

Einführung in den angewandten Terrorismus

Lars Beckers

`lars.beckers@rwth-aachen.de`

Fachschaft Mathematik/Physik/Informatik

Cryptoparty, 18. Juni 2015

Was machen wir heute?

Es geht heute um

- ▶ Crypto,
- ▶ Sicherheit,
- ▶ Praxis,
- ▶ coole Dinge
- ▶ und Party.

Was machen wir heute?

Es geht heute um

- ▶ Crypto,
- ▶ Sicherheit,
- ▶ Praxis,
- ▶ coole Dinge
- ▶ und Party.

Was machen wir heute?

Es geht heute um

- ▶ Crypto,
- ▶ Sicherheit,
- ▶ Praxis,
- ▶ coole Dinge
- ▶ und Party.

Was machen wir heute?

Es geht heute um

- ▶ Crypto,
- ▶ Sicherheit,
- ▶ Praxis,
- ▶ coole Dinge
- ▶ und Party.

Was machen wir heute?

Es geht heute um

- ▶ Crypto,
- ▶ Sicherheit,
- ▶ Praxis,
- ▶ coole Dinge
- ▶ und Party.

Und in diesem Vortrag?

- 1 Was machen wir heute?
- 2 Warum Kryptographie verwenden?
 - Diverse Überwacher und Diebe
 - Gegenmaßnahmen
- 3 Asymmetrische Kryptographie
 - Sichereres Browsen
 - Sicherere E-Mails
- 4 Wer ist nun Terrorist?

Kryptographie ist anstrengend

Sichere Software ist nicht benutzerfreundlich.

Kryptographie ist anstrengend

Sichere Software ist nicht benutzerfreundlich.

Phil Zimmermann, Erfinder von PGP, in einem Interview, ob er noch E-Mail verwende:



Kryptographie ist anstrengend

Sichere Software ist nicht benutzerfreundlich.

Phil Zimmermann, Erfinder von PGP, in einem Interview, ob er noch E-Mail verwende:

Ja, aber ich kann sie nicht mehr verschlüsseln, weil ich iPhones und iPads nutze. PGP funktioniert darauf nicht.



Warum also Kryptographie?

Zusätzliche Sicherheit macht es für den Benutzer anstrengender.

Warum also *trotzdem* Kryptographie verwenden?

- ▶ Weil es der Typ von der Cryptoparty gesagt hat?
- ▶ Weil wir es können?
- ▶ Weil es cool ist?

Warum also Kryptographie?

Zusätzliche Sicherheit macht es für den Benutzer anstrengender.

Warum also *trotzdem* Kryptographie verwenden?

- ▶ Weil es der Typ von der Cryptoparty gesagt hat?
- ▶ Weil wir es können?
- ▶ Weil es cool ist?

Warum also Kryptographie?

Zusätzliche Sicherheit macht es für den Benutzer anstrengender.

Warum also *trotzdem* Kryptographie verwenden?

- ▶ Weil es der Typ von der Cryptoparty gesagt hat?
- ▶ Weil wir es können?
- ▶ Weil es cool ist?

Warum also Kryptographie?

Zusätzliche Sicherheit macht es für den Benutzer anstrengender.

Warum also *trotzdem* Kryptographie verwenden?

- ▶ Weil es der Typ von der Cryptoparty gesagt hat?
- ▶ Weil wir es können?
- ▶ Weil es cool ist?

Warum also Kryptographie?

Zusätzliche Sicherheit macht es für den Benutzer anstrengender.

Warum also *trotzdem* Kryptographie verwenden?

- ▶ Weil es der Typ von der Cryptoparty gesagt hat?
- ▶ Weil wir es können?
- ▶ Weil es cool ist?

Und was habe ich schon zu verbergen?

Überwachung durch Staaten

- ▶ Überwachungsskandale NSA, BND, etc.
 - ▶ unkontrollierte Ausspähung
 - ▶ No-Spy-Abkommen
- ▶ Wiedereinführung Vorratsdatenspeicherung
 - ▶ Datensammlung ohne Verbrechen
 - ▶ zur „Terrorprävention“
 - ▶ bereits durch Rechtswidrigkeit gescheitert
- ▶ BKA überwacht(e) Leute, weil sie nach bestimmten Begriffen suchten.
 - ▶ Nur retrospektiv bewertbar.
- ▶ Die Freiheit schützen?

Überwachung durch Staaten

- ▶ Überwachungsskandale NSA, BND, etc.
 - ▶ unkontrollierte Ausspähung
 - ▶ No-Spy-Abkommen
- ▶ Wiedereinführung Vorratsdatenspeicherung
 - ▶ Datensammlung ohne Verbrechen
 - ▶ zur „Terrorprävention“
 - ▶ bereits durch Rechtswidrigkeit gescheitert
- ▶ BKA überwacht(e) Leute, weil sie nach bestimmten Begriffen suchten.
 - ▶ Nur retrospektiv bewertbar.
- ▶ Die Freiheit schützen?

Überwachung durch Staaten

- ▶ Überwachungsskandale NSA, BND, etc.
 - ▶ unkontrollierte Ausspähung
 - ▶ No-Spy-Abkommen
- ▶ Wiedereinführung Vorratsdatenspeicherung
 - ▶ Datensammlung ohne Verbrechen
 - ▶ zur „Terrorprävention“
 - ▶ bereits durch Rechtswidrigkeit gescheitert
- ▶ BKA überwacht(e) Leute, weil sie nach bestimmten Begriffen suchten.
 - ▶ Nur retrospektiv bewertbar.
- ▶ Die Freiheit schützen?

Überwachung durch Staaten

- ▶ Überwachungsskandale NSA, BND, etc.
 - ▶ unkontrollierte Ausspähung
 - ▶ No-Spy-Abkommen
- ▶ Wiedereinführung Vorratsdatenspeicherung
 - ▶ Datensammlung ohne Verbrechen
 - ▶ zur „Terrorprävention“
 - ▶ bereits durch Rechtswidrigkeit gescheitert
- ▶ BKA überwacht(e) Leute, weil sie nach bestimmten Begriffen suchten.
 - ▶ Nur retrospektiv bewertbar.
- ▶ Die Freiheit schützen?

Überwachung durch Firmen

- ▶ mehr Teilnehmer lassen Selbstverständlichkeiten aufkommen
 - ▶ Wer nicht teilnimmt, der ist abnorm.
 - ▶ Wer kein Facebookprofil hat, ist verdächtig. (Terrorist!)
- ▶ „If Google decided to, it could find out[...]“ (Bruce Schneier)
- ▶ staatliche Geheimdienste im Gegensatz zu Firmen
 - ▶ weniger Skandale mit besserer Bedienbarkeit
- ▶ Anreizsysteme vermindern Freiheit
- ▶ Geschäftsmodelle nicht unbedingt offensichtlich

Überwachung durch Firmen

- ▶ mehr Teilnehmer lassen Selbstverständlichkeiten aufkommen
 - ▶ Wer nicht teilnimmt, der ist abnorm.
 - ▶ Wer kein Facebookprofil hat, ist verdächtig. (Terrorist!)
- ▶ „If Google decided to, it could find out[...]“ (Bruce Schneier)
- ▶ staatliche Geheimdienste im Gegensatz zu Firmen
 - ▶ weniger Skandale mit besserer Bedienbarkeit
- ▶ Anreizsysteme vermindern Freiheit
- ▶ Geschäftsmodelle nicht unbedingt offensichtlich

Überwachung durch Firmen

- ▶ mehr Teilnehmer lassen Selbstverständlichkeiten aufkommen
 - ▶ Wer nicht teilnimmt, der ist abnorm.
 - ▶ Wer kein Facebookprofil hat, ist verdächtig. (Terrorist!)
- ▶ „If Google decided to, it could find out[...]“ (Bruce Schneier)
- ▶ staatliche Geheimdienste im Gegensatz zu Firmen
 - ▶ weniger Skandale mit besserer Bedienbarkeit
- ▶ Anreizsysteme vermindern Freiheit
- ▶ Geschäftsmodelle nicht unbedingt offensichtlich

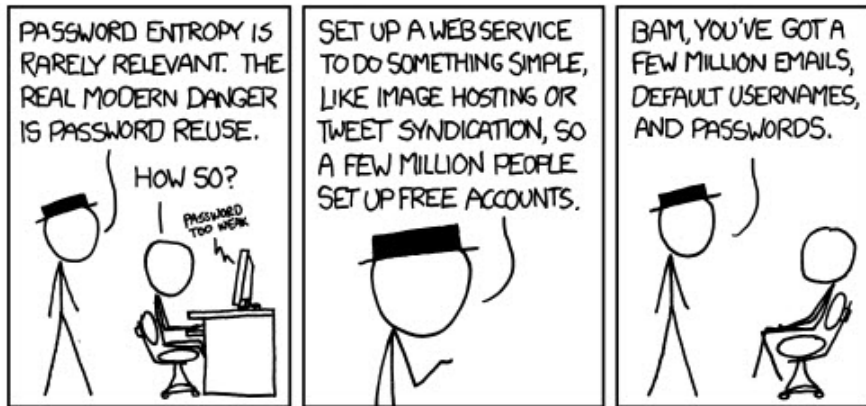
Überwachung durch Firmen

- ▶ mehr Teilnehmer lassen Selbstverständlichkeiten aufkommen
 - ▶ Wer nicht teilnimmt, der ist abnorm.
 - ▶ Wer kein Facebookprofil hat, ist verdächtig. (Terrorist!)
- ▶ „If Google decided to, it could find out[...]“ (Bruce Schneier)
- ▶ staatliche Geheimdienste im Gegensatz zu Firmen
 - ▶ weniger Skandale mit besserer Bedienbarkeit
- ▶ Anreizsysteme vermindern Freiheit
- ▶ Geschäftsmodelle nicht unbedingt offensichtlich

Überwachung durch Firmen

- ▶ mehr Teilnehmer lassen Selbstverständlichkeiten aufkommen
 - ▶ Wer nicht teilnimmt, der ist abnorm.
 - ▶ Wer kein Facebookprofil hat, ist verdächtig. (Terrorist!)
- ▶ „If Google decided to, it could find out[...]“ (Bruce Schneier)
- ▶ staatliche Geheimdienste im Gegensatz zu Firmen
 - ▶ weniger Skandale mit besserer Bedienbarkeit
- ▶ Anreizsysteme vermindern Freiheit
- ▶ Geschäftsmodelle nicht unbedingt offensichtlich

Überwachung durch Firmen



Randall Munroe, xkcd 792, *Password Reuse*

Überwachung durch sich selbst und Umfeld

- ▶ speichern eigener Lebensdaten abseits jeder Notwendigkeit
- ▶ oftmals verbunden mit der Weitergabe an irgendwelche Firmen
- ▶ oft nebenläufige Angaben als unwichtig empfundener Daten
- ▶ Freiwilligkeit durch Freiheitsgefühl effizienter
- ▶ Wer profitiert davon wie?
- ▶ Zur Cryptoparty gehen reicht als Auseinandersetzung, oder?
- ▶ Wie Glaubwürdig ist eine Cryptoparty?

Überwachung durch sich selbst und Umfeld

- ▶ speichern eigener Lebensdaten abseits jeder Notwendigkeit
- ▶ oftmals verbunden mit der Weitergabe an irgendwelche Firmen
- ▶ oft nebenläufige Angaben als unwichtig empfundener Daten
- ▶ Freiwilligkeit durch Freiheitsgefühl effizienter
- ▶ Wer profitiert davon wie?
- ▶ Zur Cryptoparty gehen reicht als Auseinandersetzung, oder?
- ▶ Wie Glaubwürdig ist eine Cryptoparty?

Überwachung durch sich selbst und Umfeld

- ▶ speichern eigener Lebensdaten abseits jeder Notwendigkeit
- ▶ oftmals verbunden mit der Weitergabe an irgendwelche Firmen
- ▶ oft nebenläufige Angaben als unwichtig empfundener Daten
- ▶ Freiwilligkeit durch Freiheitsgefühl effizienter
- ▶ Wer profitiert davon wie?
- ▶ Zur Cryptoparty gehen reicht als Auseinandersetzung, oder?
- ▶ Wie Glaubwürdig ist eine Cryptoparty?

Überwachung durch sich selbst und Umfeld

- ▶ speichern eigener Lebensdaten abseits jeder Notwendigkeit
- ▶ oftmals verbunden mit der Weitergabe an irgendwelche Firmen
- ▶ oft nebenläufige Angaben als unwichtig empfundener Daten
- ▶ Freiwilligkeit durch Freiheitsgefühl effizienter
- ▶ Wer profitiert davon wie?
- ▶ Zur Cryptoparty gehen reicht als Auseinandersetzung, oder?
- ▶ Wie Glaubwürdig ist eine Cryptoparty?

Überwachung durch sich selbst und Umfeld

- ▶ speichern eigener Lebensdaten abseits jeder Notwendigkeit
- ▶ oftmals verbunden mit der Weitergabe an irgendwelche Firmen
- ▶ oft nebenläufige Angaben als unwichtig empfundener Daten
- ▶ Freiwilligkeit durch Freiheitsgefühl effizienter
- ▶ Wer profitiert davon wie?
- ▶ Zur Cryptoparty gehen reicht als Auseinandersetzung, oder?
- ▶ Wie Glaubwürdig ist eine Cryptoparty?

Überwachung durch sich selbst und Umfeld

- ▶ speichern eigener Lebensdaten abseits jeder Notwendigkeit
- ▶ oftmals verbunden mit der Weitergabe an irgendwelche Firmen
- ▶ oft nebenläufige Angaben als unwichtig empfundener Daten
- ▶ Freiwilligkeit durch Freiheitsgefühl effizienter
- ▶ Wer profitiert davon wie?
- ▶ Zur Cryptoparty gehen reicht als Auseinandersetzung, oder?
- ▶ Wie Glaubwürdig ist eine Cryptoparty?

Überwachung durch sich selbst und Umfeld

- ▶ speichern eigener Lebensdaten abseits jeder Notwendigkeit
- ▶ oftmals verbunden mit der Weitergabe an irgendwelche Firmen
- ▶ oft nebenläufige Angaben als unwichtig empfundener Daten
- ▶ Freiwilligkeit durch Freiheitsgefühl effizienter
- ▶ Wer profitiert davon wie?
- ▶ Zur Cryptoparty gehen reicht als Auseinandersetzung, oder?
- ▶ Wie Glaubwürdig ist eine Cryptoparty?

Diebstahl

- ▶ simpelster Fall: Diebstahl
- ▶ Laptops sind handlich
- ▶ selbst stationäre Rechner haben gutes Preis/Gewicht-Verhältnis
- ▶ Account-Diebstahl kann neue Probleme implizieren
- ▶ einfache Passwörter sind schnell geraten
 - ▶ eben durch einen Computer
- ▶ zusammen mit einer Mailadresse sind *alle* Accounts betroffen

Diebstahl

- ▶ simpelster Fall: Diebstahl
- ▶ Laptops sind handlich
- ▶ selbst stationäre Rechner haben gutes Preis/Gewicht-Verhältnis
- ▶ Account-Diebstahl kann neue Probleme implizieren
- ▶ einfache Passwörter sind schnell geraten
 - ▶ eben durch einen Computer
- ▶ zusammen mit einer Mailadresse sind *alle* Accounts betroffen

Diebstahl

- ▶ simpelster Fall: Diebstahl
- ▶ Laptops sind handlich
- ▶ selbst stationäre Rechner haben gutes Preis/Gewicht-Verhältnis
- ▶ Account-Diebstahl kann neue Probleme implizieren
- ▶ einfache Passwörter sind schnell geraten
 - ▶ eben durch einen Computer
- ▶ zusammen mit einer Mailadresse sind *alle* Accounts betroffen

Diebstahl

- ▶ simpelster Fall: Diebstahl
- ▶ Laptops sind handlich
- ▶ selbst stationäre Rechner haben gutes Preis/Gewicht-Verhältnis
- ▶ Account-Diebstahl kann neue Probleme implizieren
- ▶ einfache Passwörter sind schnell geraten
 - ▶ eben durch einen Computer
- ▶ zusammen mit einer Mailadresse sind *alle* Accounts betroffen

Diebstahl

- ▶ simpelster Fall: Diebstahl
- ▶ Laptops sind handlich
- ▶ selbst stationäre Rechner haben gutes Preis/Gewicht-Verhältnis
- ▶ Account-Diebstahl kann neue Probleme implizieren
- ▶ einfache Passwörter sind schnell geraten
 - ▶ eben durch einen Computer
- ▶ zusammen mit einer Mailadresse sind *alle* Accounts betroffen

Diebstahl

- ▶ simpelster Fall: Diebstahl
- ▶ Laptops sind handlich
- ▶ selbst stationäre Rechner haben gutes Preis/Gewicht-Verhältnis
- ▶ Account-Diebstahl kann neue Probleme implizieren
- ▶ einfache Passwörter sind schnell geraten
 - ▶ eben durch einen Computer
- ▶ zusammen mit einer Mailadresse sind *alle* Accounts betroffen

Gegenmaßnahmen

- ▶ Wie ist die aktuelle Norm?
 - ▶ „The longer we wait to make changes, the harder it becomes.“
(Bruce Schneier)
- ▶ Weitermachen wie bisher? Vielleicht mit neuem Bewusstsein?
 - ▶ Das reicht nicht!
 - ▶ Nur tatsächliche Änderung hilft.
- ▶ Aller Anfang ist schwer – heute wird dabei geholfen!
- ▶ gleich: Workshop zu Passwortmanagern für bessere Passwörter
- ▶ gleich: Workshop zu Festplattenkrypto für sichere Daten

Gegenmaßnahmen

- ▶ Wie ist die aktuelle Norm?
 - ▶ „The longer we wait to make changes, the harder it becomes.“
(Bruce Schneier)
- ▶ Weitermachen wie bisher? Vielleicht mit neuem Bewusstsein?
 - ▶ Das reicht nicht!
 - ▶ Nur tatsächliche Änderung hilft.
- ▶ Aller Anfang ist schwer – heute wird dabei geholfen!
- ▶ gleich: Workshop zu Passwortmanagern für bessere Passwörter
- ▶ gleich: Workshop zu Festplattenkrypto für sichere Daten

Gegenmaßnahmen

- ▶ Wie ist die aktuelle Norm?
 - ▶ „The longer we wait to make changes, the harder it becomes.“
(Bruce Schneier)
- ▶ Weitermachen wie bisher? Vielleicht mit neuem Bewusstsein?
 - ▶ Das reicht nicht!
 - ▶ Nur tatsächliche Änderung hilft.
- ▶ Aller Anfang ist schwer – heute wird dabei geholfen!
- ▶ gleich: Workshop zu Passwortmanagern für bessere Passwörter
- ▶ gleich: Workshop zu Festplattenkrypto für sichere Daten

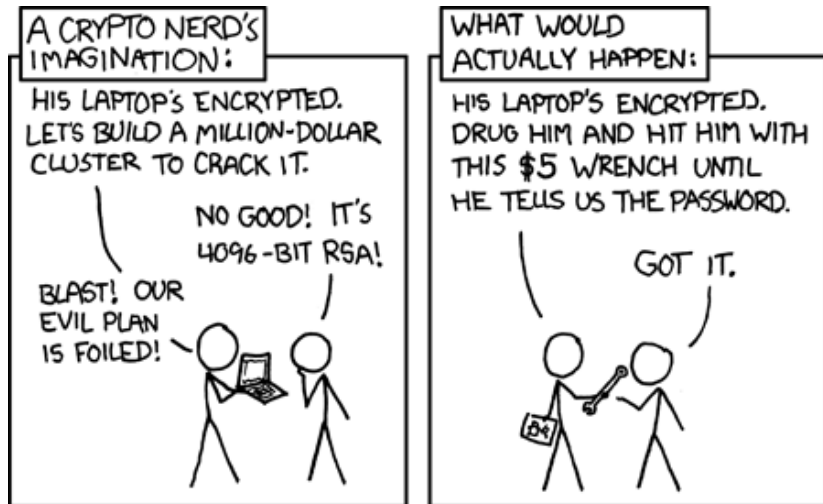
Gegenmaßnahmen

- ▶ Wie ist die aktuelle Norm?
 - ▶ „The longer we wait to make changes, the harder it becomes.“
(Bruce Schneier)
- ▶ Weitermachen wie bisher? Vielleicht mit neuem Bewusstsein?
 - ▶ Das reicht nicht!
 - ▶ Nur tatsächliche Änderung hilft.
- ▶ Aller Anfang ist schwer – heute wird dabei geholfen!
- ▶ gleich: Workshop zu Passwortmanagern für bessere Passwörter
- ▶ gleich: Workshop zu Festplattenkrypto für sichere Daten

Gegenmaßnahmen

- ▶ Wie ist die aktuelle Norm?
 - ▶ „The longer we wait to make changes, the harder it becomes.“
(Bruce Schneier)
- ▶ Weitermachen wie bisher? Vielleicht mit neuem Bewusstsein?
 - ▶ Das reicht nicht!
 - ▶ Nur tatsächliche Änderung hilft.
- ▶ Aller Anfang ist schwer – heute wird dabei geholfen!
- ▶ gleich: Workshop zu Passwortmanagern für bessere Passwörter
- ▶ gleich: Workshop zu Festplattenkrypto für sichere Daten

Gegenmaßnahmen – gegen was?



Randall Munroe, xkcd 538, *Security*

Asymmetrische Kryptographie

- ▶ bei *symmetrischer Kryptographie* muss jeder den Schlüssel kennen
 - ▶ oftmals ungeeignet
 - ▶ Schlüssel wie übertragen?
 - ▶ Ist jeder vertrauenswürdig?
- ▶ asymmetrische Kryptographie ist ähnlich zu einem Briefkasten
- ▶ Verschlüsselung mit einem *öffentlichen Schlüssel*
 - ▶ daher oft als *Public-Key-Cryptography* bezeichnet
 - ▶ hier: Einwurfsschlit
- ▶ Kommunikation über einen unsicheren Kanal
 - ▶ normalerweise: Internet
 - ▶ hier: Rik
- ▶ Entschlüsselung mit einem *privaten Schlüssel*

Asymmetrische Kryptographie

- ▶ bei *symmetrischer Kryptographie* muss jeder den Schlüssel kennen
 - ▶ oftmals ungeeignet
 - ▶ Schlüssel wie übertragen?
 - ▶ Ist jeder vertrauenswürdig?
- ▶ asymmetrische Kryptographie ist ähnlich zu einem Briefkasten
- ▶ Verschlüsselung mit einem *öffentlichen Schlüssel*
 - ▶ daher oft als *Public-Key-Cryptography* bezeichnet
 - ▶ hier: Einwurfsschlitze
- ▶ Kommunikation über einen unsicheren Kanal
 - ▶ normalerweise: Internet
 - ▶ hier: Rikis
- ▶ Entschlüsselung mit einem *privaten Schlüssel*

Asymmetrische Kryptographie

- ▶ bei *symmetrischer Kryptographie* muss jeder den Schlüssel kennen
 - ▶ oftmals ungeeignet
 - ▶ Schlüssel wie übertragen?
 - ▶ Ist jeder vertrauenswürdig?
- ▶ asymmetrische Kryptographie ist ähnlich zu einem Briefkasten
- ▶ Verschlüsselung mit einem *öffentlichen Schlüssel*
 - ▶ daher oft als *Public-Key-Cryptography* bezeichnet
 - ▶ hier: Einwurfsschlitze
- ▶ Kommunikation über einen unsicheren Kanal
 - ▶ normalerweise: Internet
 - ▶ hier: Rikis
- ▶ Entschlüsselung mit einem *privaten Schlüssel*

Asymmetrische Kryptographie

- ▶ bei *symmetrischer Kryptographie* muss jeder den Schlüssel kennen
 - ▶ oftmals ungeeignet
 - ▶ Schlüssel wie übertragen?
 - ▶ Ist jeder vertrauenswürdig?
- ▶ asymmetrische Kryptographie ist ähnlich zu einem Briefkasten
- ▶ Verschlüsselung mit einem *öffentlichen Schlüssel*
 - ▶ daher oft als *Public-Key-Cryptography* bezeichnet
 - ▶ hier: Einwurfsschlitze
- ▶ Kommunikation über einen unsicheren Kanal
 - ▶ normalerweise: Internet
 - ▶ hier: Rikuz
- ▶ Entschlüsselung mit einem *privaten Schlüssel*

Asymmetrische Kryptographie

- ▶ bei *symmetrischer Kryptographie* muss jeder den Schlüssel kennen
 - ▶ oftmals ungeeignet
 - ▶ Schlüssel wie übertragen?
 - ▶ Ist jeder vertrauenswürdig?
- ▶ asymmetrische Kryptographie ist ähnlich zu einem Briefkasten
- ▶ Verschlüsselung mit einem *öffentlichen Schlüssel*
 - ▶ daher oft als *Public-Key-Cryptography* bezeichnet
 - ▶ hier: Einwurfsschlitze
- ▶ Kommunikation über einen unsicheren Kanal
 - ▶ normalerweise: Internet
 - ▶ hier: Rikis
- ▶ Entschlüsselung mit einem *privaten Schlüssel*

Asymmetrische Kryptographie

▶ Sicherheit

- ▶ Schwierigkeit ein mathematisches Problem effizient zu berechnen
- ▶ normalerweise: Schlüssellänge
- ▶ hier: Bauart des Briefkastens

▶ Aber den öffentlichen Schlüssel kennt jeder!

- ▶ Mit wem kommuniziere ich?

▶ Lösung: Digitale Signaturen

- ▶ mit dem *eigenen* privaten Schlüssel signieren
- ▶ über den öffentlichen Schlüssel prüfbar
- ▶ hier: Versiegelung des Briefes

▶ Gelöste Probleme:

- ▶ Vertraulichkeit durch Verschlüsselung
- ▶ Authentizität durch Signaturen

Asymmetrische Kryptographie

- ▶ Sicherheit
 - ▶ Schwierigkeit ein mathematisches Problem effizient zu berechnen
 - ▶ normalerweise: Schlüssellänge
 - ▶ hier: Bauart des Briefkastens
- ▶ Aber den öffentlichen Schlüssel kennt jeder!
 - ▶ Mit wem kommuniziere ich?
- ▶ Lösung: Digitale Signaturen
 - ▶ mit dem *eigenen* privaten Schlüssel signieren
 - ▶ über den öffentlichen Schlüssel prüfbar
 - ▶ hier: Versiegelung des Briefes
- ▶ Gelöste Probleme:
 - ▶ Vertraulichkeit durch Verschlüsselung
 - ▶ Authentizität durch Signaturen

Asymmetrische Kryptographie

- ▶ Sicherheit
 - ▶ Schwierigkeit ein mathematisches Problem effizient zu berechnen
 - ▶ normalerweise: Schlüssellänge
 - ▶ hier: Bauart des Briefkastens
- ▶ Aber den öffentlichen Schlüssel kennt jeder!
 - ▶ Mit wem kommuniziere ich?
- ▶ Lösung: Digitale Signaturen
 - ▶ mit dem *eigenen* privaten Schlüssel signieren
 - ▶ über den öffentlichen Schlüssel prüfbar
 - ▶ hier: Versiegelung des Briefes
- ▶ Gelöste Probleme:
 - ▶ Vertraulichkeit durch Verschlüsselung
 - ▶ Authentizität durch Signaturen

Asymmetrische Kryptographie

- ▶ Sicherheit
 - ▶ Schwierigkeit ein mathematisches Problem effizient zu berechnen
 - ▶ normalerweise: Schlüssellänge
 - ▶ hier: Bauart des Briefkastens
- ▶ Aber den öffentlichen Schlüssel kennt jeder!
 - ▶ Mit wem kommuniziere ich?
- ▶ Lösung: Digitale Signaturen
 - ▶ mit dem *eigenen* privaten Schlüssel signieren
 - ▶ über den öffentlichen Schlüssel prüfbar
 - ▶ hier: Versiegelung des Briefes
- ▶ Gelöste Probleme:
 - ▶ Vertraulichkeit durch Verschlüsselung
 - ▶ Authentizität durch Signaturen

Asymmetrische Kryptographie

- ▶ Bleibt das so?
 - ▶ privater Schlüssel muss geheim bleiben
 - ▶ privaten Schlüssel mit einem Passwort schützen
 - ▶ Signaturen müssen geprüft werden
- ▶ Welcher Schlüssel gehört zu wem?
 - ▶ direktes Vertrauen
 - ▶ Zertifizierungsstelle
 - ▶ Web of Trust
- ▶ Und was macht man nun damit?
 - ▶ Sicherer Browsen
 - ▶ Sicherere E-Mails
 - ▶ ...

Asymmetrische Kryptographie

- ▶ Bleibt das so?
 - ▶ privater Schlüssel muss geheim bleiben
 - ▶ privaten Schlüssel mit einem Passwort schützen
 - ▶ Signaturen müssen geprüft werden
- ▶ Welcher Schlüssel gehört zu wem?
 - ▶ direktes Vertrauen
 - ▶ Zertifizierungsstelle
 - ▶ Web of Trust
- ▶ Und was macht man nun damit?
 - ▶ Sicherer Browsen
 - ▶ Sicherere E-Mails
 - ▶ ...

Asymmetrische Kryptographie

- ▶ Bleibt das so?
 - ▶ privater Schlüssel muss geheim bleiben
 - ▶ privaten Schlüssel mit einem Passwort schützen
 - ▶ Signaturen müssen geprüft werden
- ▶ Welcher Schlüssel gehört zu wem?
 - ▶ direktes Vertrauen
 - ▶ Zertifizierungsstelle
 - ▶ Web of Trust
- ▶ Und was macht man nun damit?
 - ▶ Sicherer Browsen
 - ▶ Sicherere E-Mails
 - ▶ ...

Sichereres Browsen

- ▶ Umsetzung im Web durch HTTPS
 - ▶ Sicherung über *asymmetrische* Kryptographie
 - ▶ Datenübertragung über *symmetrische* Kryptographie
 - ▶ Verschlüsselte Übertragung
 - ▶ Authentizität des Anbieters
- ▶ Problematiken:
 - ▶ mehrfache Revisionen des Protokolls und der Software
 - ▶ Vertrauen des Browserherstellers, nicht des Users
 - ▶ zentrale Zertifizierungsstellen
z.B. RWTH Aachen, CNNIC, VeriSign, DTAG, Google, VISA, ...
 - ▶ Zertifikate sind nicht fest, sondern beliebig
- ▶ Weitere Probleme: Tracking, Clouds, Phishing, ...
- ▶ gleich: Workshop mit mehr Details und Hilfen

Sichereres Browsen

- ▶ Umsetzung im Web durch HTTPS
 - ▶ Sicherung über *asymmetrische* Kryptographie
 - ▶ Datenübertragung über *symmetrische* Kryptographie
 - ▶ Verschlüsselte Übertragung
 - ▶ Authentizität des Anbieters
- ▶ Problematiken:
 - ▶ mehrfache Revisionen des Protokolls und der Software
 - ▶ Vertrauen des Browserherstellers, nicht des Users
 - ▶ zentrale Zertifizierungsstellen
z.B. RWTH Aachen, CNNIC, VeriSign, DTAG, Google, VISA, ...
 - ▶ Zertifikate sind nicht fest, sondern beliebig
- ▶ Weitere Probleme: Tracking, Clouds, Phishing, ...
- ▶ gleich: Workshop mit mehr Details und Hilfen

Sichereres Browsen

- ▶ Umsetzung im Web durch HTTPS
 - ▶ Sicherung über *asymmetrische* Kryptographie
 - ▶ Datenübertragung über *symmetrische* Kryptographie
 - ▶ Verschlüsselte Übertragung
 - ▶ Authentizität des Anbieters
- ▶ Problematiken:
 - ▶ mehrfache Revisionen des Protokolls und der Software
 - ▶ Vertrauen des Browserherstellers, nicht des Users
 - ▶ zentrale Zertifizierungsstellen
z.B. RWTH Aachen, CNNIC, VeriSign, DTAG, Google, VISA, ...
 - ▶ Zertifikate sind nicht fest, sondern beliebig
- ▶ Weitere Probleme: Tracking, Clouds, Phishing, ...
- ▶ gleich: Workshop mit mehr Details und Hilfen

Sichereres Browsen

- ▶ Umsetzung im Web durch HTTPS
 - ▶ Sicherung über *asymmetrische* Kryptographie
 - ▶ Datenübertragung über *symmetrische* Kryptographie
 - ▶ Verschlüsselte Übertragung
 - ▶ Authentizität des Anbieters
- ▶ Problematiken:
 - ▶ mehrfache Revisionen des Protokolls und der Software
 - ▶ Vertrauen des Browserherstellers, nicht des Users
 - ▶ zentrale Zertifizierungsstellen
z.B. RWTH Aachen, CNNIC, VeriSign, DTAG, Google, VISA, ...
 - ▶ Zertifikate sind nicht fest, sondern beliebig
- ▶ Weitere Probleme: Tracking, Clouds, Phishing, ...
- ▶ gleich: Workshop mit mehr Details und Hilfen

Mails verschlüsseln

- ▶ Umsetzung für Mails durch PGP und S/MIME
- ▶ S/MIME mit gleichen Zertifikatsproblemen wie HTTPS
- ▶ GPG als offene Implementation von PGP.
- ▶ Prüfung von Signaturen mittels *Web of Trust*
- ▶ zur Nutzung oft Addons im Mailprogramm nötig
- ▶ gleich: Workshop zur Hilfe bei Einrichtung und Nutzung

Mails verschlüsseln

- ▶ Umsetzung für Mails durch PGP und S/MIME
- ▶ S/MIME mit gleichen Zertifikatsproblemen wie HTTPS
- ▶ GPG als offene Implementation von PGP.
- ▶ Prüfung von Signaturen mittels *Web of Trust*
- ▶ zur Nutzung oft Addons im Mailprogramm nötig
- ▶ gleich: Workshop zur Hilfe bei Einrichtung und Nutzung

Mails verschlüsseln

- ▶ Umsetzung für Mails durch PGP und S/MIME
- ▶ S/MIME mit gleichen Zertifikatsproblemen wie HTTPS
- ▶ GPG als offene Implementation von PGP.
- ▶ Prüfung von Signaturen mittels *Web of Trust*
- ▶ zur Nutzung oft Addons im Mailprogramm nötig
- ▶ gleich: Workshop zur Hilfe bei Einrichtung und Nutzung

Mails verschlüsseln

- ▶ Umsetzung für Mails durch PGP und S/MIME
- ▶ S/MIME mit gleichen Zertifikatsproblemen wie HTTPS
- ▶ GPG als offene Implementation von PGP.
- ▶ Prüfung von Signaturen mittels *Web of Trust*
- ▶ zur Nutzung oft Addons im Mailprogramm nötig
- ▶ gleich: Workshop zur Hilfe bei Einrichtung und Nutzung

Mails verschlüsseln

- ▶ Umsetzung für Mails durch PGP und S/MIME
- ▶ S/MIME mit gleichen Zertifikatsproblemen wie HTTPS
- ▶ GPG als offene Implementation von PGP.
- ▶ Prüfung von Signaturen mittels *Web of Trust*
- ▶ zur Nutzung oft Addons im Mailprogramm nötig
- ▶ gleich: Workshop zur Hilfe bei Einrichtung und Nutzung

Mails verschlüsseln

- ▶ Umsetzung für Mails durch PGP und S/MIME
- ▶ S/MIME mit gleichen Zertifikatsproblemen wie HTTPS
- ▶ GPG als offene Implementation von PGP.
- ▶ Prüfung von Signaturen mittels *Web of Trust*
- ▶ zur Nutzung oft Addons im Mailprogramm nötig
- ▶ gleich: Workshop zur Hilfe bei Einrichtung und Nutzung

PGP Keysigning

- ▶ **keine** zentrale Zertifizierungsstelle
- ▶ gegenseitiges Signieren von Schlüsseln
- ▶ Ziel: möglichst viele Pfade im Web of Trust
- ▶ Feststellung der Zugehörigkeit von Schlüssel zu Inhaber
 - ▶ persönliches Treffen
 - ▶ Bestätigung über Ausweisdokumente
- ▶ Austausch über *Keyserver*
 - ▶ andere können die neuen Signaturen nutzen
- ▶ „Facebook des Vertrauens“
- ▶ gleich: mehrfaches Keysigning nach Ankündigung

PGP Keysigning

- ▶ **keine** zentrale Zertifizierungsstelle
- ▶ gegenseitiges Signieren von Schlüsseln
- ▶ Ziel: möglichst viele Pfade im Web of Trust
- ▶ Feststellung der Zugehörigkeit von Schlüssel zu Inhaber
 - ▶ persönliches Treffen
 - ▶ Bestätigung über Ausweisdokumente
- ▶ Austausch über *Keyserver*
 - ▶ andere können die neuen Signaturen nutzen
- ▶ „Facebook des Vertrauens“
- ▶ gleich: mehrfaches Keysigning nach Ankündigung

PGP Keysigning

- ▶ **keine** zentrale Zertifizierungsstelle
- ▶ gegenseitiges Signieren von Schlüsseln
- ▶ Ziel: möglichst viele Pfade im Web of Trust
- ▶ Feststellung der Zugehörigkeit von Schlüssel zu Inhaber
 - ▶ persönliches Treffen
 - ▶ Bestätigung über Ausweisdokumente
- ▶ Austausch über *Keyserver*
 - ▶ andere können die neuen Signaturen nutzen
- ▶ „Facebook des Vertrauens“
- ▶ gleich: mehrfaches Keysigning nach Ankündigung

PGP Keysigning

- ▶ **keine** zentrale Zertifizierungsstelle
- ▶ gegenseitiges Signieren von Schlüsseln
- ▶ Ziel: möglichst viele Pfade im Web of Trust
- ▶ Feststellung der Zugehörigkeit von Schlüssel zu Inhaber
 - ▶ persönliches Treffen
 - ▶ Bestätigung über Ausweisdokumente
- ▶ Austausch über *Keyserver*
 - ▶ andere können die neuen Signaturen nutzen
- ▶ „Facebook des Vertrauens“
- ▶ gleich: mehrfaches Keysigning nach Ankündigung

PGP Keysigning

- ▶ **keine** zentrale Zertifizierungsstelle
- ▶ gegenseitiges Signieren von Schlüsseln
- ▶ Ziel: möglichst viele Pfade im Web of Trust
- ▶ Feststellung der Zugehörigkeit von Schlüssel zu Inhaber
 - ▶ persönliches Treffen
 - ▶ Bestätigung über Ausweisdokumente
- ▶ Austausch über *Keyserver*
 - ▶ andere können die neuen Signaturen nutzen
- ▶ „Facebook des Vertrauens“
- ▶ gleich: mehrfaches Keysigning nach Ankündigung

PGP Keysigning

- ▶ **keine** zentrale Zertifizierungsstelle
- ▶ gegenseitiges Signieren von Schlüsseln
- ▶ Ziel: möglichst viele Pfade im Web of Trust
- ▶ Feststellung der Zugehörigkeit von Schlüssel zu Inhaber
 - ▶ persönliches Treffen
 - ▶ Bestätigung über Ausweisdokumente
- ▶ Austausch über *Keyserver*
 - ▶ andere können die neuen Signaturen nutzen
- ▶ „Facebook des Vertrauens“
- ▶ gleich: mehrfaches Keysigning nach Ankündigung

PGP Keysigning

- ▶ **keine** zentrale Zertifizierungsstelle
- ▶ gegenseitiges Signieren von Schlüsseln
- ▶ Ziel: möglichst viele Pfade im Web of Trust
- ▶ Feststellung der Zugehörigkeit von Schlüssel zu Inhaber
 - ▶ persönliches Treffen
 - ▶ Bestätigung über Ausweisdokumente
- ▶ Austausch über *Keyserver*
 - ▶ andere können die neuen Signaturen nutzen
- ▶ „Facebook des Vertrauens“
- ▶ gleich: mehrfaches Keysigning nach Ankündigung

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Wer ist nun Terrorist?

- ▶ Decken sichere Briefkästen den Terrorismus?
- ▶ Können Webbrowser und Mailprogramme Terrorismus fördern?
- ▶ Ist Phil Zimmermann ein Terrorist?
- ▶ Ist Bruce Schneier ein Terrorist?
- ▶ Bin ich ein Terrorist?
- ▶ Wollt ihr Terroristen werden?
- ▶ Habt ihr etwas zu verbergen? Vor einem Dieb, dem Staat, Firmen oder ...?
- ▶ Haben andere etwas zu verbergen?
- ▶ Möchtet ihr Kryptographie verwenden? Oder reicht so ein Vortrag aus?

Ende

Danke für eure Aufmerksamkeit!
Habt ihr noch Fragen?