Public Key Kryptografie

mit Gnu Privacy Guard

Kendy Kutzner

2002-09-18

Warum Verschlüsselung?

”Zeige mir Einen, der keine finanziellen, sexuellen, gesellschaftlichen, politischen oder geschäftlichen Geheimnisse vor seiner Familie, seinen Nachbarn oder seinen Kollegen versteckt und ich zeige Dir jemanden, der ein außerordentlicher Exhibitionist oder ein unglaublicher Dummkopf ist.”

Warum Unterschriften?

- Sicherstellung von Identität

- Sicherstellung von Integrität

Ist Verschlüsselung böse?

Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Ruf ausgesetzt werden.
– Artikel 12 UN-Resolution 217A, 1948

”If privacy is outlawed, only outlaws will have privacy”
– Phillip R. Zimmerman, 1994

”They that can give up essential liberty to obtain a little temporary saftey deserve neither liberty nor saftey.”
– Benjamin Franklin, 1759

Verschlüsselungsverfahren

- symetrisch
  OTP, DES, IDEA, AES, TwoFish, BlowFish, CAST5

- asymetrisch (Public Key – Secret Key)
  RSA, ElGamal, DSA

- Hashfunktionen
  (CRC), MD5, SHA1, RIPEMD160

Vorsicht, Mathe!

- Drei Komponenten: symetrisches Verfahren I mit Schlüssel k, asymetrisches Verfahren mit Schlüssel S und P, Hashfunktion $h()$
- symetrischer Teil: $I_k(X) = c_1$ und $I_k(c_1) = X$
- asymetrischer Teil: $P(k) = c_2$ und $S(c_2) = k$
- Unterschrift: $S(h(X)) = c_3$ und $P(c_3) = h(X)$
- Nachricht von A an B: $c_1 c_2 c_3$ oder $P_B(k), I_k(X), I_k(S_A(h(X)))$

Geschichte, Patente, Versionen

2.3a	PRZ	erste ’funktionale’; RSA; ’Guerillia-Freeware’
2.4	ViaCrypt	kommerziell
2.5	PRZ,MIT	RSAREF; aber nicht mehr GPL
2.6		seit 1994-09-01 nicht mit 2.3 kompatibel
2.6ui		’unofficial international’
2.7	ViaCrypt	kommerziell
2.6.2i		empfohlen
2.6.3in	LD	Features wie Ablaufdatum
5.x	PGP Inc.	Windows; neu: 3DES, ElGamal, DSA; public, aber nicht GPL; anderes Dateiformat
5.0i		via Buch
5.5	PGP Inc.	ARR, RSA
6.x	NAI	Fotos, Festplatte, Kommandozeile

GNU Privacy Guard

1997-12	Version 0.0.0
1998-11	RFC2440 ”OpenPGP Message Format”
1999-09	Version 1.0.0
1999-11	BMWi vergibt 250000DM an GnuPG
2000-09	RSA Support
2002-04	Version 1.0.7

Unterschriften – Signaturen

- Unterschriften bestätigen:
  Zusammenhang Schlüssel – User ID

- Unterschriften bestätigen nicht:
  persönliche Referenzen, Vertrauen usw.

Vertrauen – Trust

- Probleme Schlüsselverteilung, Man the Middle
- Lösung Web of Trust
- Probleme Vorsatz und Dummheit, Vertrauen Privatsache
- Lösung `trustdb`: Ownertrust, Validity

Schwachstellen und Angriffe

- Der Mensch
  Passphrase, Schlüssel, Verfahren, Rubber Hose Cryptography, Bestechung, usw.

- Computer
  Multi-User Systeme, Tempest, Viren/Würmer/Trojaner, Swapfile, schwache Zufall-szahlen

- Algorithmen
  Brute Force, Man in the Middle, Choosen plaintext, choosen cyphertext, Unentdeckte Schwachstellen, Quantencomputer

Und jetzt?

- `gpg --keygen`
- (`gpg -a --gen-revoke` UID)
- `gpg -a export` UID / `gpg --send-key` UID
- `gpg --import` / `gpg --recv-key` UID
- `gpg --edit-key` UID

~/.gnupg/options

```
no-greeting
comment ""
encrypt-to 4EB1CF2D
#keyserver www.keyserver.net
#keyserver keyserver.cryptnet.net
#keyserver blackhole.pca.dfn.de
#keyserver wwwkeys.de.pgp.net
keyserver-options auto-key-retrieve include-disabled
      include-revoked verbose
```

Noch Fragen?

- RTFM
- http://www.google.com
- http://www-user.tu-chemnitz.de/~keku
- kendy.kutzner@e-technik.tu-chemnitz.de
- PGP Key ID 0xDB5BC18A