Verschüsselung leicht gemacht

Eine kleine Hilfestellung für Anfänger

Agenda

1. Warum wollen wir überhaupt verschlüsseln?
2. Grundlagen der Verschlüsselung
3. Anwendung: eMail-Verschlüsselung
4. Anwendung: Festplatten-Verschlüsselung

Was ist Sicherheit?

- Allgemein
  - gefahrenfreier Zustand
  - frei von unvertretbaren Risiken
- Informationssicherheit
  - Vertraulichkeit, Verfügbarkeit und Integrität

Netzwerksicherheit

- Angriffe
  - Mitlesen von Daten und Kontrollinformationen
    - Anfällig: POP3/SMTP/IMAP/...
  - Einschleusen von Daten oder Informationen
    - Anfällig: POP3/SMTP/...

Kompromisse eingehen

- Benutzerfreundlichkeit vs. Sicherheit
- Beispiele
  - Passwortlänge
  - Vista UAC
  - Performance bei RSA

Achtung, Theorie!

Grundlagen I

- Das Kerckhoff-Prinzip
  - Jean Guillaume Hubert Victor François Alexandre Auguste Kerckhoff von Nieuwendorf
    - Niederländsischer Linguist und Kryptologe
    - * 1835 in Nuth, heutiges Niederlande
    - † 1903 in Paris, Frankreich
  - Zentrale Aussage:
    - Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen.
    - Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.

Grundlagen II

- Bedeutung für die heutige Kryptographie
  - Höher einzuschätzen als zu Zeiten Kerkhoffs
  - Heutige Algorithmen sehr komplex
  - Sicherstellung der Integrität und Zuverlässigkeit des Algorithmus nur durch »viele« möglich

Der Anfang I

- Verschiebealgorithmus / Cäsar-Chiffre
  - Einfache Zuordnung der Buchstaben durch Verschieben; z.B. um drei Stellen:

a	b	c	d	e	...	w	x	y	z
D	E	F	G	H	...	Z	A	B	C

  - Was bedeutet die Zeichenfolge?
    - YHUVFKOVVHOXQJ OHLFKW JHPDFKW!

Der Anfang II

- Vorteile
  - Schnell zu Realisieren
  - Nicht komplex
- Nachteile
  - Sehr schnell zu knacken
  - 26 Buchstaben → 26 Möglichkeiten
  - In linearer Zeit lösbar
  - Häufigkeitsanalyse bei beliebiger Permutation

Aktuelle Konzepte I

- Symmetrische Verschlüsselung
  - Verschlüsselung und Entschlüsselung mittels gleichen Schlüssels
    - z.B. Realisierung durch Blockchiffre
    - Teilschlüssel repräsentiert durch Zufallszahlen fester Länge
  - Vorteile
    - Kurze Schlüssellänge ausreichend
    - Schnelles Ver- und Entschlüsseln

Aktuelle Konzepte II

- Symmetrische Verschlüsselung
  - Nachteile
    - Schlüsselaustausch über sicheren Kommunikationsweg notwendig
    - Schlüssel muss überall geheim gehalten werden (Problem bei großer Teilnehmerzahl)
  - Bekannte standardisierte Verfahren
    - 3DES (Data Encryption Standard)
      - offiziell abgelöst 2001 durch AES
    - AES (Advanced Encrpytion Standard)
      - seit 2001 offizieller Standard

Aktuelle Konzepte III

- Asymmetrische Verschlüsselung
  - Verschlüsselung und Entschlüsselung mittels unterschiedlicher Schlüssel
    - Große Primzahlen zum erstellen der Schlüssel notwendig (Einwegfunktion)
    - Beruht auf langwieriger Faktorisierung großer Zahlen
    - Public Key Infrastructure (PKI)
  - Vorteile
    - Geheimhaltung nur des privaten Schlüssels notwendig
    - Kleineres Schlüsselverteilungsproblem im Vergleich zum symmetrischen Verfahren

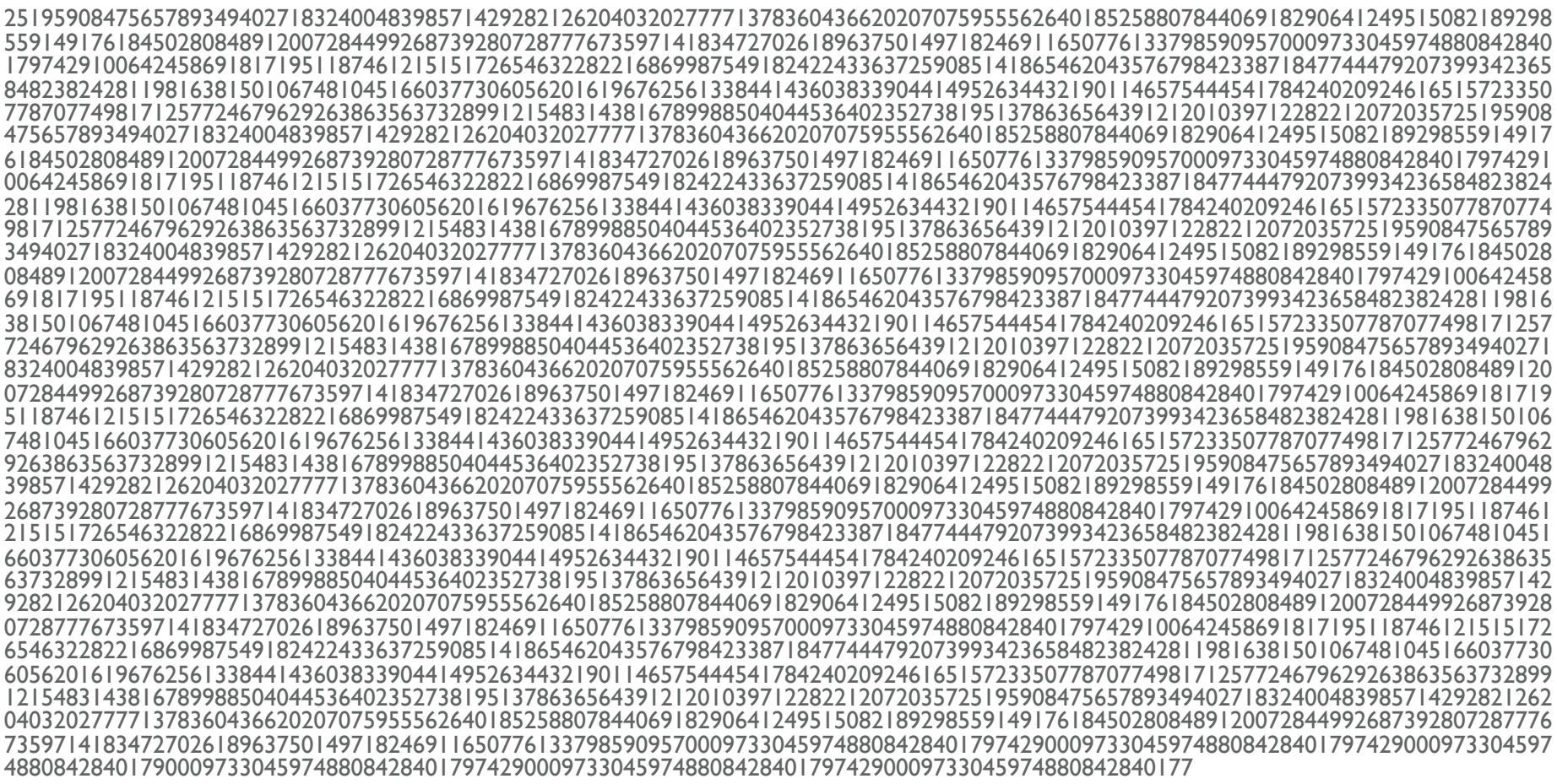
Aktuelle Konzepte IV

- Asymmetrische Verschlüsselung
  - Nachteile
    - Sehr langsam im Vergleich zu Symmetrischen Verfahren (Faktor ≈ 1000)
    - Sicherheit der zugrunde liegenden Einwegfunktion nur angenommen
  - Bekanntes standardisiertes Verfahren:
    - RSA (nach den Erfindern **R**ivest, **S**hamir und **A**dleman benannt)

4096Bit

OUTPUT´08

von Studenten für Studenten



Email-Verschlüsselung

mittels Thunderbird + Enigmail + GPG

OpenPGP

- OpenPGP-Standard (RFC 4880)
  - Hybride Verschlüsselung (asymmetrisch + symmetrisch)
    - **P**retty **G**ood **P**rivacy (kommerziell)
    - **G**NU **P**rivacy **G**uard (kostenlosen + OpenSource)

Signierung

- Gewährleistet **NUR** Unverfälschtheit
- Daten weiterhin unverschlüsselt
- Verfahren
  1. Fingerabdruck der Nachricht erstellen
  2. Verschlüsselung des Fingerabdruckes mit privaten Schüssel
  3. Empfänger entschlüsselt mit öffentlichem Schlüssel
  4. Empfänger erzeugt seinen eigenen Fingerabdruck
  5. Vergleich der beiden Fingerabdrücke

Warum verschlüsseln?

- Schutz vor Mitlesern
  - Geheimdienste sammeln alles
- Briefgeheimnis §202 Stgb gilt nicht für eMails
  - aber §202a wenn man verschlüsselt
- Schutz vor organisierter Kriminalität
- Warum nicht? Meine Tür schließe ich auch zu

Vorgehensweise

1. Schlüssel erstellen (einmalig)
2. öffentlichen Schlüssel publizieren
    1. auf Keyserver laden
    2. Link in der Signatur publizieren
3. Nachrichten signieren/verschlüsseln
4. Empfänger entschlüsselt

Konto einrichten

- Benutzername: e040XX@abwesend.com
- Passwort: e040XX
- IMAP-Server: mail.abwesend.com
- SMTP-Server: mail.abwesend.com

Festplattenverschlüsselung

mittels TrueCrypt

Sichere Datenhaltung I

- Warum überhaupt verschlüsseln? Meine Wohnung ist doch sicher...
  - Innerhalb der "sicheren" Wohnung
    - Wohnung keinesfalls 100%-ig sicher
      - → z.B. Einbruch (physisch wie digital)
    - Benutzung des Computers durch mehrere Personen
    - Abgrenzung vertraulicher Daten
  - Außerhalb der "sicheren" Wohnung
    - → Was passiert, wenn mein Laptop gestohlen wird?

Sichere Datenhaltung II

- Was sind schützenswerte Daten?
  - Steuererklärung und Amtliche Dokumente
  - Persönliche Patientenakte/ Krankenversicherungsnachweise
  - Digitale Rechnungen und Kontoauszüge
  - Persönliche Tagebücher
  - Private Schlüssel (z.B. für E-Mail-Kommunikation)
  - Generelles Bedürfnis nach Privatsphäre!
    - Entgegenwirken des »Gläsernen Nutzers«

TrueCrypt I

- TrueCrypt - Eine Möglichkeit der Datenverschlüsselung
  - Was ist TrueCrypt?
    - Ein Programm zur (relativ) einfachen Datenverschlüsselung
    - Verfügbar für Microsoft Windows, Linux und MacOS
  - Was kann TrueCrypt?
    - Daten mittels vier unterschiedlicher Verfahren verschlüsseln ...
    - ... dabei diese (je nach Paranoiagrad) performant zu benutzen
    - Anlegen versteckter Datenträger für hohe Sicherheitsanforderungen

TrueCrypt II

- Was kann TrueCrypt nicht?
  - Mich davon abhalten mein Passwort an den Monitor zu kleben.
  - Mich daran hindern den Rechner “offen“ stehen zu lassen.
  - Mit der Installation mich von aller Last zu befreien und ein digital sicheres Leben zu führen.

TrueCrypt III

- Wodurch wird die Sicherheit von TrueCrypt bestimmt?
  - Wahl des Verschlüsselungsalgorithmus
    - AES, Serpent, Twofish, Cascades
    - Oder Kombinationen dieser
      - Erhöht die Sicherheit
      - Senkt die Performance u.U. drastisch

- Wahl des Passworts
  - Was wäre ein einfaches Passwort?
    - z.B.: baumkuchen
  - Was wäre ein ideales Passwort?
    - untere Grenze: g yZSljmk/ICet9 {g3*
  - Was wäre ein realistisches Passwort?
    - »Myran blickte sich um und sah die 16 Tore zu Baskinth ...«
      - Mbsuusd16TzB

- Wahl des Hash-Algorithmus zur Schlüsselerzeugung
  - Whirlpool, SHA-512 und RIPEMD-160

Und weiter?

- Sichere E-Mail-Kommunikation
  - Mozilla Thunderbird: http://www.mozilla-europe.org/de/products/thunderbird/
  - Enigmail: http://www.erweiterungen.de/detail/Enigmail/
  - GnuPG/MacGPG: http://www.gnupg.org/download/index.de.html http://macgpg.sourceforge.net/
- Sichere Datenhaltung
  - TrueCrypt: http://www.truecrypt.org/
  - TrueCrypt - Anleitungen: http://www.truecrypt.org/docs/
  - TrueCrypt - Sprachpakete: http://www.truecrypt.org/localizations.php
  - Anleitung: http://www.heise.de/software/download/special/windows_verschluesseln/26_1
- Sicheres W-LAN
  - Wikipedia Artikel zu WPA: http://de.wikipedia.org/wiki/Wi-Fi_Protected_Access
  - Heise Security Artikel zu WPA: http://www.heise.de/security/Angriffe-auf-WPA--/artikel/53014
- Passwortverwaltung
  - Heise Sofware Archiv für verschiedenste Passwortmanager:
    - http://www.heise.de/software/download/o0g1s313k306?stq=30

Danke

- Aufwachen!
- Fragen?
- Anmerkungen?
- Folien auf www.abwesend.com