Kryptographie
WS 2022/23

Vorlesungen: Montags, 13:00–14:30, Sr K 2077 und Dienstags, 09:00–10:30, Sr H 2509
(Achtung: Einzelne Termine werden ausfallen. Gesamtstundenzahl: 46.)
Übungen: Mittwochs (U), 11:00–12:30, Sr K 2035 (Philipp Schlag)

Martin Dietzfelbinger

Stand: 21. Oktober 2022

Für: Studierende der Informatik (Bachelor, Wahlpflichtbereich „Algorithmen, Automaten und Komplexität“ und „IT-Sicherheit“) und Interessierte.

Modulprüfung: schriftlich, 90 Minuten.

Literatur:

* Ralf Küsters und Thomas Wilke: Moderne Kryptographie, Vieweg + Teubner 2011 („modern“, Vorlesung orientiert sich an diesem Buch).
* Jonathan Katz und Yehuda Lindell, Introduction to Modern Cryptography, Second Edition, CRC Press, 2015 (weitergehendes „modernes“ Buch).
- Dan Boneh und Victor Shoup, A Graduate Course in Applied Cryptography, `https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf`.
- Ulrike Baumann, Elke Franz, Andreas Pfitzmann, Kryptographische Systeme, SpringerVieweg 2014 („klassisch“, näher an der Praxis).
- Albrecht Beutelspacher, Heike B. Neumann, Thomas Schwarzpaul: Kryptografie in Theorie und Praxis, Vieweg, 2005 („klassisch“, gute Einführung).
- Douglas R. Stinson: Cryptography - Theory and Practice, CRC Press, 1995 („klassisch“, sehr umfangreich).
- Dietmar Wätjen: Kryptographie, Spektrum Akademischer Verlag, 2004 („klassisch“)
- David Kahn: The Codebreakers, Scribner, 1996 (Interessante Details aus der Geschichte).
* **Material über Moodle2.**

$\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$ – kryptos (griech.): verborgen; $\gamma\rho\acute{\alpha}\phi\varepsilon\iota\nu$ – graphein (griech.): schreiben.

Kryptographie im klassischen Wortsinn betrifft also Methoden, Nachrichten so zu schreiben, dass sie „verborgen“ bleiben, das heißt von keinem Unberechtigten (mit)gelesen werden können. Das hier angesprochene „Sicherheitsziel“ heißt „Vertraulichkeit“ oder „Geheimhaltung“ oder *Konzelation*[1]. Verfahren, die dieses Ziel erreichen, heißen *Konzelationssysteme*.

Simples Schema für dieses Problem (Aktion schreitet von links nach rechts fort, zu Schlüsseln später mehr):

Senderin Alice hat *Klartext* x	Verschlüsselung (Chiffrierung)	*Chiffretext* y über unsicheren *Kanal*	Entschlüsselung (Dechiffrierung)	Empfänger Bob rekonstruiert *Klartext* x
	[↑] [Schlüssel k]	$\Longrightarrow$ ↓ Gegnerin Eva (enemy, eavesdropper, Kryptoanalytiker/in, Angreifer/in)	[↑] [Schlüssel k']	

„**A**lice“ ist dabei ein eingebürgerter Name für die sendende Instanz, „**B**ob“ der für die empfangende Instanz. Dabei kann es sich um Personen, Organisationen oder auch Computer(systeme) o. ä. handeln. Der Verschlüsselungsbereich von Alice (links von der ersten senkrechten Linie) ist gegen Zugriffe von Eva *geschützt*, ebenso der Entschlüsselungsbereich von Bob (rechts von der zweiten senkrechten Linie).

Beispiel 1: Alice = Bank (und ihr Computersystem), Bob = Online-Bankkunde, Nachricht x = Kontoauszug. Übermittlung des Kontoauszugs über das Internet („offener Kanal“). Sicherheitsziel: Stelle sicher, dass die Angreiferin Eva (der Internetkriminelle) die vertrauliche Information nicht mitlesen kann, obgleich sie die verschlüsselte Version y der Nachricht sehen kann.

Beispiel 2: Alice = Bob = eine Universität. Nachricht x = die Liste aller persönlichen Daten aller Studierenden. Diese große Datei soll auf einem Cloudserver (im Ausland) gespeichert werden. Dazu wird sie als y verschlüsselt, um Zugriffe dritter Parteien auf die vertraulichen Daten zu verhindern.

Im Kontext der modernen elektronischen Kommunikation ergeben sich neben der Kon-

[1] *concelare* (lat.): sorgfältig verbergen, davon englisch: *conceal*.

zelation auch weitere, andersartige und *unabhängige* Aufgaben, die mit kryptographischen Methoden, also von Kryptosystemen ausgeführt werden. Wir führen auf:

- **Konzelation: Geheimhaltung/Vertraulichkeit/Zugriffsschutz**
  (kein Unberechtigter kann Nachrichteninhalt mithören oder mitlesen)
- **Integrität/Fälschungsschutz**
  (stelle sicher, dass Nachrichten auf dem Übertragungsweg nicht manipuliert worden sind)
- **Authentizität/Signaturen: Garantiere Absenderidentität**
  (Bob kann *kontrollieren*, dass Nachricht vom behaupteten Absender Alice kommt)
- **Nichtabstreitbarkeit**
  (Bob kann gegenüber Dritten beweisen, dass die Nachricht in der empfangenen Form vom behaupteten Absender Alice kam)
- ...

Integrität bzw. **Authentisierung**: Hier ist die Aufgabenstellung verändert. Eva hat nicht nur die Fähigkeit, Nachrichten passiv mitzulesen, sondern sie kann in den Kommunikationskanal eingreifen. Sie kann Nachrichten abfangen (und sogar die Weiterleitung verhindern) und/oder eine neue bzw. veränderte Nachricht in den Kanal einspeisen. Ihre Absicht ist es, Bob dazu zu bringen, diese Nachricht für die echte von Alice abgeschickte Nachricht zu halten. Diese Art von Angriff soll verhindert werden. Hierfür verwendet man einen Mechanismus, der *message authentication code* (MAC) heißt. Darunter kann man sich eine Funktion vorstellen, die aus einer Nachricht x einen (nicht allzu langen) Code $\text{mac} = \text{MAC}(x)$ berechnet. Diese Funktion ist ein Geheimnis von legitimen Sendern von Nachrichten an Bob. Inbesondere kann Eva bei gegebener Nachricht x' (verwandt zu x oder nicht) keinen korrekten MAC für x' berechnen. Bob verfügt über ein Prüfverfahren, das es ihm erlaubt, ein empfangenes Paar (x, mac) darauf zu testen, ob der zweite Teil der zu x gehörende MAC-Wert ist. Wenn Alice die einzige Instanz ist, die die geheime Funktion MAC kennt, dann kann Bob sogar überprüfen, ob Alice tatsächlich die Absenderin ist.

Senderin Alice hat *Text* x	S-Bearbeitung (authentisieren, signieren) [↑] [Schlüssel k]	Text + MAC: (x, mac) $\Longrightarrow$ ↕ Gegnerin Eva (Ziel: Nachricht ändern oder eigene Nachricht mit Identität „Alice“ senden)	E-Bearbeitung Text auf Unversehrtheit bzw. Absenderidentität prüfen [↑] [Schlüssel k']	Empfänger Bob hat (*geprüften*) *Text* x

Wieder ist der Arbeitsbereich von Alice gegen Zugriffe der Gegnerin Eva geschützt, ebenso der Arbeitsbereich von Bob.

Beispiel 3: Alice = Bankkundin, Bob = Bank, Nachricht = Überweisungsauftrag.
Integrität: Stelle sicher, dass Eva nicht Aufträge von Alice, obgleich über offenen Kanal (Internet) übermittelt, abfangen und durch manipulierten oder ganz neuen Auftrag ersetzen kann (nicht Kontonummern oder Beträge ändern kann).

Authentizität: Eva soll nicht, ohne Aktivität von Alice, der Bank vortäuschen können, dass sie Alice ist, und Aufträge erteilen.

Die **Nichtabstreitbarkeit** ist eine noch stärkere Anforderung an Geschäftsvorgänge, die über das Internet abgewickelt werden. Bei Streit (vor Gericht) soll die Bank *nachweisen* können, dass ein Auftrag, den sie ausgeführt hat, tatsächlich von Alice stammt. (Im analogen Leben wird dies durch eine als echt nachgewiesene Unterschrift bewirkt.) Hier übernimmt also sogar Alice, die Kundin, die Rolle der Gegenspielerin.

Die Kryptographie im engeren und „klassischen“ Sinn beschäftigt sich mit Verfahren, um in verschiedenen Kommunikationsszenarien eine gegen Angriffe von Gegnern (Mitlesen, Verändern, Unterschieben, Abstreiten) abgesicherte Kommunikation zu ermöglichen.

Auf der anderen Seite steht die Kryptoanalyse (englisch *cryptanalysis*). Ursprünglich und jahrhundertelang entwickelten Kryptoanalytiker Methoden zum „Brechen“ von Konzelationssystemen, also zum unberechtigten Mitlesen trotz Verschlüsselung. Heute gehören zur Kryptoanalyse auch Angriffe auf andere kryptographische Methoden, mit dem Ziel, ihre Sicherungsfunktion zu umgehen. Es ist wichtig, im Auge zu behalten, dass die Gleichsetzung von Kryptoanalyse mit der Absicht, unberechtigt in die Kommunikation einzugreifen, nicht unbedingt richtig ist. Um die Sicherheit von kryptographischen Verfahren sicherzustellen, ist es unbedingt nötig, dass mit kryptoanalytischen Methoden versucht wird, Schwachstellen solcher Verfahren offenzulegen. Erst die Kenntnis von Schwachstellen macht es möglich, diese zu beseitigen.

Eine klassische Einteilung ist also folgende:

Kryptologie = Kryptographie (Entwicklung von kryptographischen Verfahren) + Kryptoanalyse (Versuche, kryptographische Verfahren zu brechen).

Für sehr lange Zeit war (und ist auch immer noch) die Beziehung zwischen diesen beiden Seiten die eines Katz- und Maus-Spiels. Die Kryptographie war bestrebt, immer cleverere und „sicherere“ Verfahren zu entwickeln, die Kryptoanalyse versuchte, Schwächen in diesen Verfahren aufzuspüren, und zwar sowohl, um unberechtigte Zugriffe auszuführen, als auch, um die Schwächen offenzulegen, um ihre Beseitigung zu ermöglichen. (Die Liste der jemals vorgeschlagenen Systeme und Verfahren, die sich früher oder später als „schwach“ erwiesen, ist sehr lang.)

Eine Randbemerkung: Man könnte auf den ersten Blick den Eindruck bekommen, dass das Anliegen, Nachrichten vertraulich und ohne Manipulationen auszutauschen, zunächst einmal legitim ist und dass Angriffe illegitim sind. Dieser Eindruck wird eventuell durch die Verwendung der harmlosen Bezeichnungen „Alice“ und „Bob“ für die Kommunikationsparteien einerseits und „Eva“ (Gegnerin, Angreiferin, usw.) andererseits verstärkt. Sicherlich ist diese Sicht für viele Situationen insbesondere in der Geschäftswelt passend. Es zeigt sich aber nach kurzem Überlegen, dass nicht in allen Fällen der Schutz das legale oder moralisch gute Ziel sein muss, dass kryptographische Verfahren auch für rechtswidrige, unethische, gefährliche, völkerrechtswidrige, terroristische Zwecke eingesetzt werden (können) und die Kryptoanalyse, das Eingreifen in solche Kommunikation, manchmal rechtlich und moralisch geboten ist. Man landet hier schnell bei interessanten und schwierigen ethischen Fragen. Wie sehr viele Technologien, natürlich eigentlich die gesamte IT und die Informatik, ist die Kryptologie eine Wissenschaft, deren verschiedene Ergebnisse und Entwicklungen für erstrebenswerte wie auch für schlimme Ziele benutzt werden können – wir sind hier beim grundlegenden Thema „Dual Use“.

Seit den 1980er Jahren wurde eine neue Sicht auf die Kryptologie entwickelt. Dabei schlägt man für verschiedene Kommunikationsszenarien und Sicherheitsziele (Konzelation, Integrität, Authentisierung, Nichtabstreitbarkeit, usw.) ganz präzise mathematische Formulierungen vor, so genannte Sicherheitskonzepte. Anschließend ist man, wenigstens im Prinzip, in der Lage, Verfahren darauf abzuklopfen, ob sie diese präzise formulierten Sicherheitsanforderungen erfüllen.

Die *„moderne“ Kryptologie* beschäftigt sich also mit kryptographischen Verfahren, mit kryptoanalytischen Verfahren, mit Sicherheitskonzepten und mit mathematischen Methoden zur Untersuchung dieser Dinge, abstrakt und an konkreten Verfahren. *Achtung*: Man findet (heute noch mehr als früher) oft die Bezeichnung „Kryptographie“ bzw. „cryptography“ für die gesamte Kryptologie. Dies betrifft auch alle Titel von Büchern, die trotz des Namens „Kryptographie“ bzw. „cryptography“ alle Aspekte behandeln.

Ein Zitat aus dem Buch von Katz und Lindell: ***Moderne Kryptographie*** *ist die Wissenschaft von den mathematischen Methoden, die man benutzen kann, um digitale Information, Systeme und verteilte Anwendungen gegen Eingriffe („Angriffe") von unberechtigten Parteien zu schützen.* Dabei geht es sowohl um die *Konstruktion* von kryptographischen Systemen und um die *Entwicklung und Untersuchung von Angriffen* als auch um *Beweise* für die *Sicherheit von Systemen.*

Leider sind die Sicherheitsbeweise in den allermeisten Fällen relativ zu unbewiesenen (aber wenigstens plausiblen) mathematischen oder komplexitätstheoretischen oder kryptographischen Annahmen.

In der Vorlesung folgen wir zum Teil den klassischen Ansätzen, aber stellen auch den modernen Ansatz im Prinzip vor und verstehen ihn an ausgewählten Beispielen.

Bei der Diskussion im Stil des modernen Ansatzes muss man immer die folgenden Komponenten beschreiben: Was ist die Kommunikationssituation, welches sind die Akteure, was ist das Sicherheitsziel? Bei Konzelationssituationen gibt es Alice und Bob, wobei Alice eine Nachricht oder mehrere Nachrichten an Bob übermitteln möchte. Gegenspielerin Eva kann die gesendeten Nachrichten mitlesen und hat eventuell Zugriff auf einige Klartext-Chiffretest-Paare, aber sie kann nicht anderweitig eingreifen. Das Sicherheitsziel ist grob gesprochen, dass Eva aus einem Chiffretext y keine „nichttrivialen Informationen" über den Klartext x erlangen kann. (Ein „triviale Information", die sie immer erhält, ist die Tatsache, dass eine Nachricht geschickt wurde.) Es gibt mehrere Präzisierungen dieser Situation, die von folgenden Faktoren abhängen:

- Art der Kommunikation;
- Evas Fähigkeiten und Möglichkeiten (kann sie nur mitlesen oder auch Nachrichten einschleusen?)
- was wir als „nichttriviale Information" bezeichnen.

Wir werden zumindest in einfachen Situationen präzise definieren, was es heißt, „das Sicherheitsziel zu erreichen" und dabei die Komplexität der Anforderungen schrittweise erhöhen. Exemplarisch wird diskutiert werden, wie Verfahren für einfachere Situation zu Verfahren für kompliziertere Verfahren ausgebaut werden können.

Schließlich muss noch kurz das Konzept „Schlüssel" diskutiert werden. Wir beginnen mit einem Beispiel, nämlich einem jahrtausendealten Konzelationssystem.

Beispiel: Cäsar-Chiffre. Betrachte das antike lateinische Alphabet mit 21 Buchstaben:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Cäsar ließ Texte verschlüsseln, indem er folgende Ersetzung Buchstabe für Buchstabe durchführen ließ:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	A	B	C

(Man nimmt immer den Buchstaben, der im Alphabet drei Positionen „weiter rechts“ steht, mit „wraparound“ am Ende.) Beispiel: Klartext $x =$ `IMPETVS` („Angriff“) wird durch $y =$ `MPSHABX` verschlüsselt. Der Nachteil ist offensichtlich: Wer den Trick kannte, konnte jede Nachricht mitlesen.

Eine einfache „Verbesserung“ dieses sehr primitiven Ansatzes ist Folgendes: Verschiebe zyklisch um eine andere Anzahl von Buchstaben als 3. Für eine Verschiebung um $k = 9$ Positionen ergibt sich:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧
K	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I

Um hier die Verschlüsselung und die Entschlüsselung durchzuführen, musste man als „*Schlüssel*“ nur das Bild von `A` kennen (im Beispiel `K`), alternativ die Verschiebeweite k als Zahl. Es gibt dann 21 Schlüssel (wobei zunächst „`A`“ oder Verschiebeweite 0 zunächst ziemlich sinnlos erscheint). Diese Methode heißt *Verschiebechiffre*.

Eine ziemlich naheliegende Verallgemeinerung von Verschiebechiffren ist auf den ersten Blick viel mächtiger: Sie sagt, dass das Bild eines Buchstabens ein ganz beliebiger anderer Buchstabe sein soll. Dabei müssen natürlich verschiedene Buchstaben auf verschiedene Buchstaben abgebildet werden. Es ergibt sich eine „Substitutionschiffre“, die durch eine Tabelle mit ganz beliebiger Buchstabenanordnung gegeben ist. *Beispiel*:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧	↧
F	Q	M	P	K	V	T	A	E	L	H	N	I	G	D	S	B	X	O	R	C

Wenn man hier ver- und entschlüsseln möchte, muss man die gesamte zweite Tabellenzeile kennen. Diese kann hier also als „Schlüssel“ dienen. Es gibt $21! \approx 5{,}11 \cdot 10^{19}$ viele verschiedene Schlüssel.

Viel später (16. Jh.) wurde die „Vigenère-Verschlüsselung“ vorgeschlagen: Man benutzt dabei nicht *einen* Schlüssel, der dann auf jeden Buchstaben des Klartextes angewendet wird,

sondern ein Schlüsselwort $a_0 \dots a_{s-1}$ größerer Länge $s > 1$. Man könnte (und das wurde auch so getan) s verschiedene Substitutionschiffren benutzen. Zum Ver- und Entschlüsseln würde man dann eine Liste von s vielen Permutationen der 21 Buchstaben benötigen. Einfacher ist es, s Verschiebechiffren zu benutzen. Dann ist ein Schlüssel tatsächlich ein Wort über dem Alphabet $\{\mathtt{A}, \dots, \mathtt{X}\}$.

Man geht dann also wie folgt vor: $x = x_0 \dots x_{n-1}$ ist der Klartext, $k = a_0 \dots a_{s-1}$ der Schlüssel. Verschlüssle x mit den durch k gegebenen Verschiebungen wie folgt:

$$x_0 \text{ mit } \mathtt{A} \mapsto a_0,\ x_2 \text{ mit } \mathtt{A} \mapsto a_2,\ \dots,\ x_{s-1} \text{ mit } \mathtt{A} \mapsto a_{s-1}.$$

Wenn der Schlüssel k aufgebraucht ist, benutze ihn wieder von vorne: Verschlüssle x_i, $i \geq s$, mit Verschiebung $\mathtt{A} \mapsto a_{i \bmod s}$.

Beispiel: Schlüssel ist $k = \mathtt{ARCVS}$ (für *arcus*, Bogen). Buchstaben an Positionen $0, 5, 10, \dots$ bleiben gleich, da `A` Position 0 hat, Buchstaben an Positionen $1, 6, 11, \dots$ werden um 16 Positionen verschoben (da `R` Position 16 hat), Buchstaben an Positionen $2, 7, 12, \dots$ werden um 2 Positionen verschoben (da `C` Position 2 hat),und so weiter. Es ergibt sich:[2]

(wiederholter) Schlüssel:	A	R	C	V	S	A	R	C	V	S	A	R	C	V
Klartext:	S	E	N	A	T	V	S	R	O	M	A	N	V	S
Chiffretext:	S	X	P	V	P	V	N	T	M	H	A	G	A	Q

Ab hier betrachten wir meist nur Verfahren, die Schlüssel verwenden. – Bei kryptographischen Verfahren mit Schlüsseln betrachten wir zwei grundsätzlich unterschiedliche Ansätze:

- *Symmetrische* (*Private-Key-*)Kryptographie: Es gibt einen geheimen Schlüssel k, den beide der kommunizierenden Parteien kennen müssen. Bei Konzelationssystemen bedeutet dies etwa, dass das Verschlüsselungsverfahren und das Entschlüsselungsverfahren beide diesen Schlüssel $k = k'$ benutzen. Symmetrische Verfahren sind unser erstes Thema. Ein aktuelles standardisiertes symmetrisches Verfahren ist etwa AES (Advanced Encryption Standard).
- *Asymmetrische* (*Public-Key-*)Kryptographie: Nur eine Seite hat einen geheimen Schlüssel k', die andere Seite benutzt einen „öffentlichen“ Schlüssel $k \neq k'$. *Beispiel*: Bei Konzelationssystemen hat der Empfänger (Bob) einen geheimen Schlüssel k', der Sender (Alice) benutzt zur Verschlüsselung einen von Bob ausgegebenen öffentlichen Schlüssel $k \neq k'$. (Bei Authentisierung oder bei digitalen Signaturen ist es umgekehrt.) Asymmetrische Verfahren sind unser zweites Thema. Ein weit verbreitetes asymmetrisches Verfahren ist RSA (nach den Erfindern Rivest, Shamir und Adleman).

[2] In diesem Kontext macht es offensichtlich nicht so viel aus, wenn das Schlüsselwort den Buchstaben `A` enthält.

Das Kerckhoffs-Prinzip (1883, Auguste Kerckhoffs von Nieuwenhof (1835–1903), niederländischer Linguist und Kryptologe) besagt, dass man davon ausgehen muss, dass Eva die Struktur des Verschlüsselungsverfahrens kennt und die Sicherheit nur von der *Geheimhaltung des Schlüssels* abhängen darf.

Begründung:

1. Geheimhaltung eines Verfahrens ist schwer sicherzustellen. (Erfahrungstatsache.)
2. Verfahren sind aufwendig zu entwickeln. Ist das geheime Verfahren einmal bekannt, so wäre Verfahren nutzlos. (Mehrfach passiert: Enigma[3], GSM-Verfahren[4] A5/1 und A5/2 (Mobilfunknetze), Stromchiffre RC4[5].)
3. Allgemein bekannte Verfahren können von mehr Experten auf „Sicherheit“ geprüft werden. Findet niemand einen erfolgreichen Angriff, so kann man eher auf Sicherheit des Verfahrens vertrauen.
4. Nur offengelegte Verfahren können standardisiert werden und weite Verbreitung finden (DES[6], AES[7]).

Bemerkung: In der Realität gibt es auch (viele) geheimgehaltene Systeme. Naturgemäß werden solche nicht in Vorlesungen behandelt.

Im Verlauf der Vorlesung werden wir Grundlagen aus der Mathematik benötigen, insbesondere elementare Zahlentheorie, Gruppentheorie, endliche Körper, etwas Wahrscheinlichkeitsrechnung. Dies wird bereitgestellt.

Nicht behandelt werden: Quantenkryptographie, Kryptographische Protokolle (Pokern übers Internet, Zero-Knowledge-Protokolle, usw.), „Seitenkanalangriffe“ wie Angriffe mittels Eigenschaften der Hardware. Für solche Fragestellungen wird auf die Literatur verwiesen. (Beginnen Sie z. B. mit dem Buch von Dietmar Wätjen.)

[3] s. `https://de.wikipedia.org/wiki/Enigma_(Maschine)`

[4] Global System for Mobile Communcation, s. `https://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications`

[5] s. `https://de.wikipedia.org/wiki/RC4`

[6] Data Encryption Standard, 1977, s. `https://de.wikipedia.org/wiki/Data_Encryption_Standard`

[7] Advanced Encryption Standard, 2000, s. `https://de.wikipedia.org/wiki/Advanced_Encryption_Standard` und später in der Vorlesung

Teil 1
Symmetrische Verschlüsselung, Sicherheitsmodelle

In diesem Teil beschäftigen wir uns ausschließlich mit symmetrischen Konzelationsverfahren, bei denen also Alice und Bob sich auf einen geheimen Schlüssel geeinigt haben.

Mögliche Kommunikationsszenarien:

- Alice will nur einmal eine Nachricht (mit bekannter maximaler Länge) an Bob schicken.
- Alice will mehrere Nachrichten mit bekannter maximaler Länge schicken.
- Alice will beliebig viele Nachrichten beliebiger Länge schicken.

Angriffsszenarien/Bedrohungsszenarien:

Das Kerkhoffs-Prinzip impliziert, dass Eva das Ver- und das Entschlüsselungsverfahren kennt (nur den Schlüssel nicht). Folgende Möglichkeiten kann sie weiterhin haben:

1. Nur Mithören: *Nur-Chiffretext-Angriff* (*ciphertext-only attack, COA*).
2. Mithören + Eva sind einige Paare von Klartext und Chiffretext bekannt:
   Angriff mit bekannten Klartexten (known-plaintext attack, KPA).
   Beispiele: Einige Klartext-Chiffretext-Paare sind aus Versehen oder absichtlich bekannt geworden, Eva hat einige Chiffretexte mit großem Aufwand entschlüsselt, Eva war früher mit der Verschlüsselung beauftragt (ohne den Schlüssel zu kennen).
3. Mithören + Eva kann einige von ihr gewählte Klartexte verschlüsseln: *Angriff mit Klartextwahl (chosen-plaintext attack, CPA).*
   Beispiele: Eva war früher mit der Verschlüsselung beauftragt (ohne den Schlüssel zu kennen).[8]
4. Mithören + Eva kann einige von ihr gewählte Chiffretexte entschlüsseln: *Angriff mit Chiffretextwahl (chosen-cyphertext attack, CCA).*
   Beispiele: Verschiedene Authentisierungsverfahren verlangen, dass die zu prüfende Partei einen Chiffretext entschlüsselt und den Klartext zurücksendet; Eva war früher mit der *Entschlüsselung* beauftragt (ohne den Schlüssel zu kennen).
5. Eva hat Möglichkeiten 3. + 4.

[8] CPA ist immer möglich bei asymmetrischer Verschlüsselung, die wir aber erst später betrachten.

Wesentlich sind auch noch die Fähigkeiten von Eva. Einige Beispiele:

1. Unbegrenzte Rechenkapazitäten. Eva soll *keine Information* über den Klartext erhalten, egal wie viel sie rechnet („*informationstheoretische Sicherheit*“).
2. Konkrete maximale Anzahl an Rechenoperationen, z.B. 2^{60}. „*Konkrete Sicherheit*“: Mit diesem Aufwand erfährt Eva „(fast) nichts“ über Klartexte.
3. Begrenzter Speicher (z.B. 1000 TB). Analog zu 2.
4. Im Design des Verschlüsselungsverfahrens gibt es einen Stellhebel, einen „Sicherheitsparameter“. (Beispiel: Schlüssellänge, Rundenzahl bei DES und AES.) Je nach Leistungsfähigkeit von Eva kann man durch entsprechende Wahl dieses Parameters die Sicherheit des Systems an eine gegebene (geschätzte) Rechenzeitschranke anpassen.
5. Man betrachtet ganze Familien von Verschlüsselungsverfahren, für immer längere Klar- und Chiffretexte. Typischerweise werden Verschlüsselung und Entschlüsselung von Polynomialzeitalgorithmen geleistet. Wenn asymptotisch, also für wachsende Textlänge, der Rechenzeitaufwand für Eva zum Brechen des Systems schneller als polynomiell wächst, kann man sagen, dass sie für genügend lange Texte keine Chance mehr hat, das System erfolgreich zu brechen. („*Asymptotische Sicherheit*“.)

Wir untersuchen in diesem ersten Teil drei verschiedene Szenarien, jeweils symmetrische Konzelationssysteme, mit steigender Komplexität. Alice und Bob haben sich auf einen Schlüssel geeinigt.

1. *Einmalige Verschlüsselung*: Ein einzelner Klartext x vorher bekannter Länge wird übertragen, Eva hört mit (COA).

   Unvermeidlich: Triviale Information, z. B. der Sachverhalt, *dass* eine Nachricht übertragen wurde.[9]

   Was vermieden werden soll: Eva erhält nichttriviale Information, z. B. dass der Klartext x ist oder dass der Klartext aller Wahrscheinlichkeit nach weder x_1 noch x_2 ist.
2. *Frische Verschlüsselung*: Mehrere Klartexte vorher bekannter Länge werden übertragen, Eva hört mit, kann sich einige Klartexte verschlüsseln lassen (CPA).

   Triviale Information: z. B. Anzahl der Nachrichten oder Klartext, falls Eva sich zufälligerweise vorher den „richtigen“ Klartext hat verschlüsseln lassen.
3. *Uneingeschränkte symmetrische Verschlüsselung*: Mehrere Klartexte verschiedener Länge, Eva hört mit, kann sich einige Klartexte verschlüsseln lassen (CPA).

   Triviale Information: Analog zur frischen Verschlüsselung.

[9] Gegenstand der *Steganographie* sind Verfahren, Nachrichten so zu übertragen, dass noch nicht einmal die Existenz der Nachricht entdeckt werden kann.