Sicherheitsanalyse

https://iuk.one/1010-1004

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock, Germany
clemens.cap@uni-rostock.de

11. 11. 2020 Vers. 23

Ziele

Grundbegriffe der Verschlüsselung

Kenntnis der wichtigsten Schutzziele

Bedeutung einer systematischen Sicherheitsanalyse

Kenntnis der grundlegenden Elemente einer Sicherheitsanalyse

Beispiele symmetrischer Verschlüsselung
- Cäsar Chiffre
- One Time Pad

Beurteilung der Adäquatheit von Schutzzielen

Klassifikation von Angreifern

Inhaltsübersicht (1/2)

Inhaltsübersicht (2/2)

1. Grundbegriffe und Beispiele

Ziel: Wir lernen erste Grundbegriffe der Verschlüsselung im Kontext der Cäsar-Chiffre kennen. Wir verstehen die Bedeutung der Sicherheitsanalyse und dahinterstehender Modellbildungen.

1. Grundbegriffe und Beispiele

Cäsar Verschlüsselung

Situation: Römischer Feldherr Gaius Julius Caesar
will militärische Nachrichten verschlüsseln.

Ziel: Kein Unberufener soll die Nachrichten lesen können.

Vorgehen: Jeder Buchstabe wird um X Positionen im Alphabet weitergestellt.

Beispiel:

- Wir nutzen $X = 4$ als **Schlüssel**.
- Wir verschlüsseln den **Klartext (plaintext)** `Morgen angreifen`
- Wir versenden den **Chiffretext (cipher text)** `Qsvkir erkvimjir`
- Der Feind kann den Chiffretext abfangen, versteht ihn aber nicht.
- Der Freund kennt das Verfahren und den Schlüssel und kann entschlüsseln.

Grundbegriffe der Verschlüsselung

Klartext: Für jeden offen lesbare Information.

Chiffretext: Veränderte Information,
die nur mit einem geheimen Zusatzwissen (sog. Schlüssel) lesbar ist.

Schlüssel: Geheimes Zusatzwissen, das man kennen muß
um den Chiffretext lesen zu können.

Verschlüsseln: Verfahren, das aus Klartext Chiffretext macht.

Entschlüsseln: Verfahren, das aus Chiffretext Klartext macht.

Symmetrische, Asymmetrische, Hybride Verfahren

Symmetrische Verfahren (auch: *secret key* Verfahren)

- Für Verschlüsseln und Entschlüsseln wird derselbe Schlüssel genutzt.

Asymmetrische Verfahren (auch: *public key* Verfahren)

- Jeder Teilnehmer hat zwei zueinander passende Schlüssel.
- **Verschlüsselungsschlüssel (public key):** **Zum Zusperren**
  Jeder soll an jeden verschlüsseln können.
  Jeder soll alle public keys aller anderen kennen. Daher: "public"
- **Entschlüsselungsschlüssel (private key):** **Zum Aufsperren**
  Nur beabsichtigter Empfänger soll entschlüsseln können.
  Jeder Empfänger hält seinen eigenen private key geheim. Daher "private"
- **Wichtig:** Aus dem public key kann der private key nicht bestimmt werden.
- Bis ca. 1970 nicht klar, daß es so etwas überhaupt gibt.

Hybride Verfahren (siehe später)

Kerckhoffsches Prinzip

Grundlegendes Prinzip, das beim Bau sicherer Systeme eingehalten werden soll.

Kerckhoffsches Prinzip (empfohlen)

Die Sicherheit kryptographischer Verfahren beruht auf 2 Säulen.

1. Der **Algorithmus** soll öffentlich bekannt sein.
2. Der **Schlüssel** muß geheim bleiben.

Security by Obscurity (zu vermeiden)

Konzept, den Algorithmus geheim zu halten.

Begründung des Kerckhoffschen Prinzips

1. Der Algorithmus **soll** von jedem angegriffen werden können.
   Das Ziel ist, Schwachstellen möglichst bald zu finden.
2. Der Algorithmus ist meist **schwer geheim zu halten**.
   - Aus aus der Implementierung extrahierbar.
   - Allen Entwicklern bekannt (im Gegensatz zum private key, den nur der Eigentümer kennt).
3. **Security by obscurity** hilft, fahrlässige Schwachstellen zu verbergen.
4. **Security by obscurity** hilft, absichtliche Hintertüren zu verbergen.
5. **Tausch des Schlüssels einfacher** als Tausch des Algorithmus.
   Denn: Bei defektem Algorithmus ist Update oder Tausch vieler Geräte nötig.
6. **Veröffentlichung** der Algorithmen hilft Weiterentwicklung des ganzen Gebiets.
7. **Interoperabilität** erfordert Kenntnis des Algorithmus.

Ausgangspunkt

Situation: Ein Kryptograph findet einen verschlüsselten Text.

Chiffretext

Ebt jtu fjo tusfoh hfifjnfs Ufyu, efo ojfnboe mftfo ebsg...

Annahme: Der Text geht noch 30, 40 Zeilen länger.
Denn: Ein sehr kurzer Text ist eher schwer zu entschlüsseln.

Der Kryptograph macht eine Statistik aller verwendeten Zeichen.

Analyse der Buchstaben-Häufigkeit

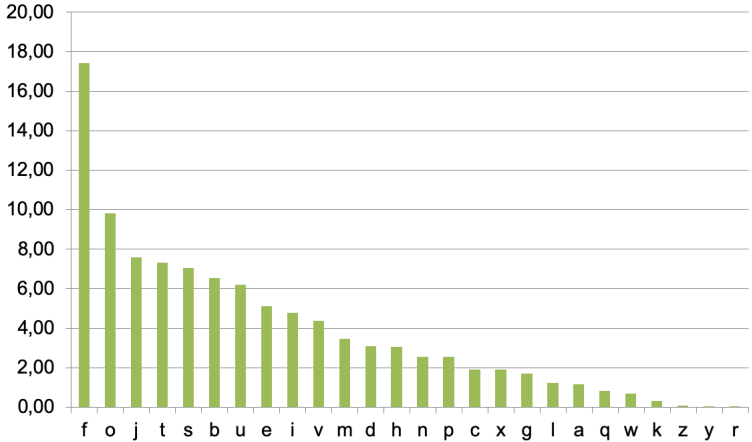


Abb. 1: Buchstaben-Häufigkeit, die der Kryptograph in einem fiktiven Chiffretext vorfindet.

Buchstabenhäufigkeit

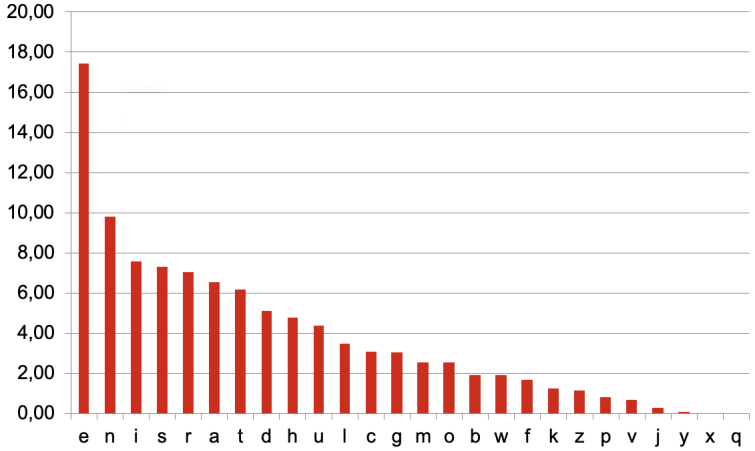


Abb. 2: Buchstabenhäufigkeit, wie sie für die deutsche Sprache typisch ist.

Buchstabenhäufigkeit im unmittelbaren Vergleich

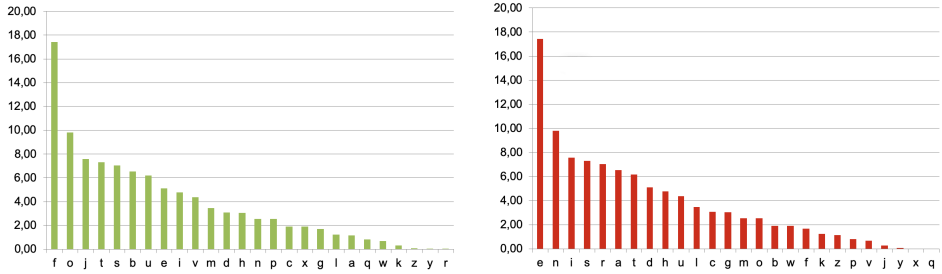


Abb. 3: Buchstabenhäufigkeiten. Links: Chiffretext. **Rechts:** Deutsche Sprache. Die Verteilungsbilder sind hier exakt identisch. In einem realen Fall sind sie näherungsweise identisch, wobei die Näherung mit der Länge des Texts besser wird. Die Bezeichner der Häufigkeitsklassen unterscheiden sich. Direkte Zuordnung gleichhäufiger Klassen ergibt die Kombinationen e-f, n-o, i-j. Handelt es sich um eine Cäsar-Chiffre mit Verschiebung $X = 1$?

Beispiel 1: Natürlichsprachliche Nachricht

Ziel: Man möchte die Vertraulichkeit einer natürlichsprachigen Nachricht sicherstellen. Es kommt eine Cäsar-Chiffre zum Einsatz.

Angreifer: Kann den Ciphertext erhalten und analysieren.

Angriff 1: Statistische Analyse

- Angreifer macht eine **Statistik der Symbolverteilung** im Chiphertext.
- Angreifer erkennt eine Verteilung, die für eine Sprache typisch ist.
- Angreifer gleicht die Häufigkeiten und Buchstaben ab.
- Angreifer kann Schlüssel ermitteln und Text lesen.

Angriff 2: Brute force Angriff

- Angreifer vermutet Cäsar-Chiffre.
- Angreifer **probiert alle Schlüssel durch** (macht bei 25 Stück auch Sinn).
- Bei $X = 7$ findet Angreifer lesbaren deutschen Text.

Beispiel 2: 4-stelliger PIN Code

Ziel: Man möchte die Vertraulichkeit einer 4-stelligen numerischen PIN sicherstellen. Es kommt eine Cäsar-Chiffre zum Einsatz.

Angreifer: Kann den Ciphertext erhalten und analysieren.

Angriff 1: Statistische Analyse

- Angreifer macht eine Statistik der Buchstabenverteilung im Chiphertext.
- 4-stellige PIN ist für statistische Analyse zu kurz.
- PIN Codes haben keine bekannte Häufigkeitsverteilung, die helfen könnte.
- Angriff schlägt fehl.

Angriff 2: Brute Force Angriff

- Angreifer probiert alle Schlüssel durch (9 Stück machen Sinn).
- Es gibt kein Kriterium für Korrektheit (eine PIN ist kein deutscher Satz).
- Ausprobieren bei Geldautomat führt nach 3 Versuchen zur Sperrung.
- Erfolgschance am Geldautomaten $\frac{3}{9} = \frac{1}{3}$ ist deutlich besser als die Erfolgschance durch reines Raten $\frac{1}{10000}$.

Beispiel 3: Ein einzelner Codebuchstabe

Ziel: In einer TV-Show befindet sich hinter einer von 26 Türen (A-Z) ein Ferrari. Rät der Kandidat die richtige Türe, gewinnt er den Ferrari. Der Moderator notiert sich den Türbuchstaben in Cäsar-Verschlüsselung. Als Schlüssel nutzt er, das weiß nur er selber, das Alter seiner Tochter. Kandidat findet den Notizzettel.

Angreifer: Kann den Ciphertext erhalten und analysieren.

Angriff 1: Statistische Analyse

- Statistische Analyse zwecklos, da keine Info über Verteilung möglich.
- Statistische Analyse liefert nicht mehr als blindes Raten.

Angriff 2: Brute Force Angriff

- Angreifer hat kein Kriterium für Korrektheit des Resultats, da nur ein Versuch.
- Brute Force Angriff liefert nicht mehr als blindes Raten.

Keiner der Angriffe hilft bei der Entschlüsselung weiter!
Mathematisch beweisbar: Cäsar-Chiffre gleich sicher wie die sicherste Verschlüsselung (das sog. One Time Pad).

Auswertung der Beispiele

Beispiel 1: Text: Durch 2 Arten von Angriffen leicht zu brechen.

Beispiel 2: 4-stellige PIN: Durch 1 Angriff deutliche Verbesserung für Angreifer.

Beispiel 3: 1 Buchstabe: Cäsar-Chiffre ist beste Technik.

Leitsatz

Eine sinnvolle Bewertung eines Verschlüsselungsverfahrens ist nur nach einer **ausführlichen Sicherheitsanalyse** möglich.

Hinweis: Manche Texte behaupten pauschal, die Cäsar-Chiffre wäre unsicher. Das ist aus zwei Gründen falsch:

1. Es wird eine Bewertung ohne vorherige Sicherheitsanalyse vorgenommen.
2. Es ist bei manchen Anwendungsfällen sachlich falsch.

Die Cäsar-Chiffre wird heute nicht mehr eingesetzt.

Zwei Arten von Angriffen

Brute Force Angriff:

- **Vorgehen:** Alle denkbar möglichen Schlüssel durchprobieren.
- **Abwehr 1:** Verfahren mit einem möglichst großen Schlüsselraum verwenden.
- **Abwehr 2:** im System vermeiden, daß alle Schlüssel durchprobiert werden können.
  Bsp: Online Dienst, der nur 1 Paßwort-Eingabe pro Sekunde erlaubt.
  Bsp: System-Sperre nach mehrfacher Fehleingabe.

Statistische Analyse:

- **Vorgehen:** Häufigkeitsverteilung im Ciphertext analysieren,
  um daraus geeignete Schlüsse ziehen.
- **Abwehr:** Gute Verfahren haben im Ciphertext eine *Gleichverteilung:*
  Alle Symbole treten mit der gleichen Wahrscheinlichkeit auf.

Überblick zur Sicherheitsanalyse

Eine **Sicherheitsanalyse** besteht aus:

1. Einer **Definition der Schutzziele:**
   Was will ich **warum** schützen und was ist mir das **wert**?
2. Einem **Modell des Angreifers:**
   Was könnte der Angreifer wollen und **welche Möglichkeiten** dazu hat er?

2. Schutzziele

Ziel: Was gibt es für wichtige Schutzziele und wie sind diese genau formuliert?

Übersicht

Schutzziele sind Eigenschaften eines Systems, einer Datenübertragung oder Datenverarbeitung, die durch technische Verfahren gewährleistet werden sollen.

CIA–Triade

1. **C**onfidentiality — Vertraulichkeit
2. **I**ntegrity — Integrität
3. **A**vailability — Verfügbarkeit

Themengruppe: Identifizierung – Authentifizierung – Autorisierung

Thema: Verbindlichkeit (Zurechenbarkeit, Nichtabstreitbarkeit, non-repudiation)

Komplexere Schutzziele.

Confidentiality: Vertraulichkeit (1)

Definition: Confidentiality (Vertraulichkeit)

Informationen sind nur einem bestimmten Benutzer, einem bestimmten System oder einem klar eingeschränkten Kreis berechtigter Benutzer oder Systeme zugänglich.

Beispiele:

- Nur Alice kann den Liebesbrief von Bob lesen.
- Nur der Computer im Studienbüro kann die Noten am Prüfungsserver abrufen.
- Nur ein Mitarbeiter im Studienbüro kann die Noten aller Studenten einsehen.

Confidentiality: Vertraulichkeit (2)

Umsetzung:

- **Logischen** Zugang beschränken. Bsp: verschlüsseln
- **Physikalischen** Zugang beschränken. Bsp: Tresor, Wachhund, Vertrauensperson

Untergliederung:

- Schutz der **Informationsinhalte**
  Die übertragenen Daten sind nur eingeschränkt zugänglich.
- Schutz des **Informationsverhaltens**
  Verschiedene Formen von Meta-Information.
  Bsp: *Unbeobachtbarkeit:* Der Angreifer kann nicht erkennen, wer mit wem kommuniziert

Integrity: Integrität

Definition: Integrity (Integrität)

Zwei Formen der Integrität:

- **Daten**integrität: Der Datenbestand kann **nicht unbefugt verändert** werden.
- **System**integrität: Die Funktionsweise des Systems kann **nicht unbefugt verändert** werden.

Wie gut wird geschützt?

- **Starke** Integrität: Eine unbefugte Veränderung **kann nicht** geschehen.
- **Schwache** Integrität: Eine unbefugte Veränderung kann geschehen aber sie **kann nicht unbemerkt** geschehen.

Availability: Verfügbarkeit

Definition: Availability (Verfügbarkeit)

Das System kann ohne Einschränkungen genutzt werden.

Mögliche Formen von Einschränkungen:

- **Funktionseinschränkung:** System funktioniert überhaupt nicht mehr
- **Leistungseinschränkung:** System funktioniert, aber extrem langsam
- **Verletzte Datenintegrität:** Dokumente bei Speicherung / Übertragung (unbemerkt) verändert

Wichtiger Aspekt ist die Erkennbarkeit von Fehlern, dh.
Wenn das System versagt, so erkennt es das selber und informiert den Benutzer.

Identifizierung

Definition: Identifizierung

Eine Person oder ein System weist seine Identität nach
gegenüber einem anderen System oder einer anderen Person.

Problem: Das ist eine sinnlose Definition, weil sie ein Wort (Identifizierung) auf ein anderes Wort (Identität) reduziert und nicht das dahinterstehende Konzept erklärt.

Bessere Definition: Identifizierung

Bei einer Person oder einem System wird das Vorliegen eines *charakteristischen Merkmals* überprüft, das nur auf diese Person oder auf dieses System zutrifft.

Wichtige Fragen:

1. **Was** ist das Merkmal?
2. Wie wird die **Bindung** des Merkmals mit der Person / dem Objekt gewährleistet?
3. Wie wird das Vorliegen des Merkmals **überprüft**?

Beispiele für identifizierende Merkmale

- **Name:** Maria Müller geb. Maier.
- **Pseudonym:** ForenId User DonaldDuck.
- **Aussehen:** Sieht so aus wie Person in Referenzbild 23.
- **Fingerabdruck:** Hat Fingerabdruck wie in Referenz 47.
- **Iris-Struktur:** Hat Iris-Abbild wie in Referenz 99.
- **Genetischer Code:** Hat eine bestimmte genetische Eigenschaft.
- **Haustorschlüssel:** Inhaber eines in das Schloß passenden Schlüssels.
- **Reisepaß:** Inhaber eines Reisepasses mit Lichtbild und Fingerabdruck.
- **Clubausweis:** Inhaber eine Plastikkarte nur mit Name, ohne Bild.
- **Simcard:** Inhaber eines Handys mit einer bestimmten SIM-Card.
- **App:** Kunde der XY Bank mit registrierter App.
- **SMS:** Fähig unter 0171 2345 6789 eine SMS zu empfangen.
- **Email:** Fähig, eine Mail unter `president@usa.gov` zu lesen.
- **Account:** Fähig, einen Tweet unter `@POTUS` abzusetzen.

Identifizierung und Merkmalsbindung

Wer hat Interesse an einer **Trennung der Merkmalsbindung**?

Beispiel 1: Person, die Merkmalsträger ist, will Merkmal loswerden.

- Peter Panzerknacker will Identifizierung durch Fingerabdruck vermeiden.
- David Dieb will ein Video sehen, ohne daß von seinem Account abgebucht wird.

Beispiel 2: Person, die nicht Merkmalsträger ist, will Merkmal erwerben.

- Bob Bösewicht will dem Bankdirektor den Tresorschlüssel stehlen.
- Hans Hacker will die Banking-TANs von Robert Reich auf dem Handy empfangen.

Stellvertretung: Eine Berechtigung kann delegiert werden.
Bob darf während ihres Urlaubs für Chefin Alice Transaktionen vornehmen.
Bob erhält zeitweilig Befugnis von Alice, muß sich aber als Bob ausweisen.
Transaktion wird als "durch Bob im Namen von Alice" verzeichnet.

Nachweis von Eigenschaften (1)

Use Case: Altersnachweis ohne Namensnennung.
Nora will `hotguys.xxx` ansehen ohne Name oder Adresse zu nennen.

Durch **Identifikation im Verbund** mit angefragter Eigenschaft

- Nora identifiziert sich (Nora Neugierig; Perso 4711; geb. 2.2.02; Markt 99, 18055 Rostock)
- Aus dem Datensatz wird Eigenschaft und weiteres (Name, Adresse, usw) abgeleitet.
- **Nachteil:** Privatheitsverletzung: Nora gibt weitere Daten preis.

Durch **Delegation an (vertrauenswürdige?) Drittinstanz**

- Nora identifiziert sich gegenüber Telekom oder Facebook.
- Telekom oder Facebook sendet Altersnachweis an `hotguys.xxx`
- **Nachteil:** Vertrauen in Telekom oder Facebook erforderlich.

Nachweis von Eigenschaften (2)

Durch **datensparsame Attributzertifikate**

- Anonymer digitaler Nachweis einer Eigenschaft durch *digital credentials*.
- Erfordert fortgeschrittene Kryptographie: [Bra02, Bra00].
- **Vorteil:** Schutz der Privatheit: Nur vom Nutzer freigegebene Attribute übertragen.

Durch **persönliche Hardware**

- Weise der Hardware nach, daß sie nicht gestohlen ist (Bsp: Fingerabdruck)
- Hardware weist dem Anfrager das angeforderte Attribut nach.
- Beispiel: Handy, Smart Card, **C**itizen **D**igital **A**ssistant [MSC02].
- **Vorteil:** Schutz der Privatheit: Nur vom Nutzer freigegebene Attribute übertragen.

Leitsatz

Der datensparsame Nachweis von Eigenschaften in SW und HW ist möglich.

Beobachtung: Oft unterlassen: Ökonomische Interessen, Überwachung, Unkenntnis.

Exkurs: Meinung zu Framing

Framing bedeutet eine Einbettung von Themen in ein sprachliches Umfeld, wodurch Zuschreibungen, Emotionalisierungen und Bewertungen nahegelegt werden.

Anonym konnotiert: Unpersönlich, an der Grenze der Legalität, negativ.

Daten*sparsam* konnotiert: Ressourcen erhaltend, nachhaltig, positiv.

Der ursprüngliche Begriff der Anonymität bedeutet, daß eine Person **nicht identifiziert** werden kann. Er hat in bestimmten Kontexten eine Abwertung erfahren.

Anonymität / Datensparsamkeit ist **Voraussetzung**, daß eine Person in der digitalen Welt

1. ihre **Persönlichkeitsrechte wahrnehmen** kann (positiv).
2. sich ihrer **Verantwortung entziehen** kann (negativ).

Die Balance zwischen diesen beiden Polen muß die digitale Gesellschaft aushandeln.

Die emotionale Konnotation bei Begriffen ist dabei nicht immer hilfreich.

Die 3 Faktoren der Identifikation

Ich kann identifiziert werden durch etwas das ich

❶	**weiß**	Passwort, PIN, TAN, Antwort auf private Frage
Typisch:		Zahl oder Symbolkette
Probleme:		Vergessen, aufschreiben, erraten, wiederverwenden, abpressen
❷	**habe**	SIM Card, Smart(card|phone|watch), (T)OTP Generator
Typisch:		Schwer kopierbares Stück Hardware
Probleme:		Verlieren, stehlen, illegal weitergeben, kopieren
❸	**bin**	Fingerabdruck, Iris, Geruch, Stimme
Typisch:		Biometrisches Merkmal
Probleme:		Hygiene, Sozialakzeptanz, manipulierte Merkmalsabgabe, Diebstahl
Beachte:		Jeder hat nur einen beschränkten Vorrat solcher Merkmale!

Beispiel: Paßwort-Generator (1)

Erzeugung von Paßworten aus einem geheimen Startwert.
Startwert kann nicht aus Paßwörtern zurückerrechnet werden.

One time password: Nur einmalige Verwendung, dann das nächste Paßwort.
Problem, wenn Nutzer und prüfende Stelle außer Synchronisation geraten.

Timed password: Nur für gewissen Zeitraum gültig.
Problem, wenn Angreifer es während des Zeitraums wiederverwendet.

Beispiel: Paßwort-Generator (2)

Abb. 4: Separater OTP-Generator und Smartphone-basierter OTP-Generator. ©

Beispiel: Photo-TAN Generatoren (1)

Abb. 5: Separater TAN-Generator und Smartphone-basierter TAN-Generator.

Beispiel: Photo-TAN Generator (2)

Benutzte Faktoren:

- **Wissen:** Passwort
- **Habe:** System mit registriertem Schlüssel
- **Sein:** Fingerabdruck

Kryptographische Bindung: Warum der farbliche QR Code?
Wird nur "Transaktion von User 4711" autorisiert, kann Angreifer Betrag ändern.
Fazit: *Alle* relevanten Daten müssen kryptographisch eingebunden sein.

Unabhängige Geräte:
Erfolgt Überweisung über nur ein Gerät, so besteht ein **single point of failure**.
Woher weiß Benutzer, daß Handy die angezeigten Daten richtig sendet.
Erfolgt Überweisung über Laptop und Handy, müßte Angreifer zwei Geräte manipulieren.

Autorisierung

Definition: Autorisierung

Nur eine bestimmte (authentifizierte) Person darf Zugriff erhalten

Autorisierung

1. Authentifizierung (Sicherstellung der Identität).
2. Ermitteln der mit dieser Identität verbundenen Rechte.

Angriffe möglich gegen Authentifizierung und gegen Speicher der verbundenen Rechte.

Kopieren eines Fingerabdrucks

Kopieren von Fingerabdrücken:

- Wasserglas mit Fingerabdruck photographieren.
- Mit Bildverarbeitungs-Software bearbeiten.
- Auf lichtempfindliche Kupferplatte projizieren.
- Abätzen der belichteten Fläche.
- Daraus einen Gummistempel fertigen.

Abb. 6: Fingerabdruck von Herrn Schäuble nach einer Kopie durch den Chaos Computer Club. ©

Mehrfaktoren Identifizierung

Definition: Mehrfaktoren Identifizierung

Die Identifizierung einer Person unter Nutzung von zwei verschieden kategorisierten Faktoren um die Nachteile nur eines Faktors auszugleichen.

Problem: Recovery

- Einer der Faktoren geht dem rechtmäßigen Eigentümer verloren.
- Wie kann defekter Faktor repariert werden?
- Oft: Recovery über einen dritten Faktor. (richtig, aber aufwendig)
- Oft: Recovery über den verbliebenen Faktor. (stellt einen systematischen Fehler dar)

Kryptographische Bindung

Sicherheitseigenschaften sind oft **an Kontexte gebunden.**

Beispiel:

1. Alice darf die Datei /etc/motd lesen
2. Bob beauftragt Überweisung 20€ von Kto 17 an Kto 19.

Es genügt nicht, einzelne Personen oder Systeme nur zu identifizieren.
Die Identifizierung muß an den Wirk-Kontext gebunden bleiben.

Verbindlichkeit

Englische Bezeichnung: **Non-Repudiation**.

Definition: Verbindlichkeit, Nicht-Abstreitbarkeit, Zurechenbarkeit

Ein Teilnehmer an einem verbindlichen Protokoll kann nach einer durchgeführten Transaktion nicht mehr behaupten, die Transaktion nicht durchgeführt zu haben.

Beispiel: Elektronischer Handel

- Ein Kunde kann nicht abstreiten, eine Ware bestellt zu haben
- Ein Kunde kann nicht abstreiten, eine Ware erhalten zu haben.

Beispiel: Auditing

- Ein User kann nicht abstreiten, auf Daten zugegriffen zu haben.

Komplexere Schutzziele

Beispiel: Elektronische Wahl via App

1. **Autorisierung:** Nur Stimmberechtigte dürfen wählen.
2. **Verfügbarkeit:** Alle Stimmberechtigte dürfen wählen.
3. **Funktionalität:** Die Summe aller Stimmen wird korrekt bestimmt.
4. **Auditierbarkeit:** Jeder Stimmberechtigte kann kontrollieren, daß seine eigene Stimme richtig gezählt wurde.
5. **Anonymität:** Niemand außer dem Abstimmenden selbst kann herausfinden, wer wie abgestimmt hat.
6. **Zeitbegrenzung:** Es werden nur Stimmen gezählt, die nach Wahlbeginn und vor Wahlende abgegeben wurden.

3. Angriffsanalyse

3.1. Möglichkeiten des Angreifers

3.2. Rechenleistung des Angreifers

3.3. One Time Pad

Ziel: Nach welchen Kriterien können Angriffe beschrieben werden?

1. Grundbegriffe und Beispiele
2. Schutzziele
3. **Angriffsanalyse**

Übersicht

Was will der Angreifer?

Was weiß der Angreifer?

Was kann der Angreifer?

Es gibt viele Arten von Angriffen,
die nach unterschiedlichen Kriterien eingeteilt werden können.

Nach dem Wissen des Angreifers

Was kennt der Angreifer bei welchen Attacken?

Ciphertext Only:	Einige Ciphertexte.
Known Plaintext:	Einige Paare (Plaintext, Ciphertext).
Chosen Plaintext:	Zu einigen von ihm einmal gewählten Plaintexten den dazugehörigen Ciphertext.
Adaptive Chosen Plaintext:	Zu von ihm immer wieder neu gewählten Plaintexten den dazugehörigen Ciphertext.

Nach dem Einblick in die Kommunikation

Eavesdropping:	Angreifer kann übertragene Daten abfangen.
Delay Attacke:	Angreifer kann den Empfang gesendeter Daten verzögern.
Modification Attacke:	Angreifer kann gesendete Daten verändern.
Replay Attacke:	Angreifer kann früher gesendete Daten erneut senden.
Verkehrsanalyse:	Angreifer findet heraus, wer mit wem kommuniziert.

In Theorie:	Angriffe sind sortenrein definiert. Eavesdropping nur Abfangen, nicht Veränderung.
In Praxis:	Meist Kombinationen möglich. Wenn Eavesdropping, dann meist auch Verkehrsanalyse.

Sinn

Einteilung der Angreifer nach ihrer **Rechenleistung** ermöglicht Aussagen über die Durchschlagskraft verschiedener Angriffe.

Insbesondere für Brute Force Angriffe wichtig.

Zwei Modelle üblich:

- **Computationally Secure** — Hat Rechner üblicher Rechengeschwindigkeit
- **Unconditionally Secure** — Hat Rechner beliebig hoher Rechengeschwindigkeit

Computationally Secure

Definition: Computationally Secure Model

Angreifer hat einen Rechner üblicher Rechengeschwindigkeit

Analyse:

- Beschreibt Gefahren eines Angriffs in **aktueller Technologie**.
- **Optimistische** Sichtweise
- **Vernachlässigt** künftige Hardware-Entwicklung.
  - **Quantitativ:** Schnellere Rechner: Mooresches Gesetz
  - **Qualitativ:** Neue Technologie: (Quantencomputer; Neurocomputer)
- **Sicherheit** beruht auf der Unfähigkeit, komplizierte Aufgaben schnell zu lösen.
- **Typische Aussage:** Verfahren ist für die nächsten 5 Jahre sicher (Vorausgesetzt der Schlüssel ist richtig gewählt).

Entwicklung von Technologie

Technologische Entwicklungen in vielen Fällen

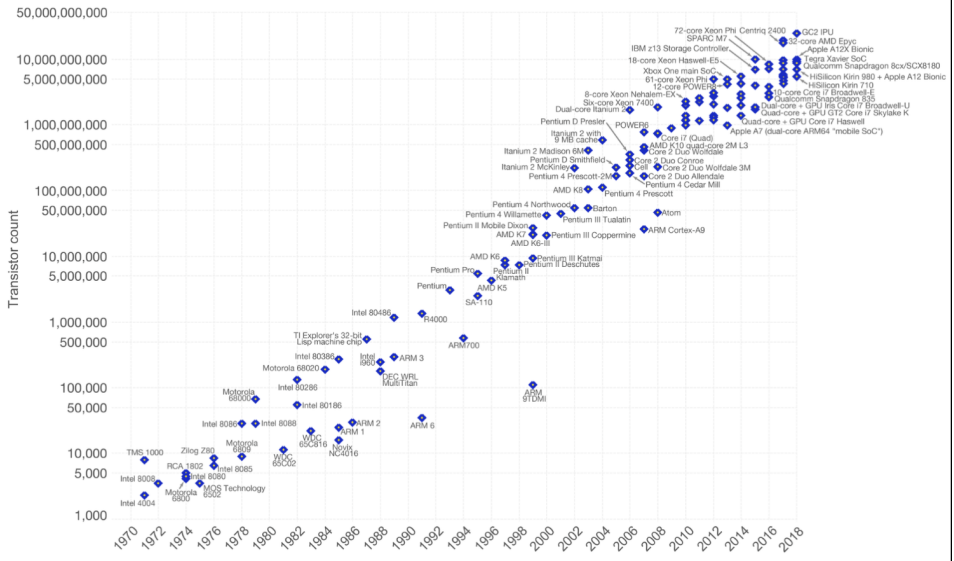
- folgen *zunächst* einem **exponentiellen Gesetz**
- kommen *dann* in eine **Sättigungsphase**
- führen *schließlich* zu einer weiteren **technologischen Innovation,** die dann zu einer Wiederholung dieses Zyklus führt.

Berühmtestes Beispiel: Mooresches Gesetz

Die Komplexität integrierter Schaltkreise verdoppelt sich ca. alle 12-24 Monate.

Ähnliche Gesetze gelten für Datenraten in optischen Netzwerken, Kapazitäten persistenter Speicher und Stromverbrauch digitaler Technologien.

Abb. 7: Moore-sches Gesetz



Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldInData.org. There you find more visualizations and research on this topic.

Unconditionally Secure

Definition: Unconditionally Secure Model

Angreifer hat einen Rechner beliebig hoher Rechengeschwindigkeit

Analyse: Beschreibt Gefahren eines Angriffs **aller zukünftiger Technologien**.

- **Pessimistische** Sichtweise
- **Sicherheit** beruht auf statistischen Effekten
- **Typische Aussage:** Ist sicher. Unconditionally
  Vorausgesetzt die Randbedingungen des Verfahrens werden eingehalten.
  Aber: Angriffe gegen Randbedingungen, beteiligte Personen & System.

Beispiele:

- One Time Pad (OTP)
- Cäser-Chiffre im Beispiel 3 (hat dieselbe *Wirkung wie* OTP)

One Time Pad

Vorbereitung: Sender sendet Empfänger geheime Zufallsbits $k = k_1, k_2, k_3, \ldots$.

Verschlüsselung:

1. Sender stellt Plaintext als Bit-String dar: $p = p_1 p_2 p_3 \ldots p_n$
2. Sender nimmt die ersten n Zufallsbits $b_1 b_2 \ldots b_n$
3. Sender bildet Ciphertext via **xor**: $c_1 = p_1 \oplus b_1$, $c_2 = p_2 \oplus b_2$ usw.

Entschlüsselung:

1. Empfänger erhält den Ciphertext $c = c_1 c_2 c_3 \ldots$
2. Empfänger bildet nun $c_1 \oplus b_1$, $c_2 \oplus b_2$ usw.

xor Operation $\oplus$

$$0 \oplus 0 = 0 \qquad 0 \oplus 1 = 1 \qquad 1 \oplus 0 = 1 \qquad 1 \oplus 1 = 0$$

Sicherheitsanalyse des One Time Pad

Sicherheit: Wenn k gleich lang wie p und c; und k zufällig.
Das Beste, was der Angreifer tun kann, ist, den Plaintext direkt zu raten.
Kenntnis des Ciphertexts bietet dem Angreifer **keine** zusätzliche Information.

Bewertung des One Time Pad

Probleme:

1. Benötigter Schlüssel ist sehr lang.
2. Schlüssel darf nur einmal verwendet werden.
3. Schlüssel muß vor der Kommunikation auf sicherem Wege ausgetauscht werden.

Hauptproblem: Mit *jedem* späteren Kommunikationspartner muß *vor* der verschlüsselten Kommunikation *auf sicherem Weg* ein Schlüssel ausgetauscht werden.

Untauglich für ad hoc Kommunikation von Partnern, die sich vorher nie getroffen haben.

Paradoxon: Wo hilft Verfahren, wenn sicherer Schlüsseltausch vorausgesetzt ist?

Auflösung: *Heute* sicherer Schlüsseltausch und *morgen* sicher kommunizieren, wenn sicherer Kommunikationsweg nicht mehr verfügbar.

Anwendungen des One Time Pad

Bereiche: Diplomatischer Dienst, Geheimdienst, Militär

Vorgehensweise am Beispiel eines Konsulats

- Schlüsselmaterial auf Datenträger mit Diplomatengepäck an Konsulat verteilt
- Konsulat oder Ministerium nutzt Schlüssel einmal und zerstört danach Datenträger
- Versandte Nachricht ist für Angreifer Datenmüll

Bewertung: Das Verfahren ist

- bei korrekter Anwendung nicht zu brechen ("unconditionally secure")
- für den Normalanwender aber wenig praktikabel.

Einziger Nutzen: Sichere Kommunikation von heute in die Zukunft zu verschieben.