Computersicherheit

14. März 2009

Inhalt

Zum Vortrag

Wir werden

- Kurz die Funktionsweise von Verschlüsselungsverfahren erklären
- Mögliche Angriffe betrachten und wie dem begegnet wird
- Anwendungsgebiete für Kryptographie (Tor,Email,Festplatte)
- Weitergehende Schutzmasnahmen erörtern

Übersicht Kryptologie

- Steganographie
  - technische Steganographie
    Bsp.: Geheimtinte, Scrambler
  - linguistische Steganographie
    - Semagramme
      Bsp.: Zeichenformen, “Bilderrätsel”
    - offene Codes
      Bsp.: Jargon, Stichwörter, Raster
- Kryptographie
- Kryptanalyse
- Anwendungen deren Kern kryptologische Verfahren bilden z.B. elektronisches Wahlsystem, elektronisches Geld, Zero Knowledge Proofs . . .

Symmetrische Verschlüsselung
Funktionsweise

Ein symmetrisches Verfahren besteht aus :

- Klartextraum T
- Geheimtextraum G
- Schlüsselraum S
- Codierfunktion $e : S \times T \longrightarrow G, (s, t) \mapsto g$
- Decodierfunktion $d : S \times G \longrightarrow T, (s, g) \mapsto t$

wobei gilt: $d(s, e(s, t)) = t, \forall s \in S, t \in T$

Symmetrische Verschlüsselung
Funktionsweise

Üblicherweise wählen wir T und G mit $|T| < \infty$ und $|G| < \infty$. Nun heisst T^* Klartextraum und G^* Geheimtextraum und wir erweitern e zu $\widehat{e}$ und d zu $\widehat{d}$ wie folgt:

$$\widehat{e} : S \times T^* \rightarrow G^*, \widehat{e}(s, t_1 t_2 \dots t_n) = e(s, t_1)e(s, t_2) \dots e(s, t_n)$$

$$\widehat{d} : S \times G^* \rightarrow T^*, \widehat{d}(s, g_1 g_2 \dots g_n) = d(s, g_1)d(s, g_2) \dots d(s, g_n)$$

Symmetrische Verschlüsselung
Monoalphabetische Substitution

Idee : Ersetze in einem Text jedes Zeichen genau durch ein anderes. z.B. fasse Buchstaben aus $\{A, \ldots, Z\}$ als Zahlen modulo 26 auf und bilde x auf $x + s \mod 26$ ab.
Beispiel Schlüssel s = 2.

x	A	B	C	...	X	Y	Z
e(2,x)	C	D	E	...	Z	A	B

$\widehat{e}(2, \text{MORGENREVOLUTION}) = e(2, \text{M})e(2, \text{O}) \ldots e(2, \text{N})$
$= \text{OQTIGPTGXQNWVKQP}$

Symmetrische Verschlüsselung
Monoalphabetische Substitution (Forts.)

- Bei Verschieben nur 26 verschiedene Schlüssel. Sehr schnell durchprobierbar.
- Bei beliebiger Substitution $26! = 26 * 25 * \ldots * 2 * 1 \approx 4 * 10^{26}$ Schlüssel. Schon bei dieser einfachen Verschlüsselung würde das Durchprobieren bei einer erschöpfende Suche mit 1 Million Schlüsseln pro Sekunde 10^{13} Jahre dauern.

Problem: Häufigkeitsanalyse von auftretenden Zeichen im Geheimtext. Dadurch wird sukzessive Zuordnung zu auftretenden Zeichen im Klartext möglich.

Symmetrische Verschlüsselung

Polyalphabetische Substitutionen Beispiel

$n = 4, s = s_1 s_2 s_3 s_4 = 12\ 0\ 17\ 23 = \text{MARX}$

Klartext	M	O	R	G	E	N	R	E	V	O	L	U
Schlüssel	M	A	R	X	M	A	R	X	M	A	R	X
Geheimtext	Y	O	I	D	Q	N	I	B	H	O	C	R

Klartext	T	I	O	N
Schlüssel	M	A	R	X
Geheimtext	F	I	F	K

Symmetrische Verschlüsselung

Polyalphabetische Substitutionen Problem

Problem : Auftretende gleiche Wörter an der gleichen Position modulo n werden gleich verschlüsselt.

...	I	S	T	...	I	S	T	...	I	S	T
...	R	X	M	...	M	A	R	...	R	X	M
...	Z	P	F	...	U	S	K	...	Z	P	F

Es gibt verschiedene Verfahren die Schlüssellänge n (oder ein vielfaches davon) bei polyalphabetischen Substitutionen zu berechnen. Koinzidenztest, Kasiskitest ... Auf die einzelnen Teilstücke kann dann wieder eine Häufigkeitsanalyse der Buchstaben angewendet werden.

Symmetrische Verschlüsselung
OnetimePad

- Gleiches Verfahren wie bei Polyalphabetische Verschlüsselung. n wird hier so gewählt, dass es der Länge des zu verschlüsselden Textes entspricht.
- Alle $s_1, s_2, \ldots, s_n$ sind zufällig gewählt.
- e ist eine einfache zyklische Verschiebung.
- Dies führt zur "perfekten Sicherheit" (wir werden hier nicht perfekte Sicherheit definieren).

Symmetrische Verschlüsselung
OnetimePad Nachteile

- Sicherer Kanal für Schlüssel der Länge $n \geq X$ notwendig
- "Echter" Zufall notwendig

Diese Punkte machen das One Time Pad impraktikabel.
Früheres Anwendungsgebiet: Rotes Telefon zwischen Moskau und Washington.

Praktikable und sichere Verfahren ?

- Man kann beweisen: Für “perfekte Sicherheit” gilt für alle Verfahren, dass die Schlüssellänge mindestens so lang sein muss wie der verschlüsselnde Text.
- Es gibt jedoch Verfahren die zwar keine perfekte Sicherheit leisten aber so gut zu sein scheinen, dass sie uns bei weitem genügen.
- Beispiel: AES,Serpent,MARS,RC6,Twofish, RSA ...

Kurze Zusammenfassung

- Einfache Verfahren : Schlüsselraum groß, Entschlüsselung einfach
- Sichere Verfahren z.b. OneTimePad aber praktisch nicht anwendbar
- Weitere Verfahren : Keine “perfekte Sicherheit”, aber scheinen relativ sicher

Symmetrische Verschlüsselung
Kategorien von Sicherheit

- Perfekte Sicherheit
- Berechnungssicherheit (Bestimmter Berechnungsaufwand beweisbar).
- Relative Berechnungssicherheit (Mindestens so schwer wie ein als schwer geltendes Problem).
- Pragmatische Sicherheit (Für uns tut es).

Die heute verwendeten Verfahren befinden sich im Bereich der pragmatischen Sicherheit. Heerschar von Kryptologen die sich an Verfahren die Zähne ausgebissen haben. Früher wurde Schlüssellänge künstlich beschränkt (NSA). Exportverbot für Kryptographie.

Asymmetrische Verschlüsselung

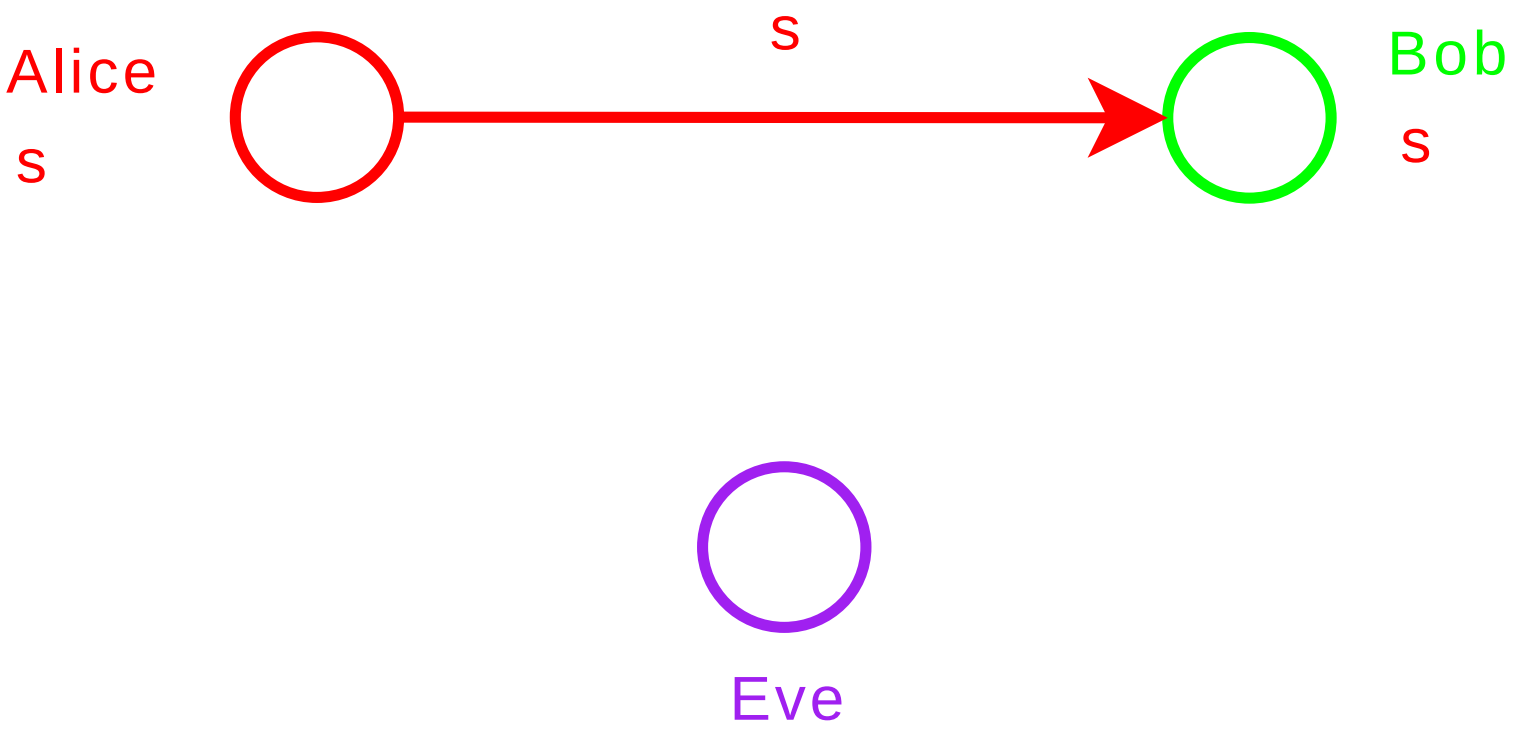
Am Beispiel RSA

Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.

Asymmetrische Verschlüsselung

Am Beispiel RSA

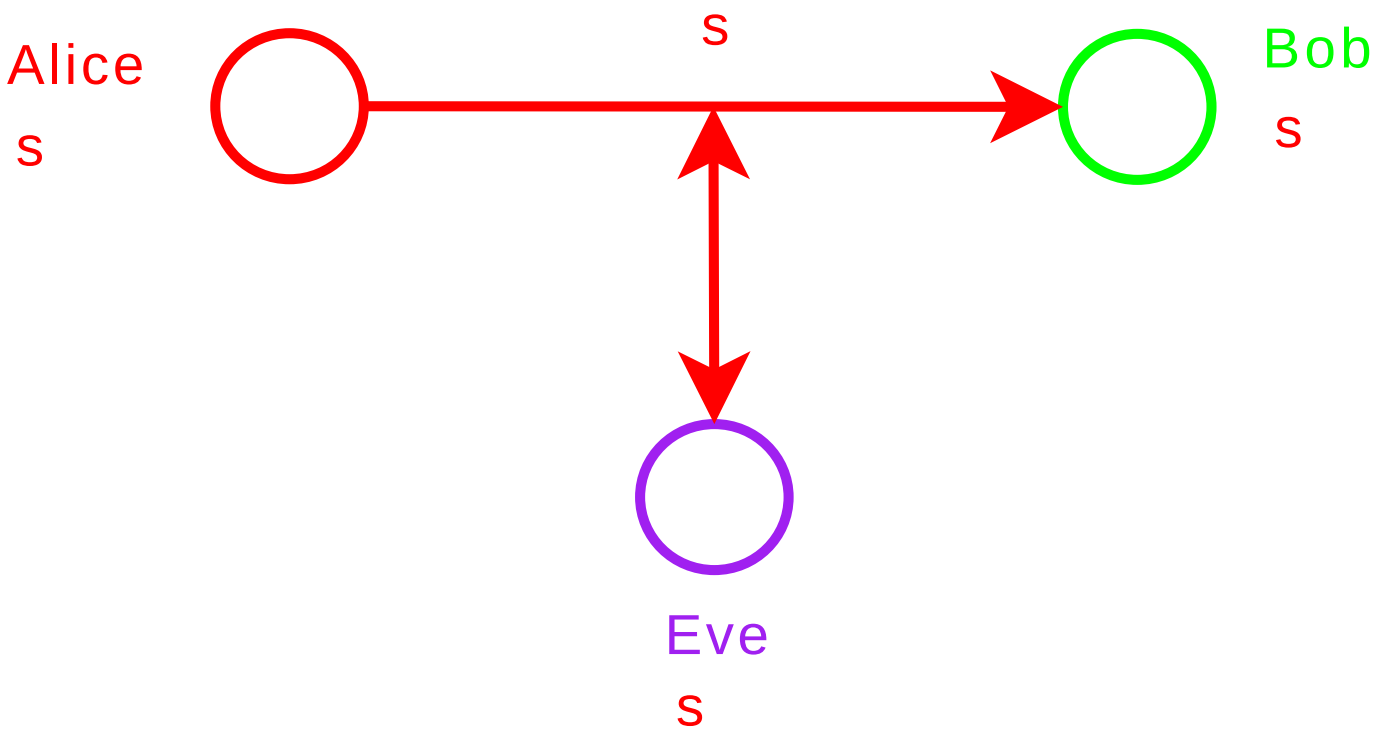
Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung

Am Beispiel RSA

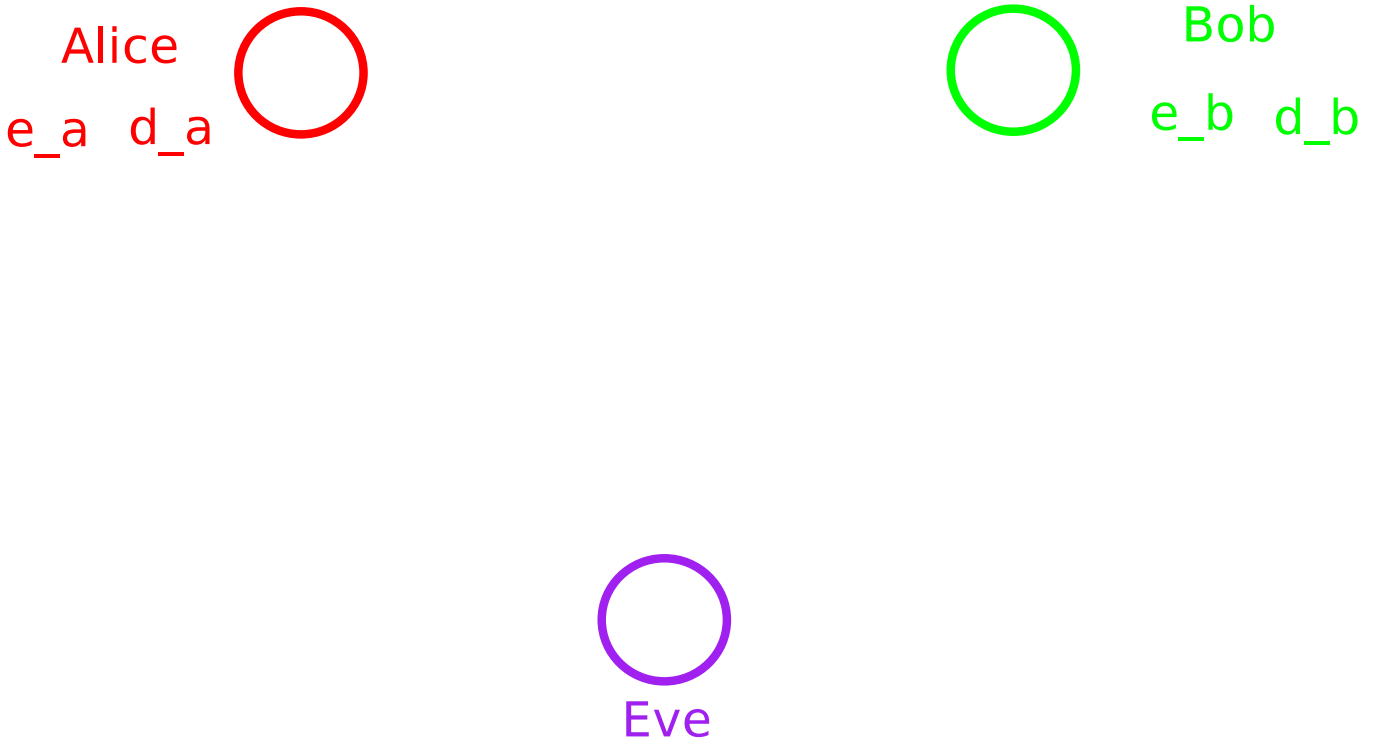
Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung

Am Beispiel RSA

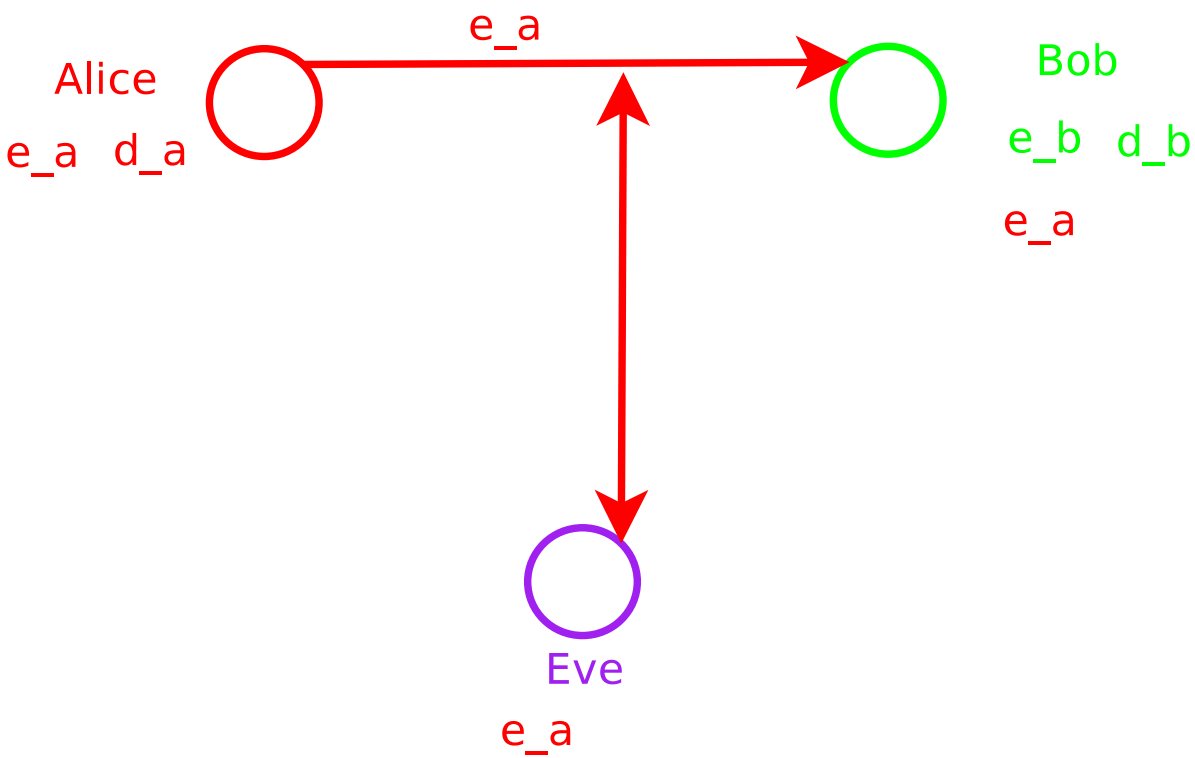
Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung

Am Beispiel RSA

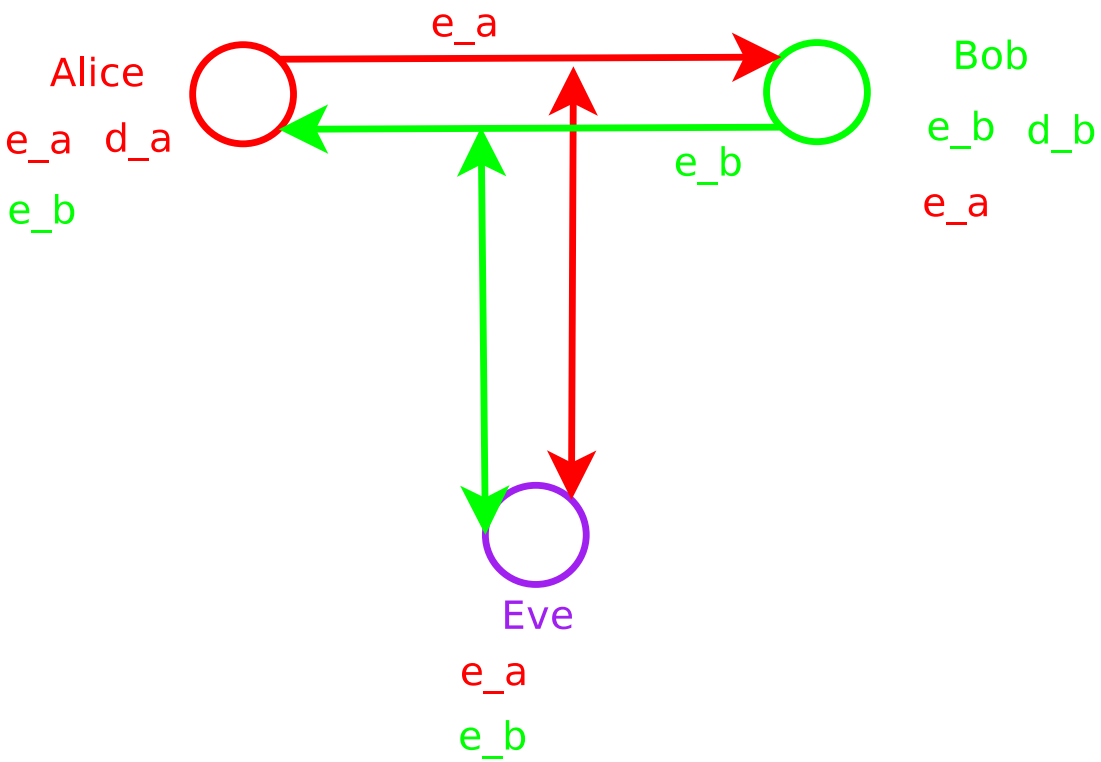
Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung

Am Beispiel RSA

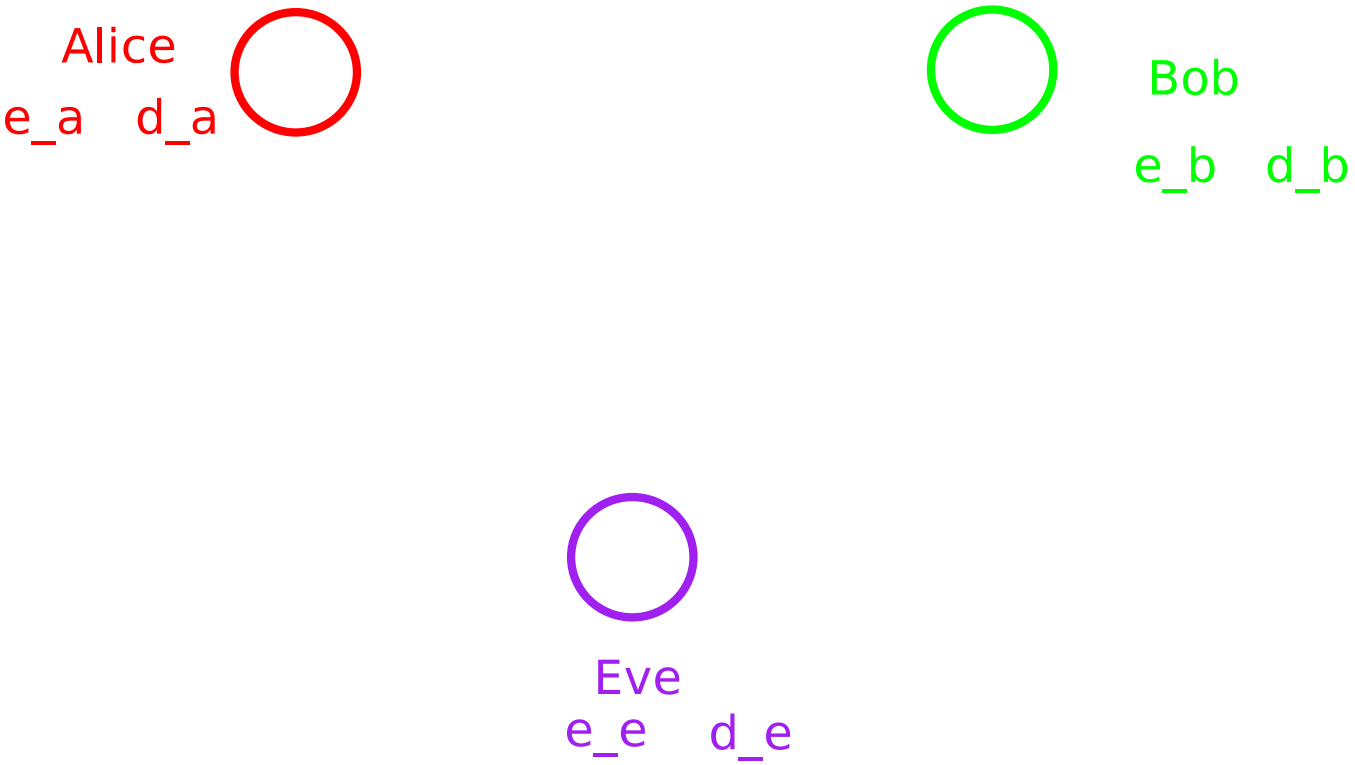
Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung

Am Beispiel RSA

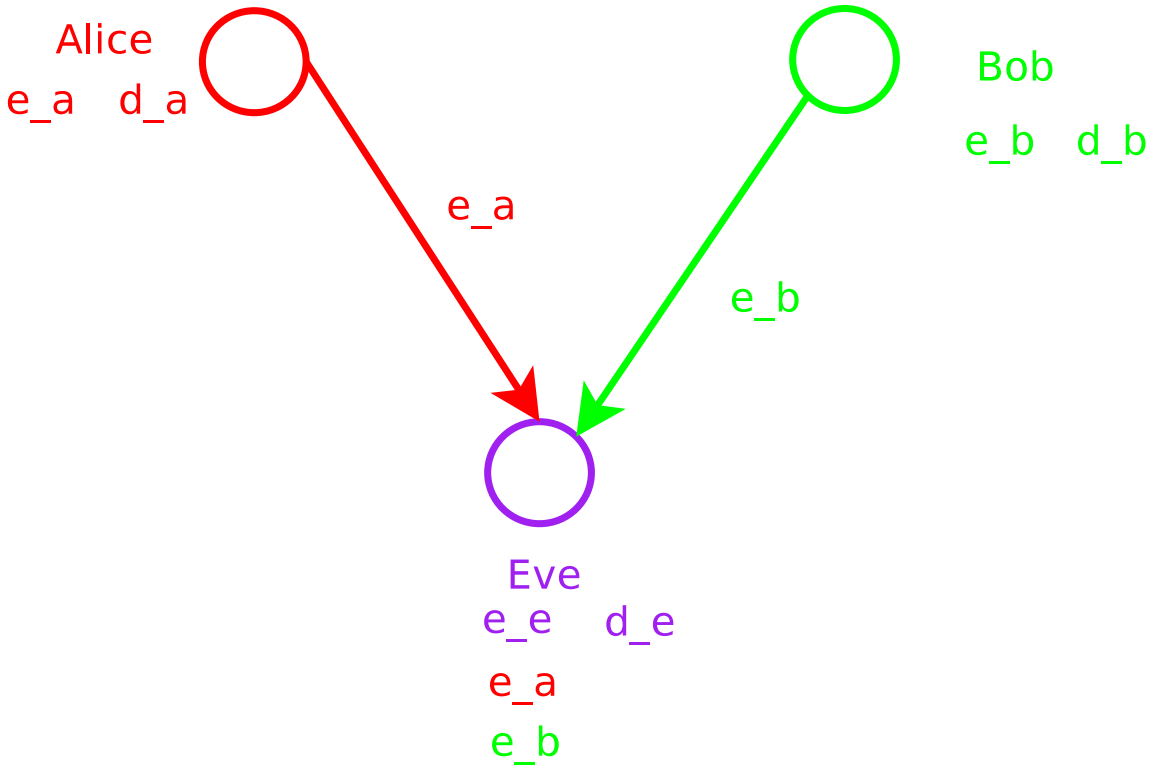
Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung

Am Beispiel RSA

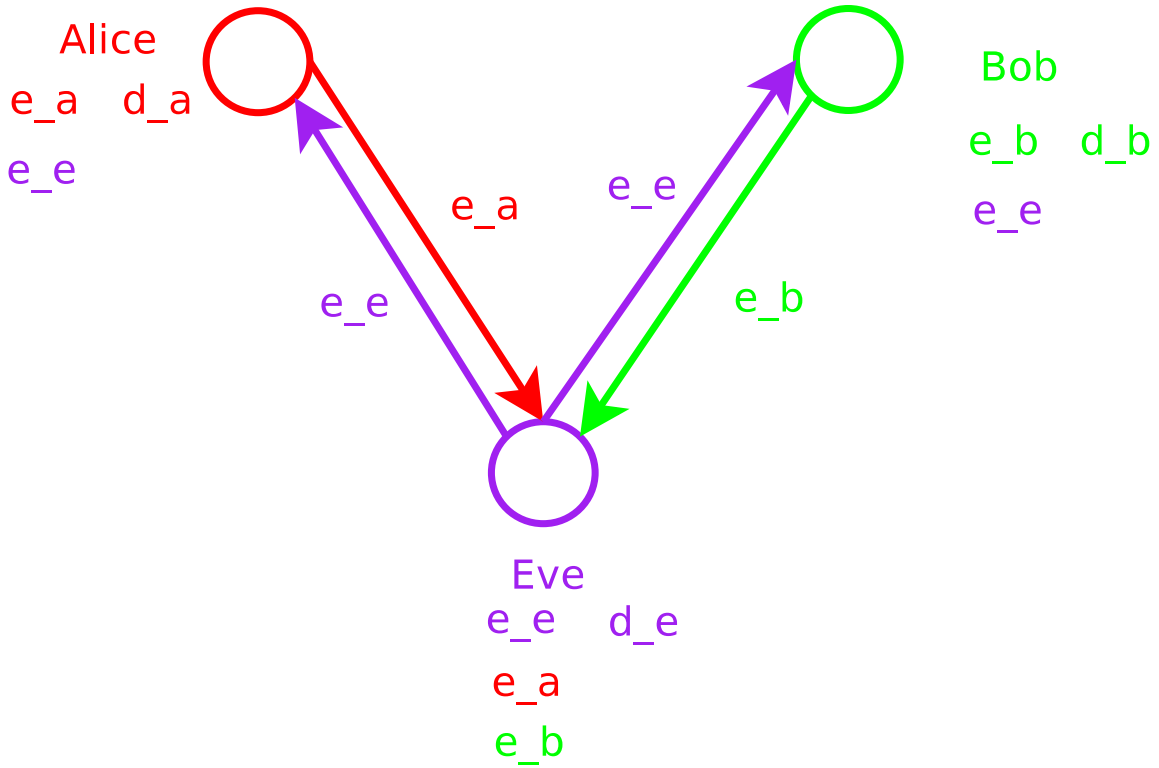
Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung

Am Beispiel RSA

Das Problem bei symmetrischen Verfahren ist der Schlüsselaustausch.



Asymmetrische Verschlüsselung
Am Beispiel RSA

- Vorteil: Kein Geheimhalten des öffentlichen Schlüssels notwendig
- Vorteil : Nur ein Schlüsselpaar für alle Kontakte notwendig
- Problem: Ist der Schlüssel wirklich von Bob (Alice)?
- Lösung : Fingerprint über “sicheren” Kanal austauschen (z.B. Telefon)
- Problem : Was wenn man die Stimme des anderen nicht kennt ? z.B. Rote Hilfe . . .

Antwort zum letzten Problem gibts später ! (**Web of Trust**)

Asymmetrische Verschlüsselung
digitale Unterschrift mit RSA

Das zweite Problem ist die Authentizität einer Nachricht. Nehmen wir an Eve schickt die mit dem öffentlichen Schlüssel von Alice verschlüsselte Nachricht “Ich hasse dich, Bob” an Alice.

Wie stellt Alice fest ob die Nachricht wirklich von Bob kommt ?

Sei d Decodierfunktion e Codierfunktion t ein Klartext und d_b, e_b privater und öffentlicher Schlüssel von Bob.

Es gilt $d(d_b, e(e_b, t)) = t$ aber auch $e(e_b, d(d_b, t)) = t$

Dadurch wird eine digitale Unterschrift möglich.

Asymmetrische Verschlüsselung
digitale Unterschrift mit RSA

Annahme Bob will denn Text k versenden. e_a ist der öffentliche Schlüssel von Alice.

Bob unterschreibt nun k mit seinem privaten Schlüssel d_b und schickt nun den Text k zusammen mit $d(d_b, k)$ verschlüsselt an Alice.

Alice entschlüsselt den Text liest den Text k und überprüft ob $e(e_b, d(d_b, k)) = k$ ist. Wenn ja ist der Text von Bob ansonst nicht.

Asymmetrische Verschlüsselung
Web of Trust

1. Alice (USA) und Carol (Russland) kennen sich nicht
2. Alice und Carol kennen beide Bob
3. Bob (Flugkapitän) kennt Alice und Carol und hat deren Schlüssel überprüft (Ausweisprüfung)
4. Bob unterschreibt Schlüssel von Alice und Carol
5. Alice und Carol verifizieren Bobs Unterschrift
6. Alice und Carol vertrauen evtl. dem Schlüssel des anderen
7. Alice und Carol unterschreiben sich **nicht !!!** gegenseitig die Schlüssel
8. Signing Partys

Asymmetrische Verschlüsselung
Web of Trust

Man unterscheidet nun grundsätzlich zwei mögliche Varianten des Unterschreibens von Schlüsseln.

Die erste Möglichkeit ist, dass es eine **zentrale Zertifizierungsstelle (Welt)** gibt die alle Schlüssel unterschreibt oder **lokale Zertifierungsstellen (Afrika,Amerika,Antarktis,Asien,Australien,Europa)** akkreditiert die wiederum Schlüssel unterschreiben.

Asymmetrische Verschlüsselung
Web of Trust

Das Problem bei diesem hierarchischen Aufbau ist jedoch, dass der zentralen Zertifizierstelle vertraut werden muss und sie **nicht kontrolliert werden kann**.

Der andere Ansatz, der z.B. bei **GPG** verwendet wird, ist der, dass jeder die öffentlichen Schlüssels jedes anderen unterschreiben kann und somit ein **dezentrales "Web of Trust"** entsteht.

Asymmetrische Verschlüsselung

RSA Funktionsweise

Wir bestimmen $n = p * q \quad , n, p, q \in \mathbb{N},\ p, q$ prim.
Desweiteren bestimmen wir $a, b \in \mathbb{N}$ mit $a * b \equiv 1 \pmod{\varphi(n)}$.
Unser Schlüssel ist nun $s = (n, p, q, a, b)$. Wir veröffentlichen nun (n, a) und (p, q, b) bleibt geheim.
$c_s(x) = x^a \bmod n$
$d_s(x) = x^b \bmod n$

Asymmetrische Verschlüsselung
RSA Sicherheit

Abschätzung bei Verdoppelung der Schlüssellänge, Primzahlssatz, nur relevant, falls gesamter Schlüsselraum durchsucht werden muss und nicht faktorisiert werden kann.

Angriffe
Watermarking etc

Zumindest bei dem symmetrischen Verfahren AES gilt, das es zwar nicht knackbar ist aber

1. Wassermarkierung möglich
2. Verschiebung von Daten möglich
3. gezielte Änderung von Daten möglich

Deswegen gibt es noch verschiedene Arten von Initialisationsvektoren **Initialisation Vector (IV)** für AES. Empfehlen tut sich hier z.B. AES mit 256 bit Schlüssellänge und XTS als IV.

Angriffe
Gefahrquellen

Es bringt bekanntlich wenig sich eine Stahltüre ins Haus einbauen zu lassen, wenn man im Erdgeschoß wohnt und immer alle Fenster offen lässt.

Das gleiche gilt auch für Verschlüsselung. Selbst wenn die obigen Verfahren sicher sind gibt es noch genügend andere Gefahrquellen .

Angriffe
Gefahrquellen

Beispiele :

- Trojaner, Virus, ...
- Verwenden eines closed source Programmen (z.B. Windows,Skype ...)
- Bug (z.B. Buffer Overflow) in einem Programm
- Aktiviertes Java,JavaScript, Flash ...im Browser
- Beteiligung an **Gewinnspielen** im Internet, persönliche Daten in StudiVZ,Facebook, ...

Angriffe
Gefahrquellen

Beispiele cont.:

- Suchmaschine und Email Acoount beim selben Anbieter !!!
- Harwarekeylogger und oder Kamera in der eigenen Wohnung (Lauschangriff, BKA,BND, . . .).
- Politik (Verbot von Kryptographie)
- Ausspähen der Kontakte (z.b. Alice kommuniziert immer mit der Antifa).
- Vorratsdatenspeicherung . . .

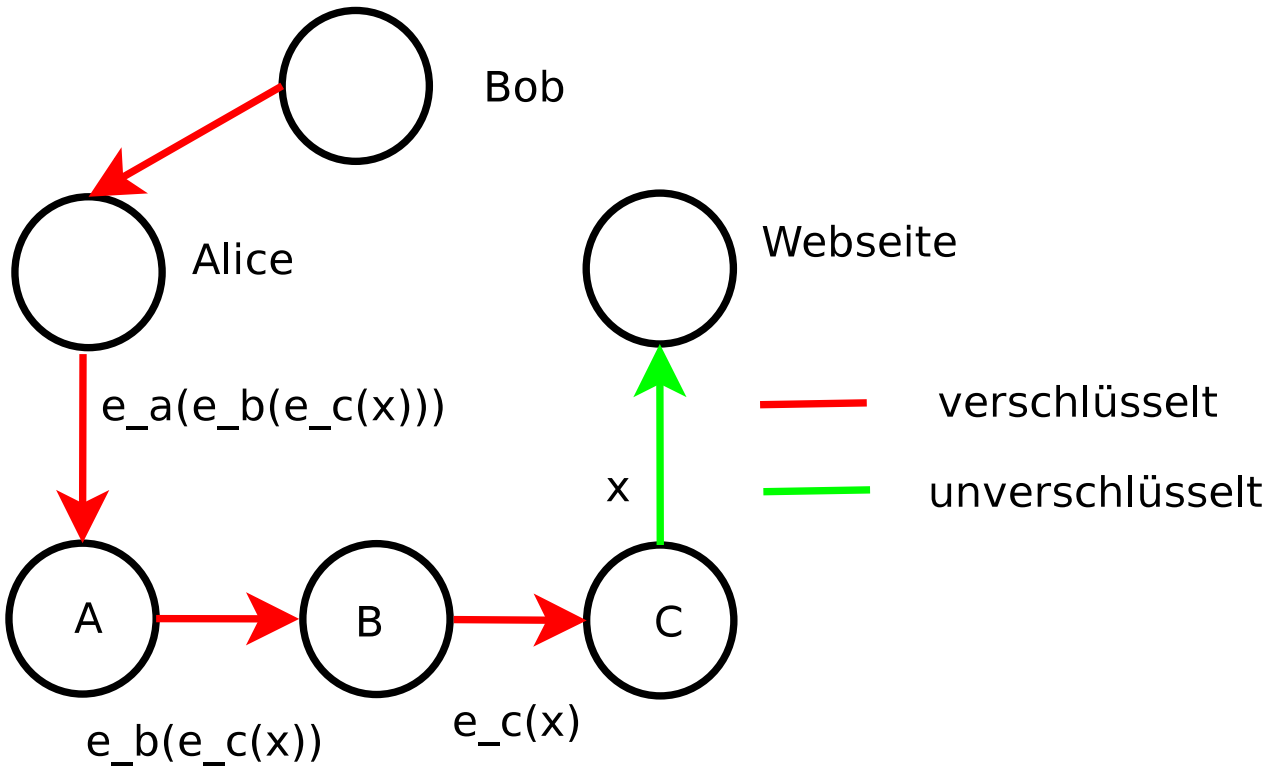
Vergleich symmetrisch asymetrisch

- Symmetrische Verfahren schnell, Problem Schlüsselübermittlung (Festplatte verschlüsseln)
- Assymetrisch langsam aber Schlüsselübermittlung besser (Email etc.)
- Hybrides Verfahren am Anfang einer Sitzung wird mittels assymetrischer Verschlüsselung ein symmetrischer Schlüssel ausgetauscht mit dem dann weiter verschlüsselt wird (VoIP,Videokonferenz etc.)

Empfohlene Verfahren

Verfahren	Min Länge	IV	Anwendungsgebiet
AES	128	XTS,CMC,EME	Datenträger verschlüsseln
Serpent	128	?	Datenträger verschlüsseln
RSA	1024	?	Email,Instant Messaging

Anonymisierung
Tor



Anonymisierung
Tor

Weitere Schutzmasnahmen :

- Nach einem gewissen Zeitintervall wird eine neue Route gewählt
- Pakete werden verzögert um Timing Angriffe zu verhindern bzw. erschweren
- Auch Zugriff auf Rechner im Tornetz möglich (Hidden Services). Dadurch sind Angebote im Tornetz nicht lokalisierbar und zensierbar
- Jedes Programm das Socks undterstützt kann Tor verwenden (Emailprogramme, InstantMessenger etc).
- Privoxy wird mitgeliefert mit dem Header z.b. vom Browser gefiltert werden können (nur http . . . , alternative Greasemonkey . . .). Eigene Regeln für JavaScript, Popups, . . .

Anonymisierung
Tor

Vorraussetzungen/ Nachteile:

- Tor ist insbesondere durch die künstliche Verzögerung von Pakten langsam
- Annahme A,B,C arbeiten nicht zusammen und Alice fungiert als Torknoten
- Liste von Torknoten muss bei der ersten Verbindung heruntergeladen werden (Vorsicht Manipulation)
- In China gehören 70 % der Torserver der Regierung
- Verbindung zur Webseite sollte falls möglich mit https erfolgen

Anonymisierung und Verschlüsselung

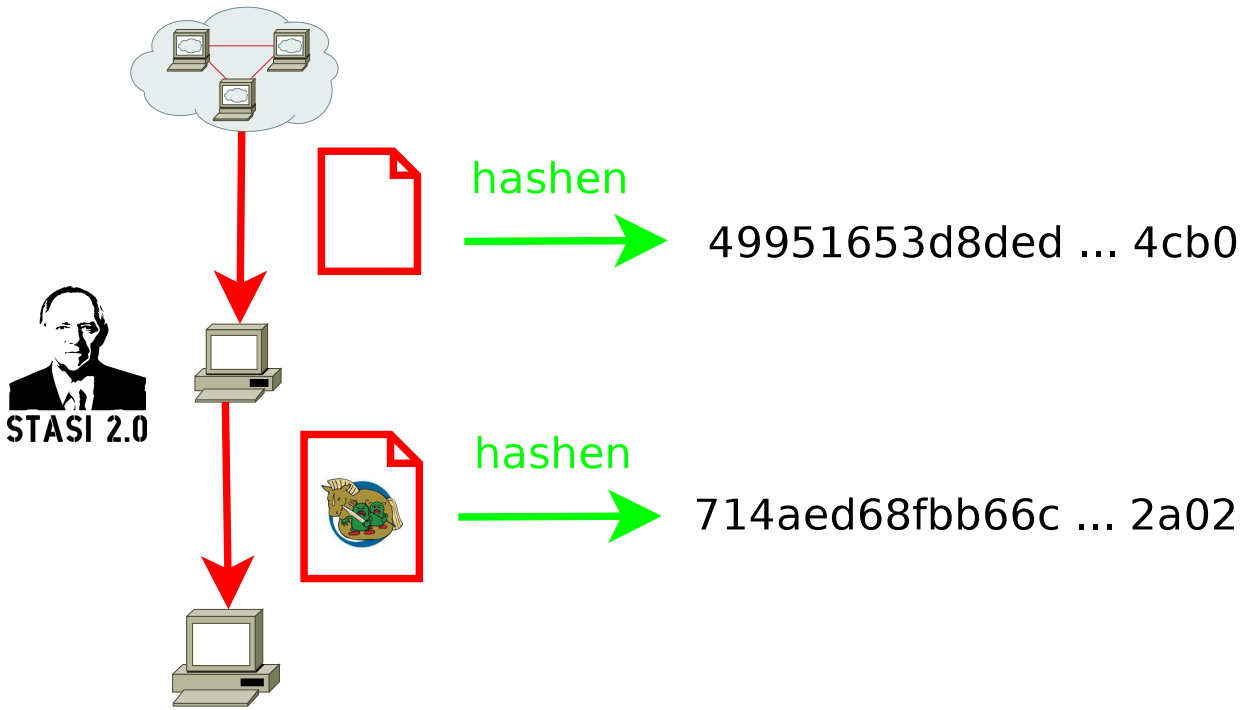
I2P - Invisible Internet Project

- Tor ist hauptsächlich entwickelt worden um als anonymisierender Proxy zu fungieren und sich mit normalen Webservern im Internet zu verbinden.
- Hidden Services werden eher seltener genutzt
- In I2P spielt sich fast alles im I2P - Netz ab, es gibt wenige Exit-Nodes.
- I2P wurde dafür entwickelt jegliches Protokoll im Internet, genauso wie die traditionellen verteilten Anwendungen (z. B. Squid oder auch DNS) zu unterstützen

Anonymes Filesharing

Es gibt spezielle Filesharing Programme, die die gleichen Funktionsweisen wie obige anonyme Netzwerke haben und mit direktem Hinblick auf Filesharing konzipiert wurden. Dadurch sind sie oft schneller.
Beispiele : Gnunet, Imule, I2Phex, Ants, Mute, ...

Hashes


hashen
49951653d8ded ... 4cb0
STASI 2.0
hashen
714aed68fbb66c ... 2a02

Hashes

Es gibt verschiedene Möglichkeiten damit umzugehen (z.B. über https und Zertifikate gesicherter Download).

Es gibt aber auch die Möglichkeit z. B. einen Hash, eine Art Fingerabdruck einer Datei zu erzeugen, diesen Hash mit seinem GPG Schlüssel zu unterschreiben und neben dem eigentlichen Download zur Verfügung zu stellen (Näheres im Workshop).

Einige Hashes gelten schon als kryptographisch geknackt z. B. Md5sum, sha1sum. Man sollte sha256sum,sha512sum . . . verwenden.

Sichere Passwoerter

Sichere Passwörter enthalten **nicht** :

- Geburtstag oder Name von Mutter, Vater, Kind, Frau, Mann, Freundin, Freund, Katze, Hund ...
- Sachen an denen man arbeitet z. B. im Beruf, Studium ...
- Keine Wörter die man mit Kenntnis deiner Person erraten könnte.
- Keine Wörter, die im Wörterbuch, egal in welcher Sprache vorkommen
- Keine berühmten Texte oder Ausschnitte davon, wie z.b. Das Manifest der kommunistischen Partei, ...

Sichere Passwoerter

Sichere Passwörter

- enthalten Buchstaben,Ziffern und Sonderzeichen
- sind möglichst “zufällig” gewählt
- sind einfach zu merken, so dass man sie nicht aufschreiben muss

Sichere Passwoerter

- keine Pseudozufallsgeneratoren verwenden
- möglichst Hardware verwenden
- Möglichkeit Passwörter auszuwürfeln
- http://world.std.com/~reinhold/diceware.html

Allgemeine Schutzmasnahmen

- Verwenden von “Free Software”
- Gnu / Linux
- Virtualisierung
- Firewall,Antivirusprogramm
- Richtige Konfiguration benötiger Dienste
- Abstellen von Java,JavaScript, Flash im Browser
- Hash
- Sichere Passwörter (Würfel verwenden)

Free Software - Freie Software

Free Software - Freie Software

Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it refers to four kinds of freedom, for the users of the software:

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and adapt it to your needs (freedom 1). Access to the source code is a precondition for this.

Free Software - Freie Software

- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this.

Richard Stallman der Marx der Informatiker.
http://www.gnu.org/philosophy/free-sw.html

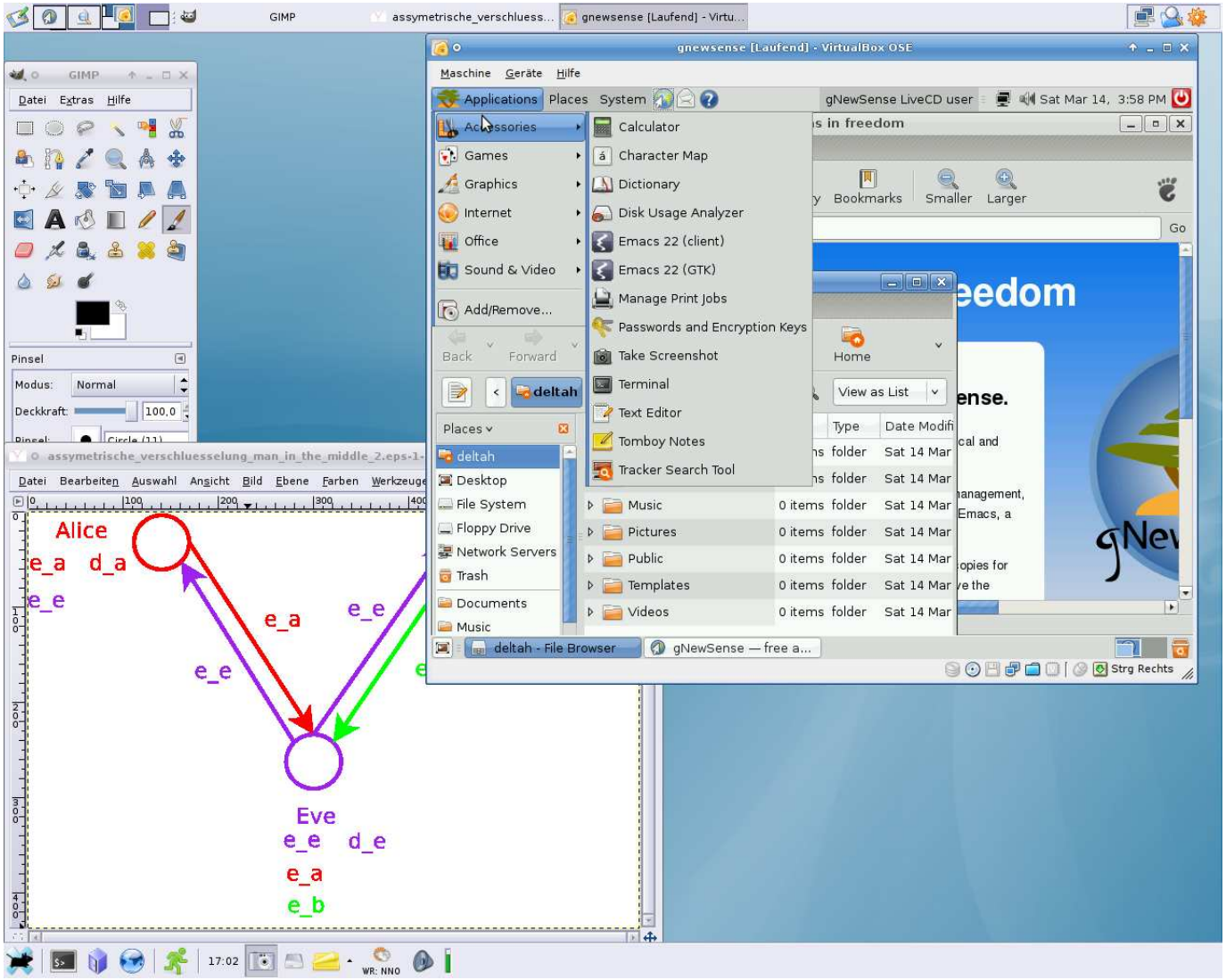
Free Software - Freie Software
GNU GPL

Eine sehr bekannte Lizenz ist die GNU **G**eneral **P**ublic **L**icense **(GNU GPL** oder kurz **GPL)**

- Quellcode muss verfügbar sein
- Anpassen, Weiterentwicklung des Quellcodes erlaubt
- Weitergabe nur unter Einräumung derselben Lizenz
- Klauseln um Hardware DRM und Softwarepatente zu bekämpfen (GPLv3)

Ein Beispiel für ein Betriebssystem, das unter dieser Lizenz steht, ist Gnu/ Linux.
Bei Windows hingegen gab es schon Verdachtsmomente, das Microsoft Hintertüren für die NSA eingebaut hat.

Virtualisierung



Was fehlt ?

- Quantenkryptographie
- Mobilfunk, RFID, Funkkameras, ...
- Überwachung des öffenlichen Raumes (Kameras ...)
- Spezielle Programme für Email,VOIP, Instant Messaging ...
- ...

Fragen ?

Fragen ?