20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.
Peer Heinlein <p.heinlein@heinlein-support.de>

20 Dinge über Verschlüsselung die Sie schon immer mal wissen (w|s)ollten.

[Vortrag per Videokonferenzschaltung zum 200. Unix-Stammtisch Chemnitz]

Peer Heinlein <p.heinlein@heinlein-support.de>

- **Heinlein Support**
  - IT-Consulting und 24/7 Linux-Support mit 25 Mitarbeitern
  - Eigener Betrieb eines ISPs seit 1992
  - Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

- 24/7-Notfall-Hotline: 030 / 40 50 5 - 110
  - 25 Spezialisten mit LPIC-2 und LPIC-3
  - Für alles rund um Linux & Server & DMZ
  - Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
  - Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil I: Grundlagen

Was ist die älteste bekannte Verschlüsselung?

Was ist die älteste bekannte Verschlüsselung?

- Kodierung bestimmter Wörter durch besondere Zeiten in alt-ägyptischen religiösen Schriften um 3000 v.Chr.
- Tonscheiben um 1500 v.Chr mit vertauschen Buchstaben
- Atbasch ist ein altes jüdisches Verschlüsselungsverfahren bei dem gegen ein Rückwärts-Alphabet verschlüsselt wird
  - A=Z, B=Y, C=X usw. usf.
- Cäser verwandte ROT-3

Wie funktioniert symmetrische Verschlüsselung?

Wie funktioniert symmetrische Verschlüsselung?

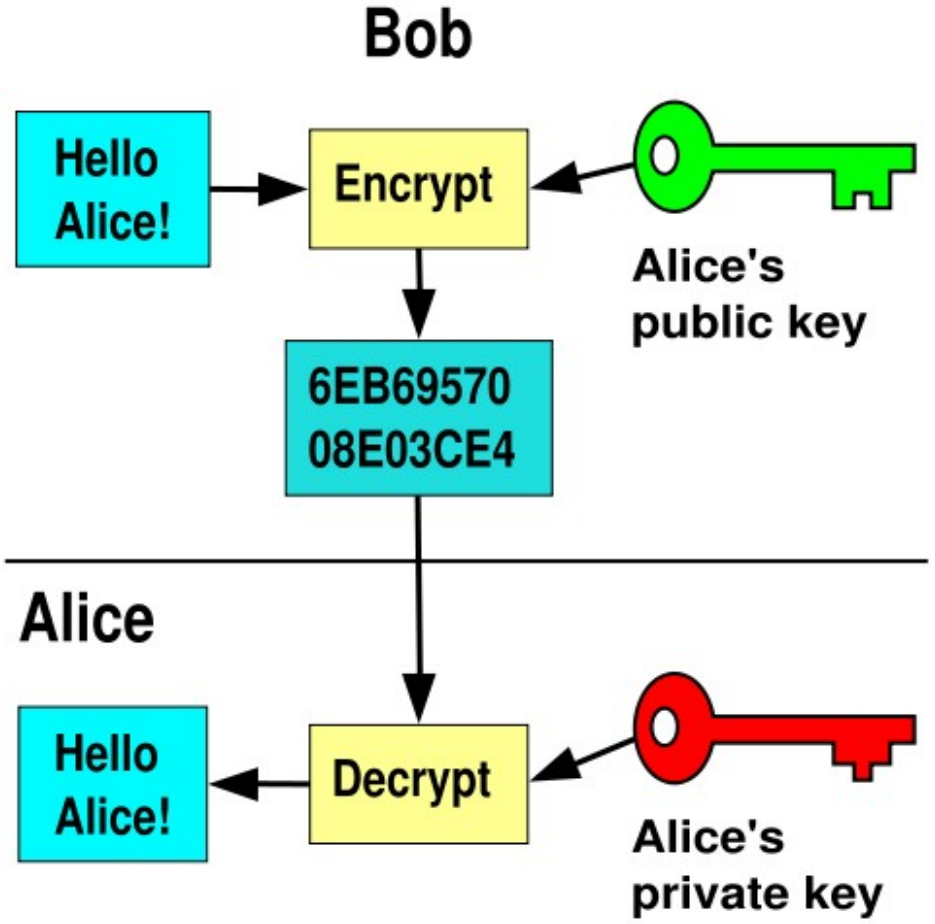
- Daten werden mit einem Schlüssel einer umkehrbaren Rechenoperation unterzogen.
  - Gleicher Schlüssel für Ver- und Entschlüsselung.
- Das Problem: Wie gelangt der Schlüssel sicher zur Gegenseite, wenn nur ein (unsicherer) Kanal zur Verfügung steht?
  - Brieftaube, Bote, anderes Geheimwissen

Wie funktioniert asymmetrische Verschlüsselung?

Wie funktioniert asymmetrische Verschlüsselung?

- Eine asymmetrische Verschlüsselung besteht immer aus zwei Key-Teilen:
- Der Private Key:
  - Kann für ihn verschlüsselte Daten entschlüsseln
  - Kann mit seiner Identität unterschreiben
- Der Public Key:
  - Kann Daten an den Private Key verschlüsseln
  - Kann die Unterschrift eines Secret Keys verifizieren
- Bei Mailkommunikation sind immer zwei Schlüsselpaare beteiligt
  - Bei SSL/TLS übrigens nur ein Schlüsselpaar. Dazu später mehr. :-)

Wie funktioniert asymmetrische Verschlüsselung?



heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

Peer Heinlein <p.heinlein@heinlein-support.de>

WHO

heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

Peer Heinlein <p.heinlein@heinlein-support.de>

THE

heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

Peer Heinlein <p.heinlein@heinlein-support.de>

FUCK

heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

Peer Heinlein <p.heinlein@heinlein-support.de>

IS

heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

Peer Heinlein <p.heinlein@heinlein-support.de>

ALICE

heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.
Peer Heinlein <p.heinlein@heinlein-support.de>

WHO THE FUCK IS ALICE

heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

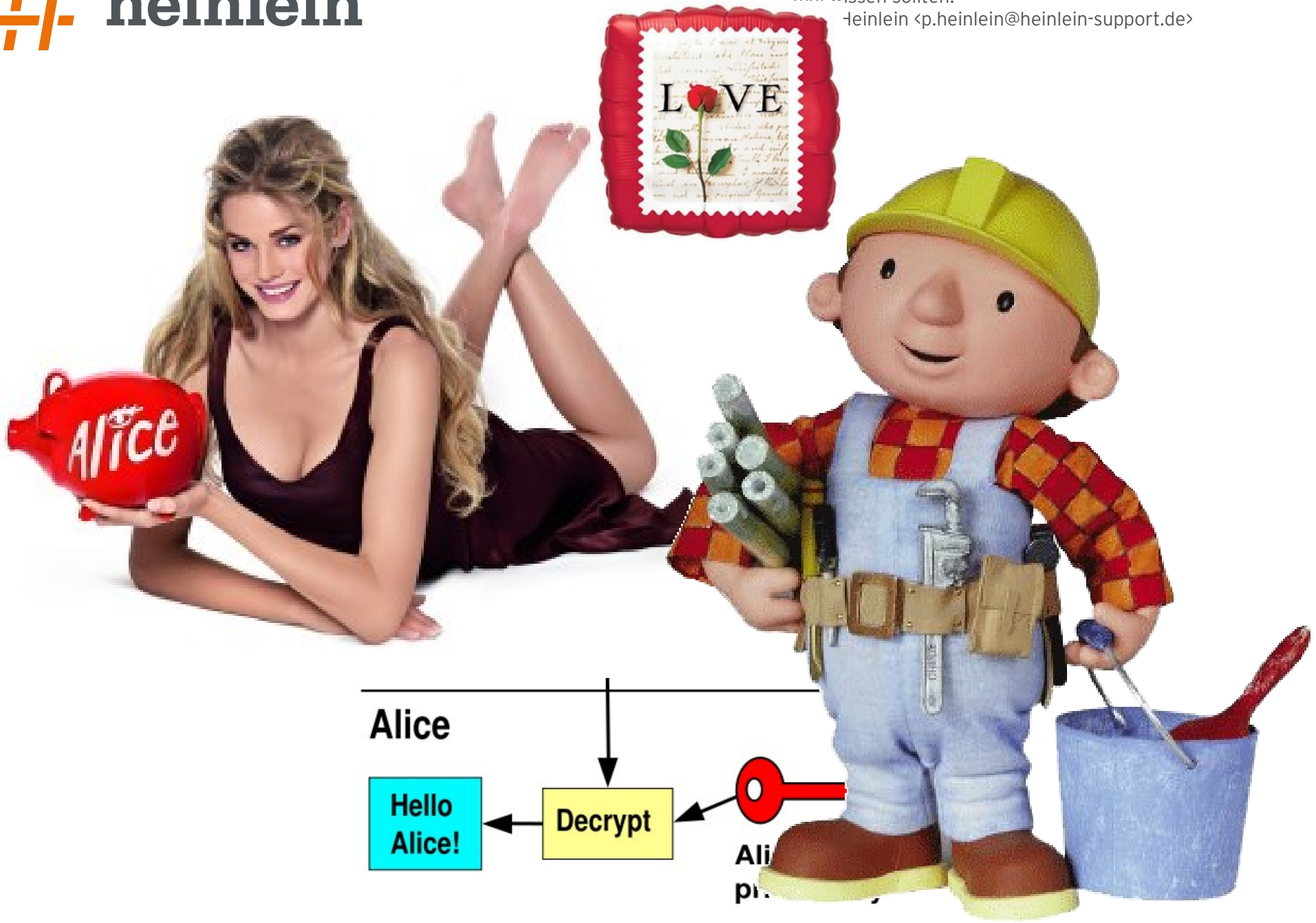
Peer Heinlein <p.heinlein@heinlein-support.de>

WHO THE FUCK IS ALICE?

heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

Heinlein <p.heinlein@heinlein-support.de>



heinlein

20 Dinge über Verschlüsselung, die Sie schon immer mal wissen sollten.

Peer Heinlein <p.heinlein@heinlein-support.de>

Alice

Hello Alice!

Teil II:
Details

Peer Heinlein <p.heinlein@heinlein-support.de>

Wieso benötigt SSL/TLS nur ein Schlüsselpaar auf dem Server?

Wieso benötigt SSL/TLS nur ein Schlüsselpaar auf dem Server?

- Client und Server generieren Zufallszahlen, begrüßen sich, teilen sich die möglichen Spezifikationen mit.
- Der Server sendet seinen Public Key an den Client
  - (Optional: Der Client könnte sich jetzt seinerseits authentifzieren)
- Der Client generiert einen symmetrischen (!) Schlüssel, verschlüsselt diesen mit dem Public Key des Servers und sendet ihn zurück
- Beide Seiten wechseln auf eine symmetrische Verschlüsselung
  - Symmetrische Verschlüsselung ist Faktor 1000 schneller!
  - Symmetrischer Schlüssel wird ggf. gecacht und wiederholt verwendet.

Was ist der Unterschied zwischen SSL und TLS?

Was ist der Unterschied zwischen SSL und TLS?

- In der Geschichte gab und gibt es:
  - SSLv1 – Version 1 (1994, obsolet, unsicher)
  - SSLv2 – Version 2 (1995, obsolet, unsicher)
    - Private Communication Technology (PCT) von Microsoft
  - SSLv3 – Version 3
  - TLS 1.0 – alias SSL-Version 3.1 (Umbenennung 1999)
  - TLS 1.1
  - TLS 1.2
- Es gibt keinen großen Unterschied zwischen TLS und SSL. TLS werden die aktuellen Versionen genannt.

Was ist der Unterschied zwischen PGP und S/MIME?

Was ist der Unterschied zwischen PGP und S/MIME?

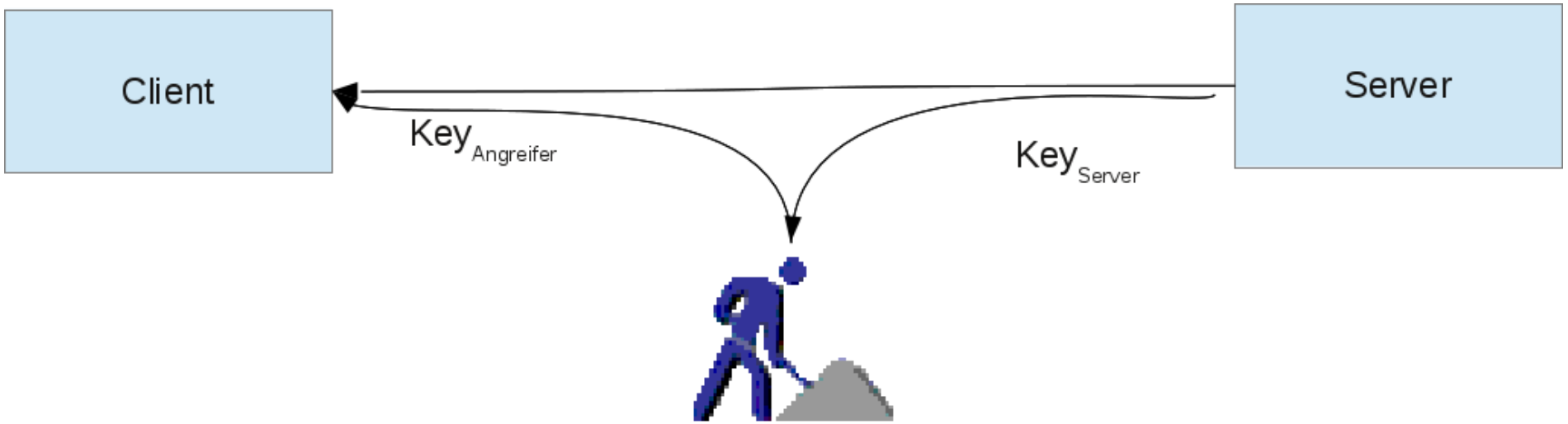
- Beide Verfahren setzen asymmetrische Verschlüsselung ein
  - Keine Unterschiede in der Qualität der Verschlüsselung!
- PGP:
  - Authentizität eines Schlüssels wird durch eine oder mehrere Unterschriften anderer vertrauenswürdiger Personen sichergestellt.
  - Es bildet sich ein „web of trust“
- S/MIME:
  - Authentizität eines Schlüssels wird durch ein x.509-Zertifikat sichergestellt, das von einer (per Definition vertrauenswürdigen) CA ausgestellt wurde
  - Es bildet sich eine „chain of trust“

Was macht eigentlich eine CA?

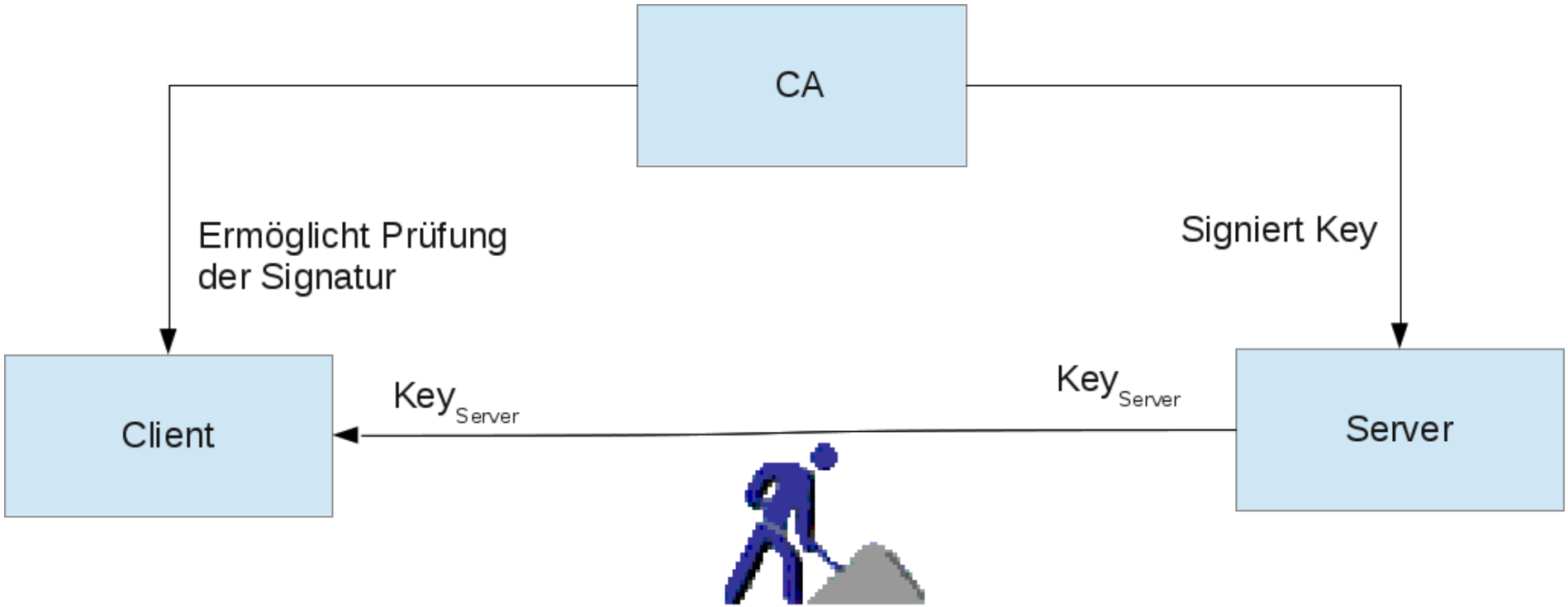
Was macht eigentlich eine CA?

- Eine CA besteht aus einem Secret Key und einem Public Key.
  - Der Public Key ist in Browsern und Betriebssystemen bereits enthalten.
  - Das ist der „Wert“ der CA.
- Ein „Certification Request“ ist ein unsignierter Public Key.
  - Die CA sollte (!) meine Identität eingehend prüfen, bevor sie signiert.
- Der Client erhält vom Server den signierten Public Key.
  - Er kann jetzt aber die Signatur der CA prüfen.
  - Die CA-Signatur schützt vor Schlüsseltausch. Dafür bezahle ich

Was macht eigentlich eine CA?



Der Angreifer entschlüsselt, liest und verschlüsselt mit dem Server-Key neu.



Der Angreifer kann den Schlüssel nicht mehr unbemerkt austauschen.

Welche vertrauenswürdige CAs kann man benutzen?

Welche vertrauenswürdige CAs kann man benutzen?

- Natürlich kann man sich eine „besonders sichere“ CA für das eigene Zertifikat aussuchen
  - Entscheidend für mich ist, dass möglichst viele Clients das Zertifikat akzeptieren
  - Ob die eigene CA besonders vertrauenswürdig ist, oder nicht, ist egal!
- Sobald aber irgendeine (!) weit verbreitete CA ein unberechtigtes Zertifikat ausstellt, ist die Sicherheit im Eimer.
  - Auch die meiner eigenen Server, selbst wenn ich eine tolle CA habe!
- Entscheidend ist also ganz allgemein „welche“ CAs es da draußen so gibt und ob da jemand Mist baut.
  - Es gibt CAs, die kurzlebige Zertifikate ohne ausreichende Prüfung ausstellen.

Sind selbstsignierte Zertifikate schlechter?

Sind selbstsignierte Zertifikate schlechter?

- Selbstsignierte Zertifikate haben das Manko, daß sie nicht von einer bekannten CA unterschrieben sind.
  - Die Authentizität des Keys kann also nicht mehr überprüft werden
  - Ein man-in-the-middle könnte den Keys ausgetauscht haben
- Das Risiko liegt also nur darin, dass beim allerersten Key-Austausch kein man-in-the-middle anwesend war.
  - Spätere Schlüsselmanipulationen würden wieder eine Warnung liefern.
- Verschlüsselung auf Basis selbstsignierter Zertifikate ist jedoch ansonsten genauso sicher oder unsicher, wie sonst auch

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil III:
Sicherheit im Praxistest

Welche Cipher gelten derzeit als sicher?

Welche Cipher gelten derzeit als sicher?
Strom-/Blockverschlüsselungen

- RC4 Stromverschlüsselung: Vermutlich sehr gut decodierbar.
  - Teilweise Vorhersehbarkeit, nicht ausreichend zufällig genug
  - Viel in WEP und SSL/TLS im Einsatz
  - In den vergangenen Jahren wurde wegen CBC-Problemen zu RC4 gewechselt
  - Akut unsicher
- AES-Blockverschlüsselung (Rijndael), AES-128, AES-192, AES-256
  - Supercomputer für 80 Mrd. Dollar könnte AES-128 knacken
  - Strombedarf aber 4 Terawatt (mehr als USA gesamt)
  - Ausreichend sicher.
  - Aber: Blockverschlüsselungen unter TLS benötigen cipher-block chaining (CBC), hier gibt es vor TLS 1.2 akute Implementierungsprobleme.

Welche Cipher gelten derzeit als sicher?
Asymmetrische Cipher

- RSA (Rivest, Shamir und Adleman)
  - 512 und 1024 Bit sind brechbar, gelten nicht mehr als sicher
  - Es gilt als sicher, daß die NSA ein RSA 1024 im Einzelfall knacken kann
  - Aber geht das auch in großer Masse?
  - RSA mit 2048 Bit gilt als sicher
- DSA Digital Signatur Algorithmus (ElGamal)
  - Von einem ehemaligen NSA-Mitarbeiter entwickelt
  - Lange war DSA 1024 Standard bei PGP
  - Gilt aber als sehr gut untersucht und sicher
  - Hat gleiche Schlüssellängensicherheit wie RSA
  - Braucht aber sehr gute Zufallszahlen, sonst unsicher. RSA gilt als besser.

Welche Cipher gelten derzeit als sicher?
Elliptic Curve Cryptographie

- ECDSA Elliptic Curve DSA
  - Basieren auch auf dem Problem diskreter Lograrithmen
  - Aber im Sinne der Komplexitätstheorie schwerer umzukehren, darum sind kürzere (=schnellere) Schlüssel möglich
  - Diese elliptischen Kurven wurden jedoch in einem geschlossenen Verfahren vom US-NIST entwickelt
  - Aktuell unklar, wieviel Einfluß die NSA auf das US-NIST und die Kurvengestaltung genommen hat! Hintertür vorstellbar.
  - Bruce Schneier, Dan Bernstein und Tanja Lange: NIST-Kurven nicht nutzen.

Welche Cipher gelten derzeit als sicher?
Hash-Verfahren

- MDA5 und SHA-1 sind als Hashverfahren oft beteiligt
  - Kollisionsangriffe sind denkbar. Digitale Signaturen begünstigen das.
- SHA-2 wurde von der NSA mitentwickelt, gilt aber als sicher
- SHA-3 noch nicht abschließend spezifiziert

Kann die NSA in Echtzeit entschlüsseln?

Kann die NSA in Echtzeit entschlüsseln?

- Genaues weiß man nicht, aber es spricht vieles dafür, daß die NSA gewisse Crypto-Standards so gut angreifen kann, daß auch eine Entschlüsselung im großen Stil denkbar ist.
- Gerade der bei SSL/TLS zum Einsatz kommende RC4-Algorithmus gilt mittlerweile als ausreichend schnell durch die NSA decodierbar.
- Die NSA präsentierte 2010 bei GHCQ: „*Neue kryptoanalytische Fähigkeiten werden jetzt eingesetzt. Unmengen verschlüsselter Internet-Daten, die bis bis jetzt verworfen werden mussten, sind jetzt nutzbar.*“

Was hat es mit diesem „Perfect Forward Secrecy“ auf sich?

Was hat es mit diesem „Perfect Forward Secrecy“ auf sich?

- Das Problem: Einmal aufgezeichnete verschlüsselte Daten könnten nachträglich decodiert werden, wenn „jemand“ in den Besitz der verwendeten Langzeitschlüssel gelangt.
- Die NSA speichert gezielt verschlüsselte Daten, um sie später zu decodieren.
- Snowden: Wer verschlüsselt erhöht die Chance, daß die NSA seine Daten speichert. Wer verschlüsselt, macht sich verdächtig.
  - Gerade darum sollte man immer verschlüsseln und nicht nur dann, wenn es „geheim“ zugehen soll.
  - Nadel-im-Heuhaufen-Prinzip.

Was hat es mit diesem „Perfect Forward Secrecy“ auf sich?

- „Perfect Forward Secrecy“ basiert auf DHE- (Diffie Hellmann) und ECDHE-Verfahren (Elliptic Curve DHE).
  - DHCE mit openssl 0.9x ist rechenaufwändig
  - EDHCE ab openssl 1.0 ist recht performant
- Zu Beginn wird ein weiterer kurzlebiger Sitzungsschlüssel ausgerechnet, der nicht übertragen werden muß.
- Aufgezeichnete Kommunikation ist nachträglich nicht mehr entschlüsselbar

Teil IV: Mathematik (Hefte raus!)

Wie funktionieren elliptische Kurven in der Kryptographie?

Definition [Bearbeiten]

E heißt elliptische Kurve über dem Körper K, falls die folgenden äquivalenten Bedingungen erfüllt sind:

- E ist eine glatte projektive Kurve über K vom Geschlecht 1 mit einem Punkt $\mathcal{O}$, dessen Koordinaten in K liegen.
- E ist eine glatte projektive Kubik über K mit einem Punkt $\mathcal{O}$, dessen Koordinaten in K liegen.
- E ist eine glatte, durch eine Weierstraß-Gleichung
  $$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$
  gegebene projektive Kurve mit Koeffizienten $a_i \in K$. Schreibt man
  $$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$
  so ist E gerade die Nullstellenmenge des homogenen Polynoms $F \in K[X,Y,Z]$. (Beachte: Der Punkt $(0:1:0) = \mathcal{O}$ erfüllt auf jeden Fall die Polynomgleichung, liegt also auf E.)

Fasst man E als affine Kurve auf, so erhält man eine affine Weierstraß-Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

bzw. ein affines Polynom $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in K[x,y]$. In diesem Fall ist E gerade die Menge der (affinen) Punkte, die die Gleichung erfüllen, zusammen mit dem so genannten "unendlich fernen" Punkt $\mathcal{O}$, auch als ∞ geschrieben.

Affine und projektive Ebene [Bearbeiten]

Der zweidimensionale Raum der K-rationalen projektiven Punkte ist definiert als

$$\mathbb{P}^2(K) = \{(X,Y,Z) | X,Y,Z \in K \text{ nicht alle gleich } 0\} / \sim$$

mit der Äquivalenzrelation

$$(X_1,Y_1,Z_1) \sim (X_2,Y_2,Z_2) \Leftrightarrow \exists \lambda \in K^* : (X_1,Y_1,Z_1) = (\lambda X_2, \lambda Y_2, \lambda Z_2).$$

Punkte aus $\mathbb{P}^2(K)$ werden üblicherweise als $(X:Y:Z)$ notiert, um sie von Punkten im dreidimensionalen affinen Raum zu unterscheiden.

Die projektive Ebene $\mathbb{P}^2(K)$ kann dargestellt werden als Vereinigung der Menge

$$\{(X:Y:1) | X,Y \in K\},$$

mit der durch $Z = 0$ erzeugten Hyperebene H von $\mathbb{P}^2(K)$.

$$H = \{(X:Y:0) | X,Y \in K \text{ nicht beide gleich } 0\}.$$

Um projektive Kubiken in der affinen Ebene darzustellen, identifiziert man dann für $Z \neq 0$ den projektiven Punkt $(X:Y:Z) = (\frac{X}{Z} : \frac{Y}{Z} : 1) = (x:y:1)$ mit dem affinen Punkt (x,y).

Im Fall einer elliptischen Kurve hat die (projektive) Polynomgleichung genau eine Lösung mit $Z = 0$, nämlich den Punkt im Unendlichen $\mathcal{O} = (0:1:0)$.

Beispiele [Bearbeiten]

- $E_1 : y^2 = x^3 - x + 1$ und $E_2 : y^2 = x^3 + 2x - \sqrt{3}$ sind elliptische Kurven über $\mathbb{R}$, da $\Delta_{E_1} = -4 + 27 = 23 \neq 0$ und $\Delta_{E_2} = 32 + 81 = 113 \neq 0$ sind.
- $E : y^2 = x^3 - x$ ist eine elliptische Kurve sowohl über $\mathbb{Q}$ als auch über $\mathbb{R}$, da die Diskriminante $\Delta_E = -4 \neq 0$ ist. Über einem Körper mit Charakteristik 2 dagegen ist $\Delta_E = 0$ und E singulär, also keine elliptische Kurve.
- $E : y^2 = x^3 + 1$ ist über jedem Körper mit Charakteristik ungleich 3 eine elliptische Kurve, da $\Delta_E = 27 = 3^3 \neq 0$ ist.

Über den reellen Zahlen gibt die Diskriminante eine Information über die Form der Kurve in der affinen Ebene. Für $\Delta_E < 0$ besteht der Graph der elliptischen Kurve E aus zwei Komponenten (linke Abbildung), für $\Delta_E > 0$ hingegen nur aus einer einzigen Komponente (rechte Abbildung).

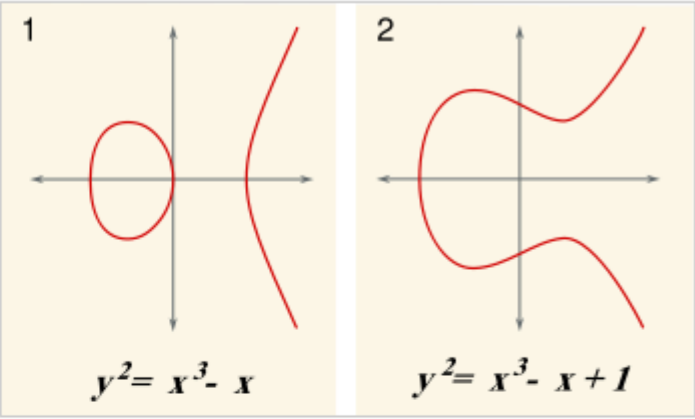


Schaubild der Kurven $y^2 = x^3 - x$ und $y^2 = x^3 - x + 1$

Elliptische Kurven über den komplexen Zahlen [Bearbeiten]

Interpretiert man wie üblich die komplexen Zahlen als Elemente der Gaußschen Zahlenebene, so stellen elliptische Kurven über den komplexen Zahlen eine zweidimensionale Fläche dar, die in den vierdimensionalen $\mathbb{C}^2$ eingebettet ist. Obwohl sich solche Flächen der Anschauung entziehen, lassen sich dennoch Aussagen über ihre Gestalt treffen, wie zum Beispiel über das Geschlecht der Fläche.

Komplexe Tori [Bearbeiten]

Es sei Γ ein (vollständiges) Gitter in der komplexen Zahlenebene $\mathbb{C}$. Die Faktorgruppe $\mathbb{C}/\Gamma$ ist eine eindimensionale abelsche kompakte komplexe Liegruppe, die als reelle Liegruppe isomorph zum Torus $S^1 \times S^1$ ist. Für eine Veranschaulichung kann man Erzeuger v, w von Γ wählen; der Quotient $\mathbb{C}/\Gamma$ ergibt sich dann aus der *Grundmasche*

$$\{\lambda v + \mu w \mid 0 \leq \lambda, \mu \leq 1\},$$

indem man jeweils gegenüberliegende Seiten verklebt.

Bezug zu ebenen Kubiken [Bearbeiten]

Ist Γ ein Gitter in der komplexen Zahlenebene, so definieren die zugehörige weierstraßsche p-Funktion und ihre Ableitung eine Einbettung

$$\mathbb{C}/\Gamma \to \mathbb{P}^2(\mathbb{C}), \quad z \mapsto (1 : \wp(z) : \wp'(z)),$$

deren Bild die nichtsinguläre Kubik

$$y^2 = 4x^3 - g_2(\Gamma)x - g_3(\Gamma)$$

ist. Jede nichtsinguläre ebene Kubik ist isomorph zu einer Kubik, die auf diese Weise entsteht.

Teil V: Verschlüsselung und E-Mails

Was ist eigentlich besser? SSL/TLS oder PGP+S/MIME?

Was ist eigentlich besser? SSL/TLS oder PGP+S/MIME?

- Weder noch.
- SSL/TLS verschlüsselt den Transportweg von Server zu Server.
  - Unklar bleibt, wieviele E-Mails / Daten übertragen werden
  - Unklar bleibt, wer mit wem reden
  - Unklar bleibt, zu welchem Thema (Subject) sie reden.
  - Aber auf dem Server und im Postfach selbst liegt die Mail im Klartext vor.
- PGP oder S/MIME verschlüsseln den Body (!) der E-Mail.
  - Wer mit wem wieviele E-Mails zu welchem Subject austauscht bleibt offen!
  - Dafür aber liegt für den Body eine Ende-zu-Ende-Verschlüsselung vor.
- BEIDE Verfahren sind sinnvoll und ergänzen sich!

Was ist eigentlich besser? SSL/TLS oder PGP+S/MIME?

- Viele Unternehmen setzen sündhafte teure S/MIME-Mailgateways ein, obwohl sie eigentlich nur eine Site-to-Site-Verschlüsselung für zu anderen Niederlassungen wollen.
- SSL/TLS wäre hier viel besser geeignet, aber das kostet kein Geld.
- S/MIME hingegen offenbahrt eklatante Kommunikationsdetails und / oder öffnet social engineering Tür und Tor.
  - Einige Krankenkassen kommunizieren mit Patientenbezug halböffentlich...
- War aber teuer, muß also gut sein. Für so'n SSL/TLS-Bastelkram ist die Kommunikation von $KONZERNVORSTAND nun wirklich zu wichtig.
  - („Ihr Admins seht das immer zu einfach. Wir brauchen was RICHTIGES.“)

Peer Heinlein <p.heinlein@heinlein-support.de>

Was taugt „E-Mail made in Germany“?

Was taugt „E-Mail made in Germany“?

Marketing

- E-Mail made in Germany ist ein geniales Marketing-Trick
  - Zur rechten Zeit am rechten Ort mal richtig fix gewesen! Respekt.
- Technisch ist es nichts anderes als

  20 Jahre nach allen anderen aktivieren auch web.de, GMX, T-Online und Freenet bahnbrechende Technologien wie SSL/TLS.
  - *Aber da muss es doch ganz bestimmt noch mehr geben?*
  - Nein, gibt es (derzeit zumindest) nicht.
  - *Aber so was wie eine Verifizierung der Gegenstelle?*
  - Nein. An Konzept wird noch überlegt...
  - *Aber dann kann ein man-in-the-middle das ja aufbohren?*
  - Ja. Kann er.

Bietet wenigstens DE-Mail eine sichere Verschlüsselung?

Bietet wenigstens DE-Mail eine sichere Verschlüsselung?

- DE-Mail bietet keine Ende-zu-Ende-Verschlüsselung auf Basis von nutzerindividuellen Schlüsseln.
- Stattdessen wird von Station zu Station verschlüsselt.
  - Auf dem jeweiligen Speicherserver liegt die E-Mail entschlüsselt herum.
  - Von der Qualität so wie SSL/TLS.
  - „Lawful interception“ ist also Tür und Tor geöffnet.
- DE-Mail hat nichts mit (Daten-) Sicherheit zu tun.
  - DE-Mail ist vor allem ein juristisches Konstrukt mit fragwürdigem Nutzen für den Bürger.

Welches Dilemma haben Unternehmen mit Kommunikationsverschlüsselung?

Welches Dilemma haben Unternehmen mit Kommunikationsverschlüsselung?

- Verschlüsseln Mitarbeiter auf dem Desktop, macht das Probleme:
  - Der Mitarbeiter ist krank oder scheidet aus
  - Mails müssen Langzeitarchiviert werden
  - Virencheck kann erst spät bei der Entschlüsselung durchgeführt werden
  - Mitarbeiter könnte den Schlüssel, das Unternehmen sein Wissen verlieren
- Wird nur Netz-Netz auf dem Gateway verschlüsselt, so bleibt als Restrisiko:
  - Der man-in-the-middle im eigenen Netz
  - Der unbefugte Zugriff auf ein Postfach mit Klartext-Mails
  - Der zentraler Speicherort für alle Keys des Unternehmens

Teil VI zum Abschied: Verschlüsselung, die keine Verschlüsselung ist.

Welche Verschlüsselung wurde am schnellsten geknackt?

Welche Verschlüsselung wurde am schnellsten geknackt?

Fail!

- 1998 wurde auf einer AES-Konferenz [illegible] Nachfolger für d[illegible] Verschlüsselungsverfahren DES gesuc[illegible]
- Die Telek[illegible]sentie[illegible]MAGENTA:

  M[illegible]tional Algorithm[illegible]-pur[illegible] Encryption and Net[illegible] Telecommunica[illegible]n App[illegible]ons
- Noch [illegible] der 20-mi[illegible]räsentation wurden bereits theore[illegible]e Angriffsmethoden dargelegt und nur wenig später auch pr[illegible] praktisch bewiesen.
  - Und dar[illegible]t die Telekom 8 Jahre lang gebastelt...

Hausaufgaben

- Erarbeiten Sie in Partnerarbeit mit ihrem Nachbarn die Grundmasche komplexer und reeller Liegruppen üblicher Tori indem Sie die gegenüberliegenden Seiten verkleben.
- Alternativ: Schreiben Sie Alice Schwarzer einen Brief und erklären Sie ihr das Geschlecht zweidimensionaler Flächen elliptischer Kurven.
- Kopieren Sie 1500 Bytes aus /dev/random und schicken Sie es an $KONZERNVORSTAND mit dem Betreff „Wichtig. EU-Ausschreibung“
- Entwickeln Sie einen unknackbaren Krypto-Algorithmus, der auf einen Bierdeckel paßt („Merz'sches Realitätstheoretikum“)

In diesem Sinne...

- Dank an Bertin Klein vom AGE der MPG hier in Köln für die Video-Konferenzschaltung

- Dank an Edward Snowden :-/
- Dank an alle vom Chemnitzer LinuxTag
- Dank an Euch alle Zuhörer für Spaß, Aufmerksamkeit und Ehre, hier den 200. Unix-Stammtisch Chemnitz bestreiten zu dürfen!

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich über Feedback!

Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 - 42

- Wenn's brennt:

  Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110