ANWALTSCONTOR

# FREIHEIT GESTALTEN

## VERSCHLÜSSELUNG ALS FREIHEIT IN DER KOMMUNIKATION

**Christian R. Kast, Rechtsanwalt**
**und Fachanwalt für IT Recht**

# INHALTSÜBERSICHT

ANWALTSCONTOR

- „Risiken“ für die Sicherheit von Kommunikation und die Freiheit sicher zu kommunizieren
- Technische Grundlagen von Verschlüsselung
- Beispiele von Verschlüsselung bei unterschiedlichen Kommunikationswegen
  - E-Mail, DE-Mail, IP Telefonie
  - Gesicherte Leitungsverbindungen (VPN etc.)
  - Gesicherte Datenverbindungen (Speicherung, Cloud Computing)
- Verschlüsselung als Freiheit?
- Der Anwalt, das „Netz“ und § 203 StGB
- Verschlüsselung als Datenschutz?

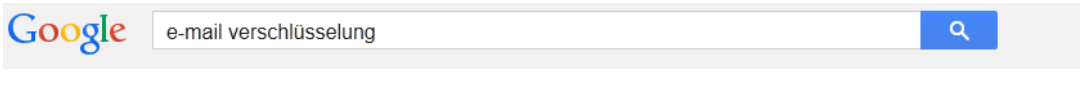
# „Risiken“ für die Sicherheit von Kommunikation …

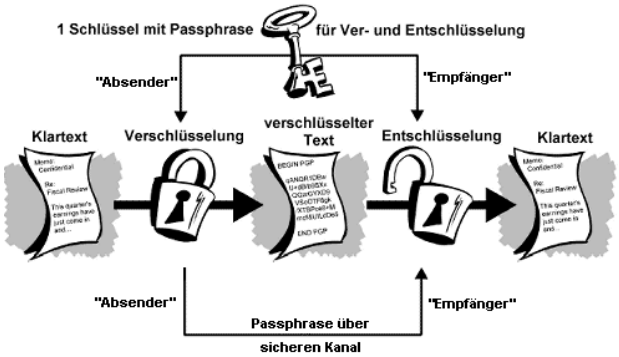
ANWALTSCONTOR



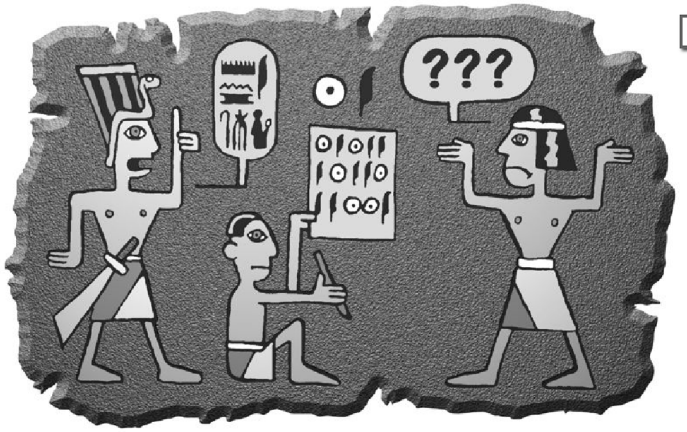

# … UND DIE FREIHEIT SICHER ZU KOMMUNIZIEREN

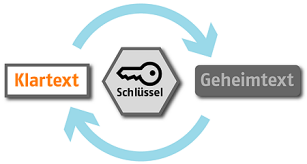
ANWALTSCONTOR





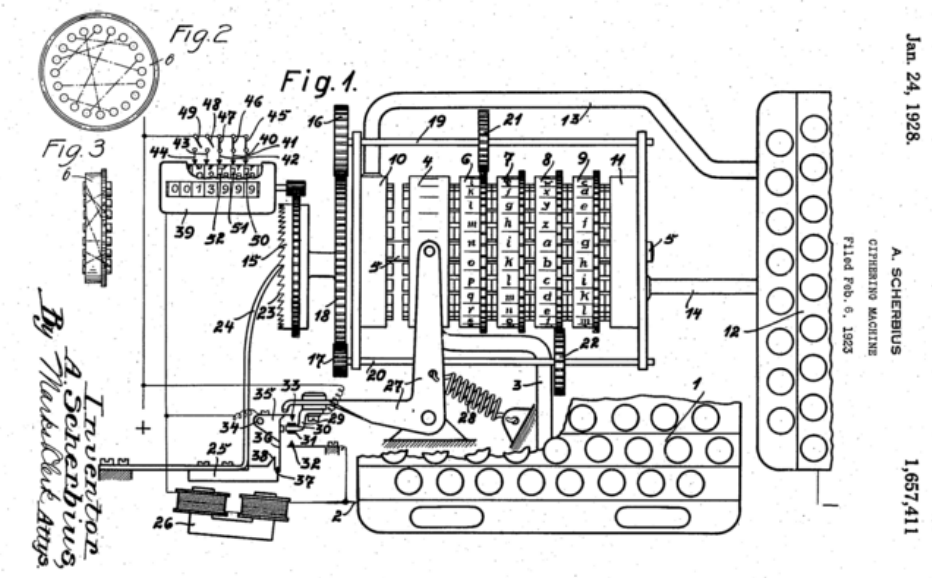



Bundesamt für Sicherheit in der Informationstechnik

# TECHNISCHE GRUNDLAGEN VON VERSCHLÜSSELUNG

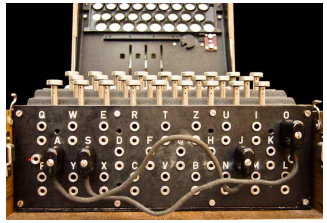
ANWALTSCONTOR




| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | E | K | M | F | L | G | D | Q | V | Z | N | T | O | W | Y | H | X | U | S | P | A | I | B | R | C | J |
| II | A | J | D | K | S | I | R | U | X | B | L | H | W | T | M | C | Q | G | Z | N | P | Y | F | V | O | E |
| III | B | D | F | H | J | L | C | P | R | T | X | V | Z | N | Y | E | I | W | G | A | K | M | U | S | Q | O |
| IV | E | S | O | V | P | Z | J | A | Y | Q | U | I | R | H | X | L | N | F | T | G | K | D | C | M | W | B |
| V | V | Z | B | R | G | I | T | Y | U | P | S | D | N | H | L | X | A | W | M | J | Q | O | F | E | C | K |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| UKW A | AE | BJ | CM | DZ | FL | GY | HX | IV | KW | NR | OQ | PU | ST |
| UKW B | AY | BR | CU | DH | EQ | FS | GL | IP | JX | KN | MO | TZ | VW |
| UKW C | AF | BV | CP | DJ | EI | GO | HY | KR | LZ | MX | NW | QT | SU |

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



# Technische Grundlagen von Verschlüsselung

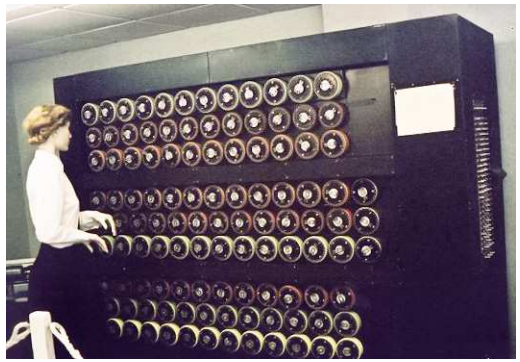
ANWALTSCONTOR

$$\frac{1}{n!}\prod_{i=1}^{n}\frac{(26-2i+2)(26-2i+1)}{2} = \frac{26!}{2^n \cdot n! \cdot (26-2n)!}$$

| Stecker n | Möglichkeiten für Steckverbindung | genau n Steckverbindungen | bis zu n Steckverbindungen |
|---|---|---|---|
| 0 | 1 | 1 | 1 |
| 1 | 325 | 325 | 326 |
| 2 | 276 | 44850 | 45176 |
| 3 | 231 | 3453450 | 3498626 |
| 4 | 190 | 164038875 | 167537501 |
| 5 | 153 | 5019589575 | 5187127076 |
| 6 | 120 | 100391791500 | 105578918576 |
| 7 | 91 | 1305093289500 | 1410672208076 |
| 8 | 66 | 10767019638375 | 12177691846451 |
| 9 | 45 | 53835098191875 | 66012790038326 |
| 10 | 28 | 150738274937250 | 216751064975576 |
| 11 | 15 | 205552193096250 | 422303258071826 |
| 12 | 6 | 102776096548125 | 525079354619951 |
| 13 | 1 | 7905853580625 | 532985208200576 |

Maximal

**$3x10^{114}$**



= circa 77 BIT Verschlüsselung

# Technische Grundlagen von Verschlüsselung

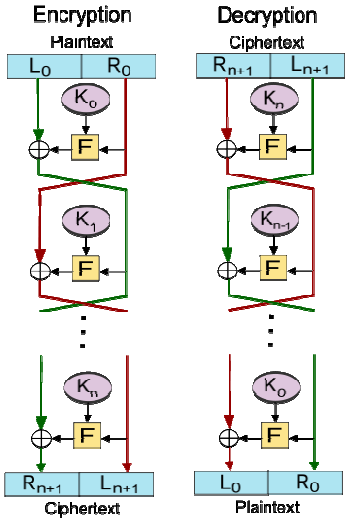
ANWALTSCONTOR

- Caesar-Verschlüsselung: Schlüsselanzahl 25 (Schlüssellänge von ungefähr 5 Bit)
- DES: 256 = 72.057.594.037.927.936 (entspricht 56 Bit)
- Enigma I: 206.651.321.783.174.268.000.000 (entspricht ungefähr 77 Bit)
- Enigma-M4: 60.176.864.903.260.346.841.600.000 (entspricht fast 86 Bit)
- Monoalphabetische Substitution: 26! (Fakultät) = 403.291.461.126.605.635.584.000.000 (entspricht ungefähr 88 Bit)
- Triple-DES: 2112 = 5.192.296.858.534.827.628.530.496.329.220.096 (entspricht 112 Bit)
- AES: wählbar
  - 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 (entspricht 128 Bit),
  - 2192 = 6.277.101.735.386.680.763.835.789.423.207.666.416.102.355.444.464.034.512.896 (entspricht 192 Bit)
  - 2256 = 115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936 (entspricht 256 Bit)

ANWALTSCONTOR

# Aber Schlüssellängen

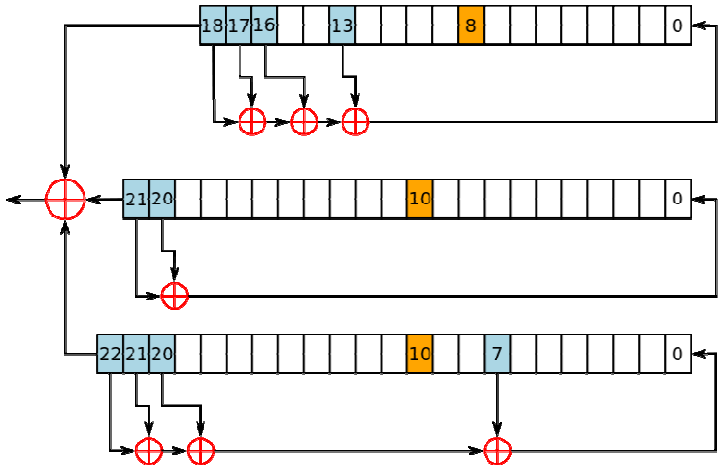
# sind nicht alles !



# TECHNISCHE GRUNDLAGEN: STROMVERSCHLÜSSELUNG

ANWALTSCONTOR

- kryptographischer Algorithmus zur symmetrischen Verschlüsselung
- die zu verschlüsselnde Information wird einzeln mit den Zeichen eines Schlüsselstroms verknüpft
- der Schlüsselstrom ist in der Regel eine pseudozufällige Zeichenfolge, die durch den Schlüsselalgorithmus generiert wird
- bei selbstsynchronisierenden Stromchiffren gehen außer dem Schlüssel auch Teile der Nachricht in die Berechnung des Schlüsselstroms ein.

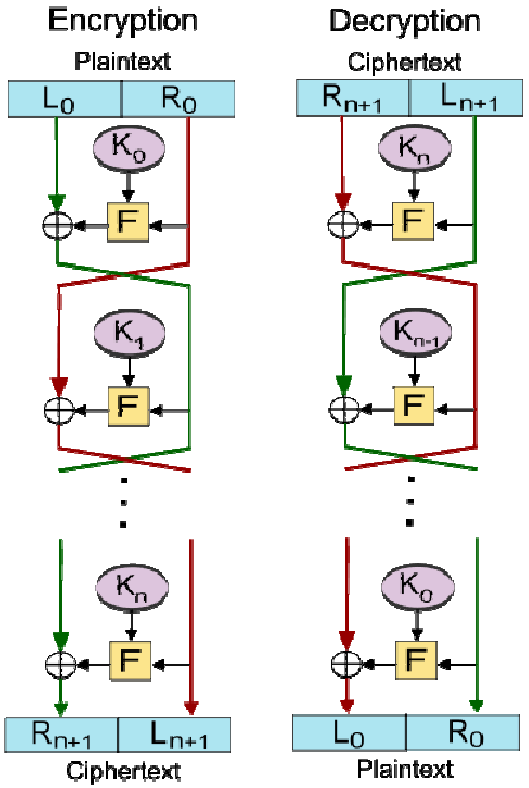



- Beispiel GSM Verschlüsselung

# TECHNISCHE GRUNDLAGEN: BLOCKVERSCHLÜSSELUNG

ANWALTSCONTOR

- es wird jeweils ein ganzer Block an Daten gleichzeitig verschlüsselt
- Die Verschlüsselungsmethode wird dabei durch den Schlüssel-Algorithmus bestimmt
- der gängigste Betriebsmodus ist der „Cipher Block Chaining Mode“
  - der zu verschlüsselnde Block wird vor dem Verschlüsseln mit dem vorhergehenden bereits verschlüsselten Block verknüpft
  - klare Verschlüsselungskette, die ein Vertauschen einzelner Blöcke unmöglich macht
  - zwei gleiche Nachrichten werden selbst mit dem gleichen Schlüssel nie gleich ver-schlüsselt

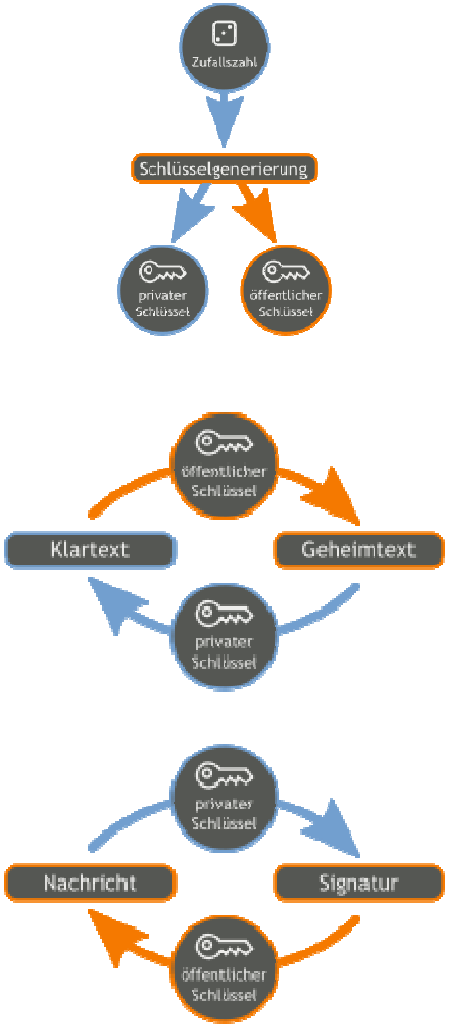



z.B. AES Verschlüsselung

# Technische Grundlagen: Asymmetrische Verschlüsselung

ANWALTSCONTOR

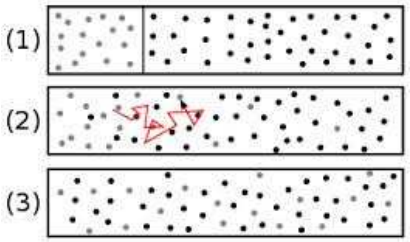
- der Sender benutzt zum Verschlüsseln einer Nachricht einen öffentlichen Schlüssel des Empfängers
- der Empfänger verwendet dann zur Entschlüsselung seinen privaten Schlüssel, der nur ihm bekannt ist
- das „Schlüsselübermittlungsproblem“ der symmetrischen Verschlüsselungsver-fahren entfällt, da der öffentliche Schlüssel nur zum Verschlüsseln, nicht aber zum Entschlüsseln verwendbar ist
- Nachteil ist, dass asymmetrische Verschlüsselungsverfahren relativ langsam sind



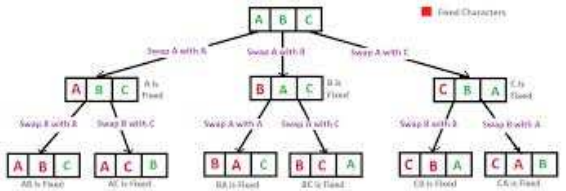
# Maßnahmen im Rahmen der Verschlüsselung

ANWALTSCONTOR

- Diffusion
  die Verteilung der Daten im Block




- Permutation
  Austausch der Blöcke in den Verschlüsselungsschritten



Recursion Tree for Permutations of String "ABC"

- Konfusion
  die Anwendung verschiedener Schlüssel

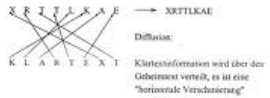
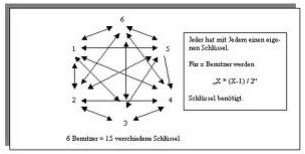




*Abbildung 4.1: Konfusion und Diffusion*

- Schlüsselverteilung



ANWALTSCONTOR

## Organisatorische Mängel

- Fehlende oder unzureichende Regelungen zu Rollenmodellen/Berechtigungssystemen
- Unzureichende Kenntnis über Regelungen (insbesondere Rollenmodelle/Berechtigungssysteme)
- Unzureichende Kontrolle der Sicherheitsmaßnahmen
- Unzureichendes Schlüsselmanagement bei Verschlüsselung

## Menschliche Fehlhandlungen

- Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
- Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren
- Fehlbedienung der Verschlüsselungssoftware

ANWALTSCONTOR

## Technisches Versagen

- Software-Schwachstellen oder Fehler der Verschlüsselungssoftware
- Fehlende oder unzureichende technische Umsetzung von Rollenmodellen/Berechtigungssystemen
- Fehlende oder unzureichende technische Umsetzung von Nutzungs-Protokollen
- Schlechte oder fehlende Authentikation
- Ausfall einer Verschlüsselungssoftware
- Unsichere kryptographische Algorithmen
- Fehler in verschlüsselten Daten
- Fehlende „Transportsicherheit“ in internen und externen Netzen

ANWALTSCONTOR

# Vorsätzliche Handlungen

- Nichtanerkennung einer Nutzungshandlung in eine Datenbank
- Vertraulichkeitsverlust schützenswerter Informationen
- Unautorisierte Benutzung einer Verschlüsselungssoftware
- Manipulation eines Kryptomoduls/ Verschlüsselungssoftware
- Kompromittierung kryptographischer Schlüssel
- Gefälschte Zertifikate
- Integritätsverlust schützenswerter Informationen
- Angriffe über Schwachstellen in Software oder Hardware

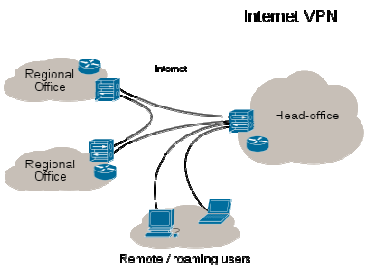
# VERSCHLÜSSELUNG BEI UNTERSCHIEDLICHEN KOMMUNIKATIONSWEGEN

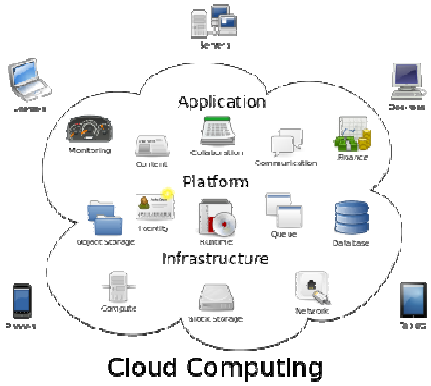
ANWALTSCONTOR

**Brüssel unterstützt Merkels Vorstoß für "Schengen-Netz"**

heute, 18:37 Uhr 44

Die Idee eines innereuropäischen Datenverkehrs oder auch "Schengen-Netzes" bekommt Rückenwind aus der Politik: Bundeskanzlerin Merkel will darüber in Paris sprechen, die EU-Kommission signalisiert Unterstützung. Mehr...




Bundesamt für Sicherheit in der Informationstechnik

Kontakt | Impressum | Service | Gebärdensprache | Leichte

Das BSI | Themen | Aktuelles | Presse | Publikationen

**Produkte / Tools**

- Übersicht
- Anoubis
- Browser in the Box
- BOSS
- Chiasmus
- ERPOSS4
- Gpg4win
- IT-Grundschutz GSTOOL
- mapWOC
- Mobilfunkdetektor MDS
- OpenVAS
- Security Surf-CD
- SiVoIP
- VS-Clean

› Startseite › Themen › Produkte / Tools › Gpg4win

**Gpg4win – Sichere E-Mail- und Datei-Verschlüsselung**

- Warum überhaupt verschlüsseln?
- Leistungsumfang
- Voraussetzungen
- Kosten / Nutzungsbedingungen
- Hilfestellungen / Support
- Historie
- Herunterladen / Bezugsquellen
- Studie "Nachhaltige Freie Software"
- Referenzen

GPG 4WIN **Warum überhaupt verschlüsseln?**

PIRATEN PARTEI

Seite Diskussion Quelltext anzeigen Versionen/Autoren

Navigation

- Hauptseite (Wiki)
- Bibliothek
- Kategorien
- Portale
- Liste aller Seiten
- Zufällige Seite
- Letzte Änderungen

Piratenpartei

- Parteiprogramm
- Bundessatzung
- FAQ
- Piraten vor Ort

Persönliche Werkzeuge

- Anmelden / Benutzerkonto erstellen

**HowTo Emails verschlüsseln mit PGP mit Thunderbird**

Dieser Artikel dürfte die meisten Piraten im Moment brennend interessieren.

Wenn du anderer Meinung bist, so diskutiere dies bitte auf der Diskussionsseite, bevor du diese

PIRATEN INFORMIEREN

**Sicherer Kommunikationsweg**

Hier entsteht ein kurzes HowTo "Sicherer Kommunikationsweg per E-Mail" (Dauer<1h). Es soll jeden Interes und in kurzer Zeit auf verschlüsselte E-Mail umzustellen. Hier wird beschrieben, wie das mit dem Mailprogr ermöglichen Verschlüsselung mit PGP, sind aber nicht Teil des HowTos hier.

**Das Problem**

ZDNet Suche

*ZDNet / News*

**T-Online führt Ende März SSL-Verschlüsselung für E-Mails ein**

*von Björn Greif am 10. Februar 2014, 17:26 Uhr*

Die Deutsche Telekom wird zum 31. März alle E-Mail-Server von T-Online auf SSL-Verschlüsselung umstellen. Dann kommunizieren die Server untereinander sowie mit mit den Geräten der E-Mail-Nutzer nur noch verschlüsselt. Für einen problemlosen Übergang müssen Kunden unter Umständen einige Änderungen an den Einstellungen ihres Computers oder Mobilgeräts vornehmen, wie die Telekom mitteilt.


T-Online-Nutzer, die einen E-Mail-Client auf PC, Notebook, Smartphone oder Tablet verwenden, sollten prüfen, ob die Verschlüsselung bereits aktiviert ist. Ist dies nicht der Fall, müssen sie einige Einstellungen manuell ändern. Für Outlook, Mozilla Thunderbird, Windows Live Mail, Apple Mail und die E-Mail-Software 6.0 der Deutschen Telekom finden sich Schritt-

# Beispiel moderner Verschlüsselung

ANWALTSCONTOR

- Homomorphe Verschlüsselungsverfahren sind asymmetrische Verschlüsselungs-verfahren, die es ermöglichen, verschlüsselte Berechnungen von verschlüsselten Daten durchzuführen
- Vorteil dieser Verfahren ist, dass die Daten, außer beim Berechtigten, nur in verschlüsselter Form vorliegen (erweiterte Ende zu Ende Verschlüsselung)
- sowohl während der Bearbeitung, Übertragung und Speicherung von Daten sind die Daten verschlüsselt und werden nur auf dem Endgerät des Nutzers entschlüsselt
- es entfallen damit Risiken der anderen Verschlüsselungsverfahren im Hinblick auf eine mögliche Überwachung des Daten-verkehrs oder Einsichtnahme in die Server oder Speichermedien, auf welchen die Daten verarbeitet und gespeichert werden

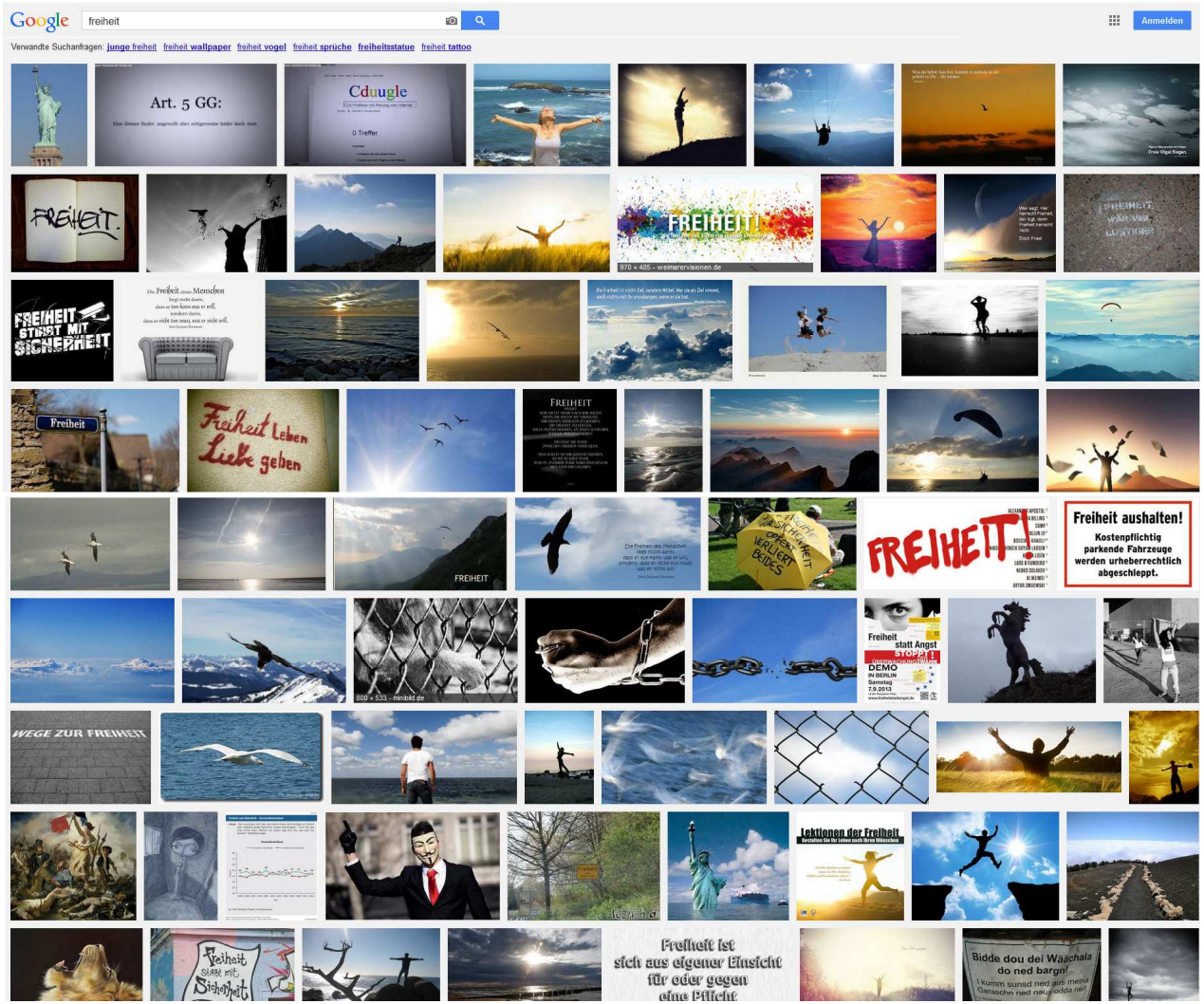
Graphic: Christine Daniloff/MIT

Karlsruhe Institute of Technology

HomER

# VERSCHLÜSSELUNG ALS FREIHEIT?

ANWALTSCONTOR



# Verschlüsselung als Freiheit?

ANWALTSCONTOR

- Freiheit ist möglich, aber anstrengend


- Technologie ist komfortabel, aber bei Handys denken wir nicht an Sicherheit, bei Autos schon

## Der Anwalt, das „Netz“ und § 203 StGB

ANWALTSCONTOR

- Die §§ 203 und 204 StGB erfassen im Schutzbereich den Eingriff in Daten, die Personen anvertraut werden, die Katalogberufe des § 203 Abs. 1 Ziffern 1 bis 6 ausüben
- Dabei ist der persönliche Lebens und Geheimbereich des Offenbarenden geschützt, also solche Tatsachen, die nicht allgemein bekannt sind und vom Offenbarenden auch nicht allgemein bekannt gegeben werden wollen
- Hierbei sind vom Schutzbereich sämtliche Informationen (ein- und ausgehend sowie gespeichert) umfasst, sowie schon das Bestehen einer eine Kommunikationsverbindung, die auf eine Vertragsbeziehung oder beispielsweise Inanspruchnahme eines Katalogberufes hindeutet
- Mit einer technisch wirksamen und sicheren Verschlüsselungs-methode, die den Eingriff in solche speziell geschützten Daten verhindert, können also auch Daten, die unter § 203 StGB fallen, zum Beispiel durch Drittanbieter gespeichert werden.

## VERSCHLÜSSELUNG ALS DATENSCHUTZ?

ANWALTSCONTOR

- Verschlüsselung als Anonymisierung oder Pseudonymisierung?
  - Anonymisieren im Sinne von § 3 Abs. 6 BDSG ist das Verändern personenbezogener Daten mit der Folge, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können
  - Pseudonymisierung liegt nach § 3 Abs. 6a BDSG dann vor, wenn bei Daten der Name und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck ersetzt werden, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren
- Verschlüsselung und § 11 BDSG
  - Erhebung, Verarbeitung oder Nutzung personenbezogene Daten im Auftrag durch andere Stellen
  - werden zum Beispiel bei Anwendung homomorpher Verschlüsselungsverfahren in Cloud Anwendungen nur verschlüsselte Daten übertragen und der Schlüssel verbleibt beim Auftraggeber, wäre schon der generelle Anwendungsbereich des BDSG insoweit nicht eröffnet

ANWALTSCONTOR

# Vielen Dank für Ihre Aufmerksamkeit !

## Für Rückfragen


Rechtsanwalt Christian R. Kast
www.anwaltscontor.de