Das „wer, wie, was, warum?“ der Verschlüsselung

Mic <nomaster@chaosdorf.de>

Chaos Computer Club Düsseldorf / Chaosdorf e.V.

8. September 2013

Outline

CryptoParty

- Wir möchten den Menschen den praktischen Nutzen von Kryptographie erklären und ihnen bei der Installation der Programme auf ihren eigenen Geräten helfen.

CryptoParty

- Wir möchten den Menschen den praktischen Nutzen von Kryptographie erklären und ihnen bei der Installation der Programme auf ihren eigenen Geräten helfen.
- Wir hoffen, dass sie durch eigenständiges Handeln
  den Nutzen und die Wichtigkeit von Kryptographie verstehen.

CryptoParty

- Wir möchten den Menschen den praktischen Nutzen von Kryptographie erklären und ihnen bei der Installation der Programme auf ihren eigenen Geräten helfen.
- Wir hoffen, dass sie durch eigenständiges Handeln den Nutzen und die Wichtigkeit von Kryptographie verstehen.
- CryptoParties finden weltweit selbstorganisiert statt. Dabei sollen sie unabhängig und kostenlos bleiben.

Zitat

"Man is least himself when he talks in his own person.
Give him a mask, and he will tell you the truth."

— Oscar Wilde

Manifest

Manifest

1. Wir alle sind die User.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.
3. Privatsphäre ist ein Recht des Individuums.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.
3. Privatsphäre ist ein Recht des Individuums.
4. Privatsphäre ist Hoheit des Individuums.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.
3. Privatsphäre ist ein Recht des Individuums.
4. Privatsphäre ist Hoheit des Individuums.
5. Alle Menschen ist dieses Recht zuteil.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.
3. Privatsphäre ist ein Recht des Individuums.
4. Privatsphäre ist Hoheit des Individuums.
5. Alle Menschen ist dieses Recht zuteil.
6. Kryptographie ist für alle da.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.
3. Privatsphäre ist ein Recht des Individuums.
4. Privatsphäre ist Hoheit des Individuums.
5. Alle Menschen ist dieses Recht zuteil.
6. Kryptographie ist für alle da.
7. Überwachung und Zensur sind untrennbar. Maschinen sollen dazu nicht dienen.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.
3. Privatsphäre ist ein Recht des Individuums.
4. Privatsphäre ist Hoheit des Individuums.
5. Alle Menschen ist dieses Recht zuteil.
6. Kryptographie ist für alle da.
7. Überwachung und Zensur sind untrennbar. Maschinen sollen dazu nicht dienen.
8. Programmcode ist Sprache und unterliegt dem Recht auf freie Meinungsäußerung.

Manifest

1. Wir alle sind die User.
2. Privatsphäre ist Menschenrecht.
3. Privatsphäre ist ein Recht des Individuums.
4. Privatsphäre ist Hoheit des Individuums.
5. Alle Menschen ist dieses Recht zuteil.
6. Kryptographie ist für alle da.
7. Überwachung und Zensur sind untrennbar. Maschinen sollen dazu nicht dienen.
8. Programmcode ist Sprache und unterliegt dem Recht auf freie Meinungsäußerung.
9. Die Feinde der Kryptographie wären im 15. Jahrhundert die Feinde der Pressefreihet gewesen.

Privatsphäre

Privatsphäre ist...

Privatsphäre

Privatsphäre ist...

- Der Bereich der persönlichen Freiheit

Privatsphäre

Privatsphäre ist...

- Der Bereich der persönlichen Freiheit
- Das Recht, in Ruhe gelassen zu werden

Privatsphäre

Privatsphäre ist...

- Der Bereich der persönlichen Freiheit
- Das Recht, in Ruhe gelassen zu werden
- Persönliche Daten, deren Verbreitung das Individuum kontrolliert

Definition

Ein System muss auch dann sicher sein,
wenn das gesamte System offen liegt,
ausgenommen des Geheimnisses.

— Kerckhoff'sches Prinzip

Sicherheit

Sicherheit

- Keine Sicherheit durch Obskurität

Sicherheit

- Keine Sicherheit durch Obskurität
- Die Software muss einsehbar sein

Sicherheit

- Keine Sicherheit durch Obskurität
- Die Software muss einsehbar sein (nehmt Freie Software!)

Sicherheit

- Keine Sicherheit durch Obskurität
- Die Software muss einsehbar sein (nehmt Freie Software!)
- Öffentliche Infrastruktur nutzbar machen

Web of Trust Vertrauen Öffentlich, privat Schlüssel Metadaten