfall auswählen können
- → Den Unterschied zwischen öffentlichem und privatem Schlüssel verstehen
- → In Grundzügen die mathematische Probleme kennen, auf denen asymmetrische Verfahren beruhen
- → Die Vor- und Nachteile von symmetrischen- und asymmetrischen Verfahren verstehen
- → Für einen gegebenen Kontext bestimmen können, ob ein symmetrisches, asymmetrisches oder hybrides Verschlüsselungsverfahren am geeignetsten ist

KRYPTOGRAPHIE SOAP OPERA

- → **Alice** will Nachricht an **Bob** senden
- → **Eve** (Eavesdropper) will Nachricht unbefugt lesen
- → **Mallory** (Malicious) will Nachricht unbefugt verändern oder sich als Alice ausgeben
- → **Trent** (Trusted Entity) ist eine vertrauenswürdige dritte Instanz, die Meinungsverschiedenheiten zwischen Alice und Bob klärt (z.B. ein Gericht)



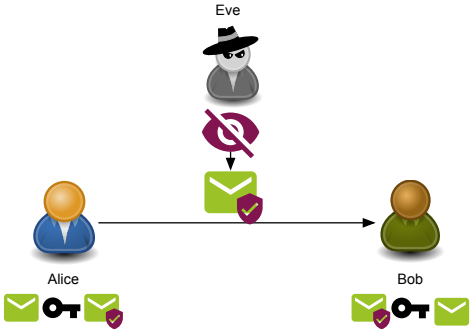
ANGRIFFSPOTENTIAL NACHRICHTENÜBERTRAGUNG

Sicherheitsziel	Beschreibung	Werkzeug	Kryptographie
Vertraulichkeit	Eve und Mallory sollen die Nachricht nicht lesen können	Verschlüsselung	X
	Bob soll nicht wissen, von wem die Nachricht kommt	Anonymisierung	
	Eve und Mallory sollen die Kommunikation nicht sehen	Steganographie	
Integrität	Änderungen der Nachricht von Mallory sollen erkannt werden	Hashfunktionen, Messages Authentication Codes, Digitale Signaturen	X
Authentizität	Bob will sichergehen, dass die Nachricht von Alice stammt	Message Authentication Codes, Digitale Signaturen	X
Verfügbarkeit	Die Nachricht muss bei Bob ankommen	Redundanz, Content Distribution	
Autorisierung	Andere Nutzende von Alice's oder Bob's Computer dürfen die Nachricht nicht senden oder sehen	Access Control	
Verbindlichkeit	Alice kann die Nachricht im Nachhinein nicht leugnen	Digitale Signaturen	X

VERTRAULICHKEIT DURCH VERSCHLÜSSELUNG

→ **Bedrohung:**
Eve liest die Nachricht mit

→ **Ziel:**
Personen ohne den entsprechenden Schlüssel können keine Informationen aus verschlüsselter Nachricht gewinnen



DEFINITIONEN

Symbol	Bezeichnung	Erklärung
P	Plaintext/Klartext	Nachricht im Klartext
C	Ciphertext/Chiffretext	Verschlüsselte Nachricht
K_E	Verschlüsselungs-schlüssel	Schlüssel der zum Verschlüsseln der Nachricht verwendet wird.
K_D	Entschlüsselungs-schlüssel	Schlüssel der zum Entschlüsseln der Nachricht verwendet wird. Muss basierend auf K_E berechnet werden ($K_D = f(K_E)$.
$C = Enc_{K_E}(P)$	Verschlüsselungsfunktion	Verschlüsselt den Plaintext P zum Ciphertext C unter Verwendung des Schlüssels K_E.
$P = Dec_{K_D}(C)$	Entschlüsselungsfunktion	Entschlüsselt den Ciphertext C zum Plaintext P unter Verwendung des Schlüssels K_D. Es gilt: $P = Dec_{K_D}(Enc_{K_E}(P))$.

Im Fall von symmetrischen Verschlüsselungsverfahren ist $K_E = K_D = K$. Bei asymmetrischen Verschlüsselungsverfahren gilt $K_E = K_{\text{public}}$ und $K_D = K_{\text{private}}$.

MONOALPHABETISCHE SUBSTITUTION - CAESAR CHIFFRE

→ Ersetze jeden Buchstaben mit dem Buchstaben K Positionen weiter hinten im Alphabet:

Plaintext	A	B	C	D	...	Z
Ciphertext	E	F	G	H	...	D

→ Einfache Vorschrift:
$C_i = P_i + K \pmod{n}$

→ Für binäre Daten kann eine XOR-Operation statt der Addition genutzt werden.

→ Behält allerdings die statistische Verteilung der Buchstaben bei!

Plaintext

CRYPTOGRAPHY, or writing in cipher, the art of writing in such a way as to be incomprehensible except to those who possess the key to the system employed. The unravelling of the writing is called deciphering.

Ciphertext

```
Oah!c.4aY!5hutMPtUPGRGLEtGLtAGNFCPu
RFCtyPRtMDtUPGRGLEtGLtQSAFtytUyWtyQ
RMtzCtGLAMKNPCFCLQGzJCtCVACNRtRM
RFMQCtUFMtNMQQCQQtRFCtICWtRMtRFC
QWQRCKtCKNJMWCBvtcFCtSLPyTCJJGLEtMD
RFCtUPGRGLEtGQtAyJJCBtBCAGNFCPGLEv
```

POLYALPHABETISCHE SUBSTITUTION - VIGENÈRE CIFFRE

- Im Gegensatz zur monoalphabetischen Substitution werden hier viele („poly“) Geheimalphabete zum Ersetzen der Buchstaben genommen:

Plaintext	H	e	l	l	o	...
Schlüssel	3	1	4	3	1	...
Ciphertext	K	f	p	o	p	...

- Einfache Vorschrift:
  $C_i = P_i + K_{i \pmod m} \pmod n$
- Wenn $m \ll n$ ergeben sich wieder statistische Strukturen

Plaintext

```
CRYPTOGRAPHY, or writing in cipher,
the art of writing in such a way as
to be incomprehensible except to
those who possess the key to the
system employed. The unravelling of
the writing is called deciphering.
```

Ciphertext

```
JaWS62OZkNUV5R5bcUplGwHoUgA7,466lP9
GvydZpG7i1MgyGrlAupq.8Fr,3MZcU!BioM
dmi!!RZ.jMksEsBm.qv!fOM3EAcsGjNw
rulmOMgoM8sBGMmcqiqbOM9lW8wBjNp3
FvmaV,cCksyCSm2 iQbOMeuP!yrzFq.eil;
6ltuuvHCv58vp4YR sCb!qswq;froc9XW
```

PERFEKTE GEHEIMHALTUNG - ONE-TIME PAD

→ Substitution wobei P und K gleich lang sind

Plaintext	A	U	F	S	T	A	N	D
Schlüssel	J	A	T	U	C	O	B	I
Ciphertext	J	U	Y	M	V	O	O	L

→ Einfache Vorschrift:
$C_i = P_i + K_i \pmod{n}$

→ Das Verfahren ist allerdings nicht praxistauglich, da der Schlüssel
  → genauso lang sein muss wie die Nachricht
  → wirklich zufällig generiert werden muss

Plaintext

```
CRYPTOGRAPHY, or writing in cipher,
the art of writing in such a way as
to be incomprehensible except to
those who possess the key to the
system employed. The unravelling of
the writing is called deciphering.
```

Ciphertext

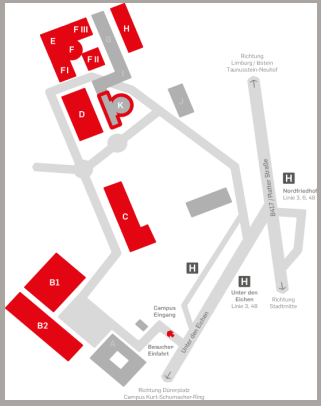
```
Vga04vNzlC.thq;t5Yk9p,8, O,luvmpXKX
hMI4LahiScEG92mAdqa!C8uzzXT6GZ,uQ2J
9SfEWdvdnI;UDroO1e8y1fPfMqXvHL G
QQy.8,l3Gm;7sP1O6 ;L t.OLtX;s3nN
!wSYa8wshgwYQx;HXdnNMosXRV2SooTsIZ2
EG4lXe,9UQyEahM.Q,2KPjLx6S;rJ;5Pcx
```

DISKUSSION IN KLEINEN GRUPPEN

Tauschen Sie sich mit Ihrem Nachbarn 5 Minuten aus:

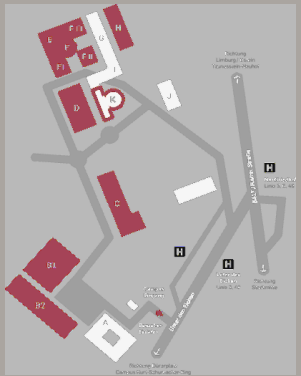
→ Diskutieren Sie darüber wieviel von der Campuskarte zu erkennen ist, wenn diese mit den verschiedenen Verschlüsselungsverfahren verschlüsselt wird.

Original



AUSWIRKUNG VON VERSCHLÜSSELUNG

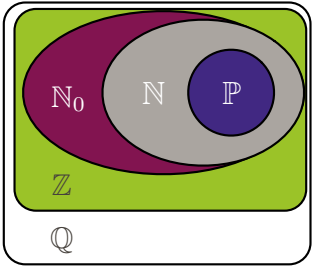
Caesar



Vigenère

MENGEN

- → $\mathbb{N}$: Menge aller positiven Zahlen **ohne** Null: $\{1, 2, 3, ...\}$
- → $\mathbb{N}_0$: Menge aller positiven Zahlen **mit** Null: $\{0, 1, 2, 3, ...\}$
- → $\mathbb{Z}$: Menge aller ganzen Zahlen: $\{...,-3, -2, -1, 0, 1, 2, 3, ...\}$
- → $\mathbb{P}$: Menge aller Primzahlen: $\{2, 3, 5, 7, 11, 13, ...\}$
- → $\mathbb{Q}$: Menge der rationalen Zahlen: $\left\{\frac{a}{b} \in \mathbb{Z}, b \neq 0, ggT(a,b) = 1\right\}$
- → $\mathbb{Z}_m$ Restklassenring modulo m: $\{1, 2, 3, ..., m - 1\}$



OPERATOREN

- → a plus b: $a + b$
- → a mal b: $a \cdot b$
- → a teilt b: $a \mid b \Rightarrow (\exists x \in \mathbb{Z})\, b = x \cdot a$
- → a teilt nicht b: $a \nmid b \Rightarrow (\exists x \in \mathbb{Z})\, b \neq x \cdot a$
- → Größter gemeinsamer Teiler von a und b: $x = ggT(a, b)$
- → Kleinstes gemeinsames Vielfaches von a und b: $x = kgV(a, b)$
- → Divisionsrest, wenn man a durch b teilt: $x = a \mod b$

MONOID $(M, \circ)$

- $(M, \circ)$ ist ein algebraisches System
- M ist eine nicht leere Menge $M = \{a, b, ...\}$
- $\circ$ ist ein Operator auf Elemente aus M, $\circ \in \{+ \text{ oder } \cdot\}$
- Ein Monoid hat folgend Eigenschaften:
  1. Nicht leere Menge: $a, b \in M \Rightarrow a \circ b \in M$
  2. Assoziativ Gesetz: $a, b, c \in M \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$
  3. Neutrales Element: $a \in M \Rightarrow \exists e, a \circ e = e \circ a = a$
     - Addition: $e = 0$
     - Multiplikation $e = 1$

GRUPPE $(G, \circ)$

- G ist eine nicht leere Menge $G = \{a, b, ...\}$
- $\circ$ ist ein Operator auf Elemente aus G, $\circ = \{+ \text{ oder } \cdot\}$
- Ein Gruppe hat folgend Eigenschaften:
  1. Ist ein Monoid: $(G, \circ), \exists e = 0$ bzw. 1
  2. Inverses Element: $a \in G \Rightarrow \exists a', a \circ a' = e$
     - Addition: $a' = -a$
     - Multiplikation $a' = a^{-1}$
- Eine Gruppe bei der das Kommutativ-Gesetz gilt, ist eine Abelsche Gruppe: $a, b \in G \Rightarrow a \circ b = b \circ a$
- Eine Algebra $(G, \circ)$ heißt Halbgruppe, wenn sie in Bezug auf die Operation $\circ$ dem Assoziativgesetz genügt.
- Sie wird kommutative Halbgruppe genannt, wenn die Operation $\circ$ zusätzlich kommutativ ist.

RING $(R, +, \cdot)$

- R ist eine nicht leere Menge $R = \{a, b, ...\}$
- Operator auf Elementpaare aus R, $+, \cdot$
- Ein Ring hat folgend Eigenschaften:
  1. Ist eine Ablsche Gruppe: $(R, +), \exists e = 0$ und $\exists a' = -a$
  2. Distributiv-Gesetz: $a, b, c \in R \Rightarrow a \circ (b + c) = (a \circ b) + (a \circ c)$
  3. ist ein Monoid: $(R, \cdot), a \in R : \exists e = 1$ und $\exists a' = -a$
  4. Inverses Element: $a \in R \Rightarrow \exists a', a \circ a' = e$
     - Es existiert zwar ein **inverses Element $a' = -a$** bezüglich der Addition aber **keine multiplikative Inverse**.

KÖRPER $(K, +, \cdot)$

- K ist eine nicht leere Menge $K = \{a, b, ...\}$
- Operator auf Elementpaare aus K, $+, \cdot$
- Ein Körper hat folgend Eigenschaften:
  1. Ist ein kommutativer Ring mit Einselment:
     - $(K, +, \cdot), a \in K$ mit $a \neq 0 \Rightarrow \exists a^{-1} \in K$ mit $a \cdot a^{-1} = 1$
- Jeder Körper $(K, +\cdot)$ ist **nullteilerfrei**
  - Def.: Nullteilerfrei: $\forall a, b \in K$ gilt: $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$
- $\mathbb{Z}_m := \{0, 1, ..., m-1\}$ ist **genau dann** ein Körper, wenn **m** eine Primzahl ist. $\mathbb{Z}_p$ mit $p \in \mathbb{P}$ ist ein Körper.

ALGEBRA ÜBERSICHT

Struktur				Bez.	Formel (Axiom)
Algebra (A, + , •)		Algebra (A, +)			
Körper	Ring	abelsche Gruppe	additive Gruppe HG	assoz.	a + (b + c) = (a + b) + c
				∃ 0	0 + a = a
				∃ - a	a + (- a) = 0
				komm.	a + b = b + a
				distri.	a (b + c) = a b + a c
		Algebra (A_0 , •)			
	Einselem.	abelsche Gruppe	multipl. Gruppe HG	assoz.	a (b c) = (a b) c
				∃ 1	1 a = a
				∃ a^{-1}	$a\ a^{-1} = 1$
				komm.	a b = b a

MODULARE ARITHMETIK

→ für $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ gibt es eindeutige Quatienten $q \in \mathbb{Z}$ mit Rest r mit:

1. $q = \frac{a}{n}$
2. $r = a \mod n$

→ Rechenregeln für Modulare Arithmetik:

- → Addition: $(a \mod n) + (b \mod n) = a + b \mod n$
- → Subtraktion: $(a \mod n) - (b \mod n) = a - b \mod n$
- → Multiplikation: $(a \mod n) \cdot (b \mod n) = a \cdot b \mod n$
- → Exponentation: $(g^a \mod n)^b \mod n = (g^a)^b \mod n = g^{a \cdot b} \mod n$

DEFINITION RESTKLASSE

- Modulo n sind alle Werte $a = i \cdot n + r$ für $i \in \mathbb{Z}$ äquivalent.
- Die Menge $\{i \cdot n + r \mid i \in \mathbb{Z}\}$ wird als Restklasse von r bezeichnet, wobei r ein Repräsentant der Restklasse ist.
- Die Menge aller Restklassen modulo n wird geschrieben als $\mathbb{Z}_n$.
- Zwei Zahlen $a, b \in \mathbb{Z}$ heißen restgleich, wenn $a \mod n = b \mod n \Rightarrow a \equiv b \mod n$ (a ist **kongruent** zu b modulo n).
- Beispiel: $\mathbb{Z}_3$ (Zahlen aus $\mathbb{Z}$ modulo 3) besteht aus den folgenden Restklassen:
  - Restklasse für $r = 0 : \{\dots, -9, -6, -3, 0, 3, 6, 9 \dots\}$
  - Restklasse für $r = 1 : \{\dots, -8, -5, -2, 1, 4, 7, 10 \dots\}$
  - Restklasse für $r = 2 : \{\dots, -7, -4, -1, 2, 5, 8, 11 \dots\}$

RING UND RESTKLASSENRING

- Ein Ring $< R, +\cdot >$ist eine algebraische Struktur bei der:
  - $< R, \cdot >$ eine **Halbgruppe** bildet
  - $< R, + >$ eine **abelsche Gruppe** bildet
  - Distirbutivgestze gelten:
    - Linke Distributivität: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ für $\forall a, b, c \in R$
    - Rechte Distributivität: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ für $\forall a, b, c \in R$
- Ein Ring $< \mathbb{Z}_n, +\cdot >$ über einer Restklasse $\mathbb{Z}_n$ wird als **Restklassenring** bezeichnet.

BEISPIEL RESTKLASSENRING $(\mathbb{Z}_6, +, \cdot)$

$< \mathbb{Z}_6, + >$ ist eine Gruppe:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$< \mathbb{Z}_6, \cdot >$ ist eine Halbgruppe:

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Zusätzlich zur Halbgruppe:

- → $< \mathbb{Z}_6, \cdot >$ hat das neutrale Element 1
- → $< \mathbb{Z}_6, \cdot >$ ist für manche Elemente invertierbar

INVERTIERBARKEIT DER MULTIPLIKATION

→ Für $< \mathbb{Z}_n, \cdot >$ sind nicht alle Elemente invertierbar

→ Aber: Teilerfremde Zahlen $z \in \mathbb{Z}$ zu n sind invertierbar ($ggT(n, z) = 1$)

Ergebnistabelle $< \mathbb{Z}_6, \cdot >$

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Für $< \mathbb{Z}_6, \cdot >$ sind nur 1 und 5 invertierbar

Ergebnistabelle $< \mathbb{Z}_5, \cdot >$

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

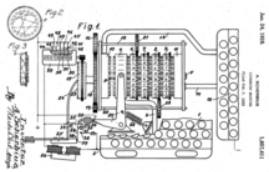
Für $< \mathbb{Z}_5, \cdot >$ sind nur 1, 2, 3, 4 invertierbar, da 5 eine Primzahl ist.

HILL-CHIFFRE

- Entwickelt von Lester S. Hill; 1891-1961, US-amer. Mathematiker, Lehrer und Kryptograph
- Ausgangslage:
  - Restklassenring
  - In einem Körper existieren die **modular Inversen**
- Algorithmus:
  - Verschlüsselung: $\mathbf{C} = \mathbf{K} \cdot \mathbf{P} \mod p$
  - Entschlüsselung: $\mathbf{P} = \mathbf{K}^{-1} \cdot \mathbf{C} \mod p$
  - $\mathbf{C}, \mathbf{P}, \mathbf{K}$ sind Matrizen

WAS BEDEUTET SICHERHEIT?

- → Enigma wurde im 2. Weltkrieg zur Verschlüsselung genutzt
  - → Verschlüsselung basiert auf Polyalphabetische Substitution
  - → Analyse war aufgrund komplexer Rotormechanik sehr schwierig
- → Um Ciphertexte zu entschlüsseln, nutzten die Alliierten verschiedene Tricks:
  - → Teile des Plaintexts waren bekannt (Datum, Absendername,...)
  - → Inhalt bestimmter Nachrichten konnte frei gewählt werden (Alliiertes Schiff hat an Position X gehalten)
- → Angriffsmodelle werden genutzt, um diese Angriffe zu formalisieren
  - → Moderne Verschlüsselungsverfahren müssen bestimmten Angriffsmodellen standhalten



Quelle: **https://de.wikipedia.org/wiki/Enigma_%28Maschine%29** - letzter Besuch 02.04.23

ANGRIFFSMODELLE

Beispiel: Abfangen von Alices‘s stud.ip Passwort

→ Kontext: Eve ist im selben Raum wie Alice und fängt alle verschlüsselten Pakete ab

→ Ziel von Eve: Die Zugangsdaten von Alice

Angriffsmodel	Beschreibung	Beispiel Szenario
Ciphertext-Only	Eve ist nur der Ciphertext bekannt	Nur verschlüsselte Zugangsdaten sind bekannt.
Known-Plaintext	Eve erhält zufällige Plaintext/Ciphertext Paare	Alice loggt sich auf ihrem Konto ein und surft auf bekanntem Teil von stud.ip
Chosen-Plaintext	Eve hat Zugriff auf ein Verschlüsselungsorakel, das beliebige Plaintexte verschlüsselt	Eve sendet eine Nachricht an Alice. Alice loggt sich ein und ruft Eve‘s Nachricht ab.
Chosen-Ciphertext	Eve hat Zugriff auf ein Entschlüsselungsorakel, das beliebige Ciphertexte entschlüsselt	Eve hat für begrenzte Zeit Zugriff auf Alice‘s Gerät mit verschlüsselter Sitzung (ohne bestehenden Login) und lässt sich manipulierte verschlüsselte Nachricht entschlüsseln. Alice kommt später wieder und loggt sich auf Webseite ein.

DISKUSSION IN KLEINEN GRUPPEN

Tauschen Sie sich mit Ihrem Nachbarn 5 Minuten aus:

- → In welchen Angriffsmodellen ist die monoalphabetische Substitution sicher?
- → Gibt es eine Hierarchie unter den Angriffsmodellen?

Angriffsmodelle
Ciphertext-Only
Known-Plaintext
Chosen-Plaintext
Chosen-Ciphertext

KRYPTANALYSE

Kryptanalyse beschäftigt sich mit Methoden und Techniken, um Verschlüsselungen zu brechen. Das Brechen eines Kryptoverfahrens ist in folgende Kategorien eingeteilt:

- **absolut sicher:**
  - wenn nicht genug Information gewonnen werden kann, um hieraus den Klartext oder den Schlüssel zu rekonstruieren.
- **analytisch sicher:**
  - wenn es kein nichttriviales Verfahren gibt, mit dem es systematisch gebrochen werden kann.
- **komplexitätstheoretisch sicher:**
  - wenn es keinen Algorithmus gibt, der das Kryptoverfahren in Polynomialzeit in Abhängigkeit der Schlüssellänge brechen kann.
- **praktisch sicher:**
  - wenn kein Verfahren bekannt ist, welches das Kryptoverfahren mit vertretbarem Ressourcen-, Kosten- und Zeitaufwand brechen kann.

PRAKTISCHES QUANTIFIZIEREN DER SICHERHEIT (1/2)

- Krypto Verfahren sind in der Praxis “ungebrochen”, solange **Brute-Force** der effizienteste Angriff ist
  - **Brute-Force:** Testen aller möglichen Schlüsselkombinationen
  - Komplexität der Brute-Force Angriffe steigt exponentiell in der Schlüssellänge

- Es existieren verschiedene Stufen des **Brechens**
  - **Theoretisch Gebrochen:** Ein effizienterer Angriff als Brute-Force wird bekannt
  - **Überholt:** Der Aufwand fällt unter eine Grenze, die mit viel Rechenkapazität erreichbar wäre
  - **Praktisch Gebrochen:** Ein Angriff wurde demonstriert

- Solange ein Verfahren noch nicht als überholt gilt, reden wir von **``Rechnerischer Sicherheit''**

PRAKTISCHES QUANTIFIZIEREN DER SICHERHEIT (2/2)

Rechnerische Sicherheit: Ein Krypto Verfahren ist zwar theoretisch zu brechen, praktisch existieren aber nicht genug Zeit oder Ressourcen

Anzahl der Schlüsselbits	Anzahl der Schlüsselkombinationen	Zeitaufwand für Brute-Force in Jahren (Annahme: Pro Kombination eine Operation der gesamten Top500 Supercomputer mit $4,9 \cdot 10^{18}$ Operationen pro Sekunde in Nov 2022)	Beispielverfahren
8 8 unsicher	256	0	—
32 32 unsicher	4.294.967.296	0	—
64 64 unsicher	$1,84 \cdot 10^{19}$	0	Simon32/64
80 80 unsicher	$1,21 \cdot 10^{24}$	0.008	PRESENT
128	$3,40 \cdot 10^{38}$	$2,20 \cdot 10^{12}$	AES-128
192	$6,28 \cdot 10^{57}$	$4,06 \cdot 10^{31}$	Serpent-192
256	$1,58 \cdot 10^{77}$	$7,49 \cdot 10^{50}$	Chacha20

KERCKHOFFS PRINZIP

- Wie kann garantiert werden, dass ein Verfahren auch wirklich sicher ist?
  - Wurden Angriffe beim Design übersehen? [Tews12]
  - Haben Entwickler Hintertüren in das Verfahren eingebaut? [BD+21]

- **Kerckhoffs Prinzip:** Die Sicherheit des Verfahrens muss auf der Geheimhaltung des Schlüssels beruhen anstatt auf der Geheimhaltung des Verfahrens selbst
  - Klassische Kryptographie ist geprägt vom Wechselspiel zwischen Kryptographie und Krypanalyse (Erkenntnisse $\Rightarrow$ Entwicklungen).
  - Die Sicherheit eines Kryptosystems darf nicht von dessen Geheimhaltung, sondern nur von der Schlüssellänge abhängen.

- Seien $\mathcal{P}, \mathcal{C}, \mathcal{K}$ die Mengen der Plaintexte, Chiffretexte bzw. Schlüssel und $\mathcal{E} : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{C}$ ein Verschlüsselungssystem. Ist ein Kryptoanalytiker im Besitz eines Plaintext-Chiffretextpaares $(P, C) \in \mathcal{P} \times \mathcal{C}$, so kann der verwendete Schlüssel K durch vollständige Suche ermittelt werden, da $\mathcal{E}(P, K) = C$ gelten muss.

STANDARDISIERUNG VON KRYPTOALGORITHMEN

- Kryptoverfahren werden via öffentlicher Ausschreibung standardisiert
  - Jede Person darf ein Verfahren einreichen
  - Verfahren müssen Rahmenbedingungen einhalten (z.B., transparentes Design, Schlüssellänge)
  - Die Verfahren werden über mehrere Jahre von Experten analysiert
  - Der Gewinner wird aus der Menge der übrig gebliebenen Verfahren ausgewählt

- Standardisierungsprozesse von der NIST:
  - Advance Encryption Standard (AES) - 2000
  - Kryptographische Hashfunktionen SHA3 - 2015
  - Lightweight Kryptographie - Gewinner bestimmt in 2023
  - Post-Quanten Kryptographie (PQC) - aktiv seit 2017

ZUSAMMENFASSUNG

- → Funktionale Anforderungen an die Sicherheit von Verschlüsselungsverfahren verstehen
- → Anhand der Berechnungskomplexität sichere von unsicheren Verfahren unterscheiden können
- → In Grundzügen die mathematischen Probleme kennen, auf denen asymmetrische Verfahren beruhen