Digitale Selbstverteidigung

Verschlüsselte Kommunikation für Politgruppen

Conundrum und Rote Hilfe

15. Januar 2013

Gliederung

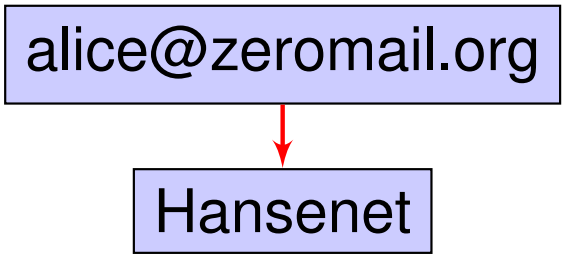
Grundlagen

- Emails werden unverschlüsselt übertragen
- Analogie: Postkarte
- Unterschied zur Postkarte:
  - Mehr Leute haben Zugriff
  - Digital -> leichter auswertbar
- 2010 sind in Dtl. 37 Mio. E-Mails in Schlüsselwörter-Filtern hängen geblieben und überprüft: http://bit.ly/xVgXNf

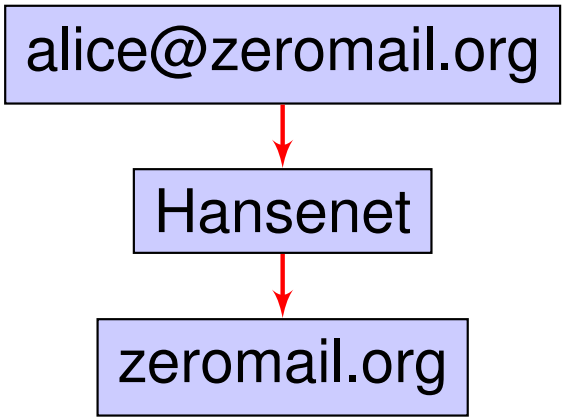
Schema

alice@zeromail.org

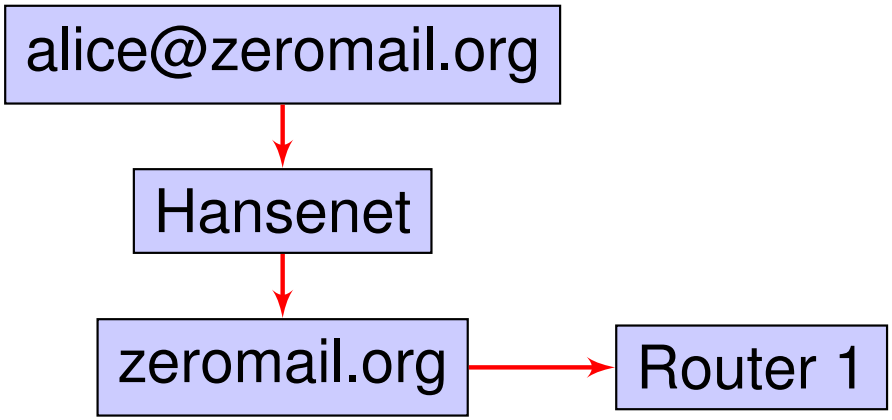
Schema



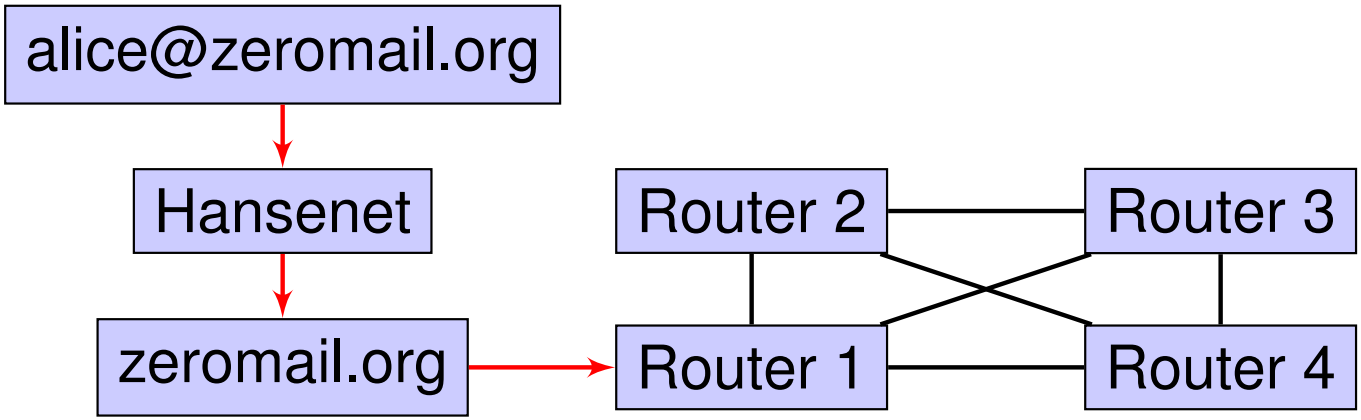
Schema



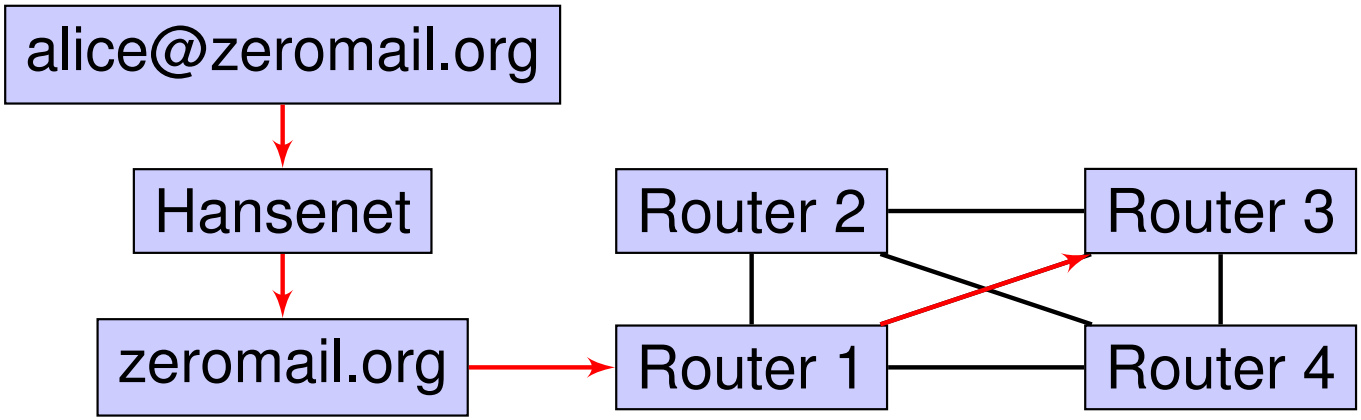
Schema



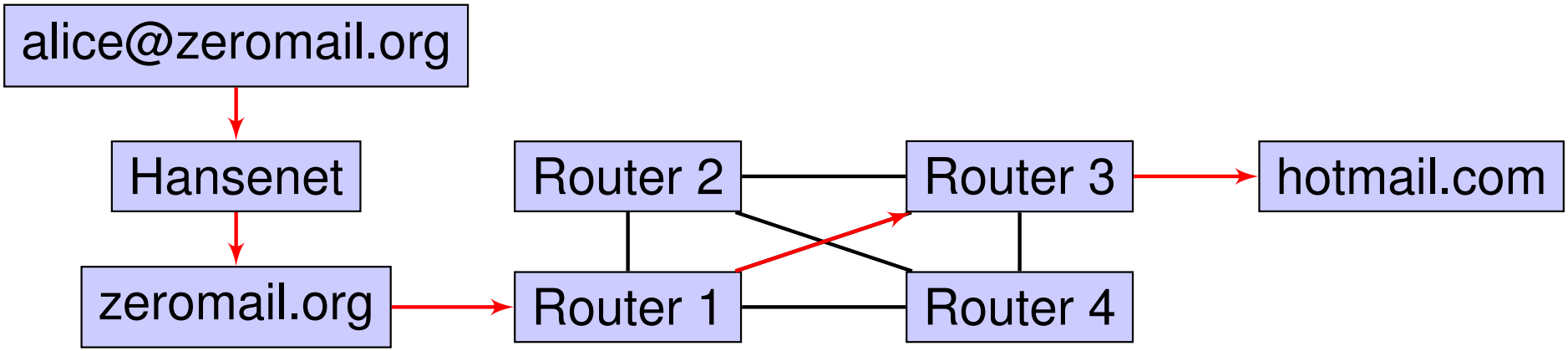
Schema


alice@zeromail.org
Hansenet
zeromail.org
Router 2
Router 3
Router 1
Router 4

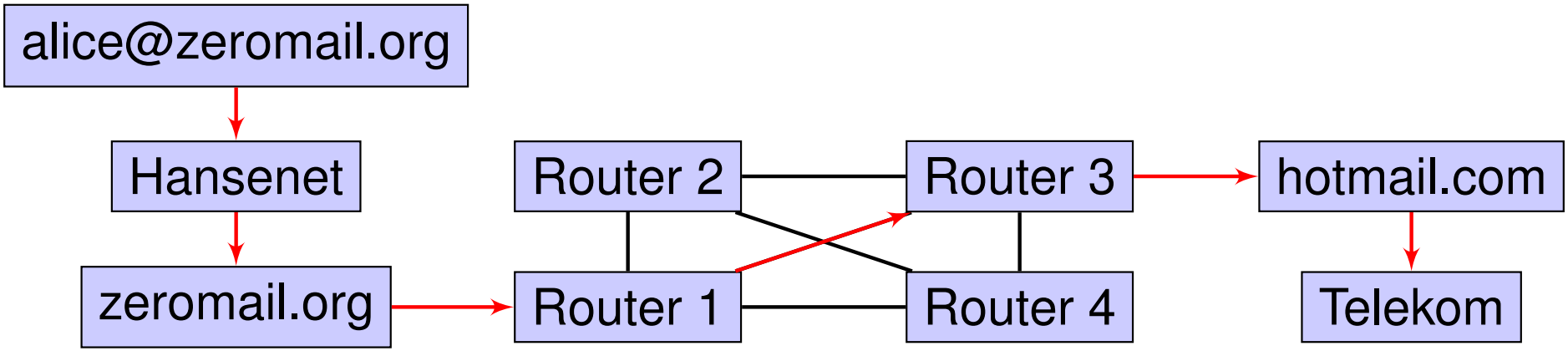
Schema


alice@zeromail.org
Hansenet
zeromail.org
Router 2
Router 3
Router 1
Router 4

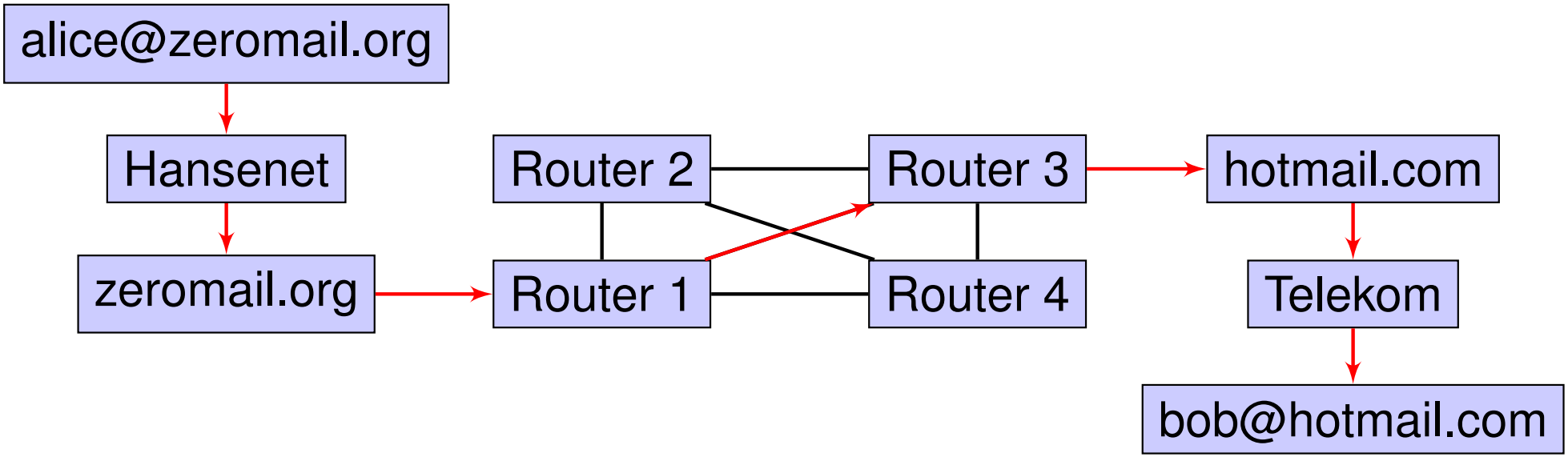
Schema


alice@zeromail.org
Hansenet
zeromail.org
Router 2
Router 1
Router 3
Router 4
hotmail.com

Schema


alice@zeromail.org
Hansenet
zeromail.org
Router 2
Router 1
Router 3
Router 4
hotmail.com
Telekom

Schema


alice@zeromail.org
Hansenet
zeromail.org
Router 2
Router 3
Router 1
Router 4
hotmail.com
Telekom
bob@hotmail.com

Deshalb verschlüsseln

- Der Weg einer Email ist nicht vorhersehbar
- Damit auch nicht der Kreis der Leute, die darauf Zugriff haben

Unverschlüsselte, reine Text EMail

```
Delivered-To: an@email.org
Received: (qmail 898); 19 Mar 2012 16:51:30 -0000
Received: from mail.email.org (HELO mail.email.org)
Message-ID: <76412.3060700@email.org>
Date: Mon, 19 Mar 2012 17:51:30 +0100
From: Von <von@email.org>
User-Agent: Mozilla
MIME-Version: 1.0
To: an@email.org
Subject: Test 1
Content-Type: text/plain; charset=ISO-8859-1

Beispielhafter EMail Inhalt
```

Verschlüsselte EMail

```
Return-Path: <von@email.org>
Delivered-To: an@email.org
Date: Mon, 19 Mar 2012 17:47:51 +0100
From: Von <von@email.org>
MIME-Version: 1.0
To: an@email.org
Subject: Test 2
X-Enigmail-Version: 1.3.5
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit

—–BEGIN PGP MESSAGE—–
Charset: ISO-8859-1
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQEMA4trrNTUNtDZAQf9EZW2LyWGoUXA0/Lszw8q5RD9JU0EUxNtia2PCV3q+Ksv
EwgNrt7Erzq1JV2SR4Zl7LuktqducaNlr6lsxf0kf9b9AKi43UzmMWpzvdalceLU
...
WAKzcQi26oDt+0F44Sghhd0mj7rQlwVJz4pMC1xSFy+vx+1o7E20cx5pIEKe4yY+
msixDenxCABEAph8L5CwX4Oayg==
=Obki
—–END PGP MESSAGE—–
```

Klassische (Symmetrische) Verschlüsselung

Wie funktioniert 'klassische' Verschlüsselung - Alice schickt Bob eine Nachricht ...

- Verschlüsselungsverfahren und Schlüssel
- Beispiel Caesar-Verschlüsselung
- Alice und Bob teilen einen geheimen Schlüssel
- Problem Schlüsselverwaltung
  - Wie verteile ich Schlüssel?
  - Wie widerrufe ich einen Schlüssel?

Klassische (Symmetrische) Verschlüsselung

Wie funktioniert 'klassische' Verschlüsselung - Alice schickt Bob eine Nachricht ...

- Verschlüsselungsverfahren und Schlüssel
- Beispiel Caesar-Verschlüsselung
- Alice und Bob teilen einen geheimen Schlüssel
- Problem Schlüsselverwaltung
  - Wie verteile ich Schlüssel?
  - Wie widerrufe ich einen Schlüssel?

Klassische (Symmetrische) Verschlüsselung

Wie funktioniert 'klassische' Verschlüsselung - Alice schickt Bob eine Nachricht ...

- Verschlüsselungsverfahren und Schlüssel
- Beispiel Caesar-Verschlüsselung
- Alice und Bob teilen einen geheimen Schlüssel
- Problem Schlüsselverwaltung
  - Wie verteile ich Schlüssel?
  - Wie widerrufe ich einen Schlüssel?

Klassische (Symmetrische) Verschlüsselung

Wie funktioniert 'klassische' Verschlüsselung - Alice schickt Bob eine Nachricht ...

- Verschlüsselungsverfahren und Schlüssel
- Beispiel Caesar-Verschlüsselung
- Alice und Bob teilen einen geheimen Schlüssel
- Problem Schlüsselverwaltung
  - Wie verteile ich Schlüssel?
  - Wie widerrufe ich einen Schlüssel?

Klassische (Symmetrische) Verschlüsselung

Wie funktioniert 'klassische' Verschlüsselung - Alice schickt Bob eine Nachricht ...

- Verschlüsselungsverfahren und Schlüssel
- Beispiel Caesar-Verschlüsselung
- Alice und Bob teilen einen geheimen Schlüssel
- Problem Schlüsselverwaltung
  - Wie verteile ich Schlüssel?
  - Wie widerrufe ich einen Schlüssel?

Klassische (Symmetrische) Verschlüsselung

Wie funktioniert 'klassische' Verschlüsselung - Alice schickt Bob eine Nachricht ...

- Verschlüsselungsverfahren und Schlüssel
- Beispiel Caesar-Verschlüsselung
- Alice und Bob teilen einen geheimen Schlüssel
- Problem Schlüsselverwaltung
  - Wie verteile ich Schlüssel?
  - Wie widerrufe ich einen Schlüssel?

Asymmetrische Verschlüsselung

- Es gibt jetzt 2 Schlüssel!
- Öffentliche und private Schlüssel (public key Verfahren)
- Öffentlicher Schlüssel verschlüsselt
- Privater Schlüssel entschlüsselt
- Löst das Schlüsselverteilproblem

Asymmetrische Verschlüsselung

- Es gibt jetzt 2 Schlüssel!
- Öffentliche und private Schlüssel (public key Verfahren)
- Öffentlicher Schlüssel verschlüsselt
- Privater Schlüssel entschlüsselt
- Löst das Schlüsselverteilproblem

Asymmetrische Verschlüsselung

- Es gibt jetzt 2 Schlüssel!
- Öffentliche und private Schlüssel (public key Verfahren)
- Öffentlicher Schlüssel verschlüsselt
- Privater Schlüssel entschlüsselt
- Löst das Schlüsselverteilproblem

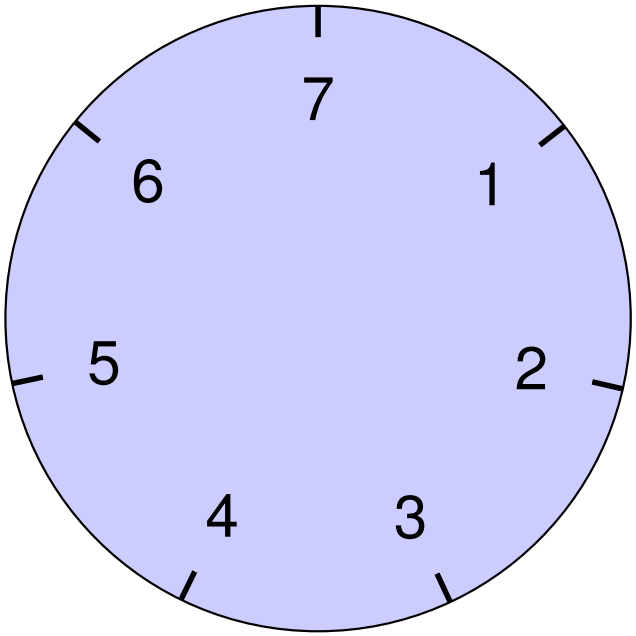
Asymmetrische Verschlüsselung

- Es gibt jetzt 2 Schlüssel!
- Öffentliche und private Schlüssel (public key Verfahren)
- Öffentlicher Schlüssel verschlüsselt
- Privater Schlüssel entschlüsselt
- Löst das Schlüsselverteilproblem

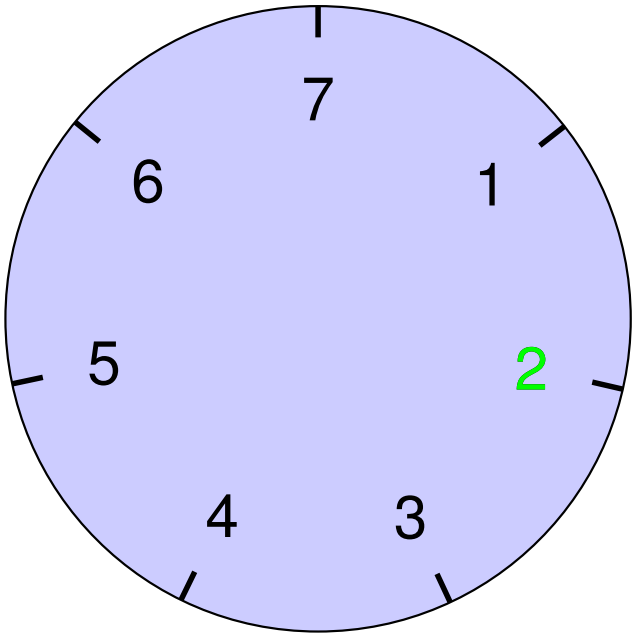
Asymmetrische Verschlüsselung

- Es gibt jetzt 2 Schlüssel!
- Öffentliche und private Schlüssel (public key Verfahren)
- Öffentlicher Schlüssel verschlüsselt
- Privater Schlüssel entschlüsselt
- Löst das Schlüsselverteilproblem

Ein Beispiel - Die Uhr

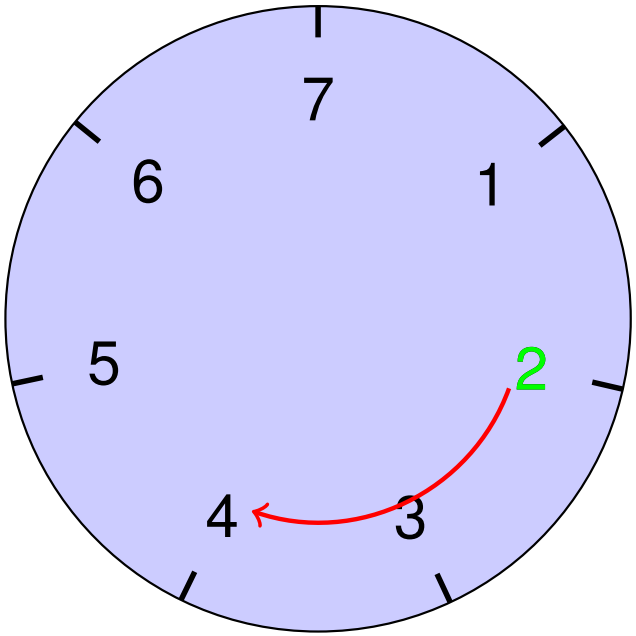


Ein Beispiel - Die Uhr



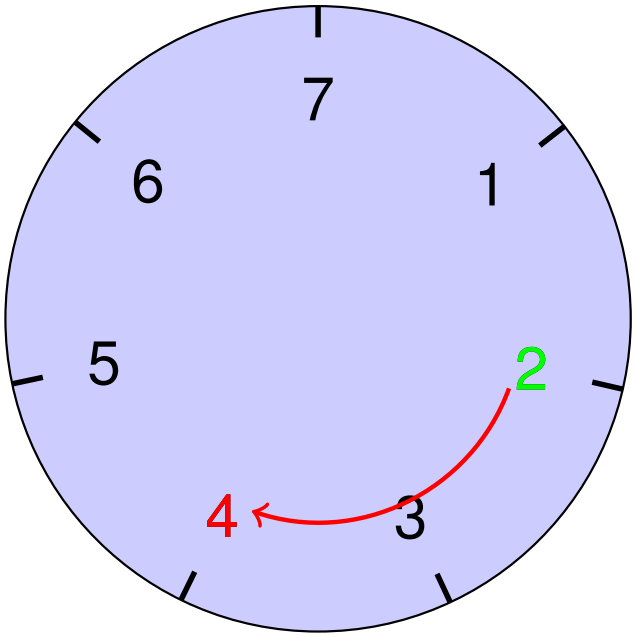
Verschlüsselung

Ein Beispiel - Die Uhr



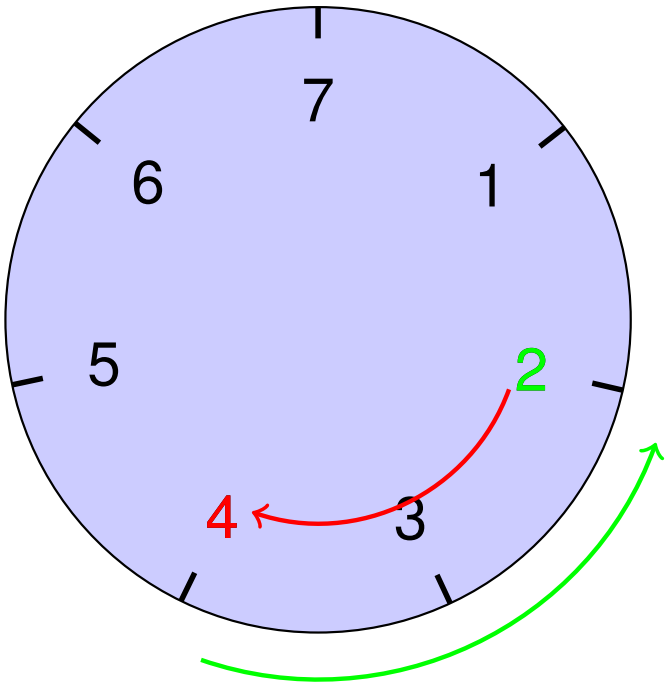
Verschlüsselung
Schlüssel: 2 Stunden plus

Ein Beispiel - Die Uhr



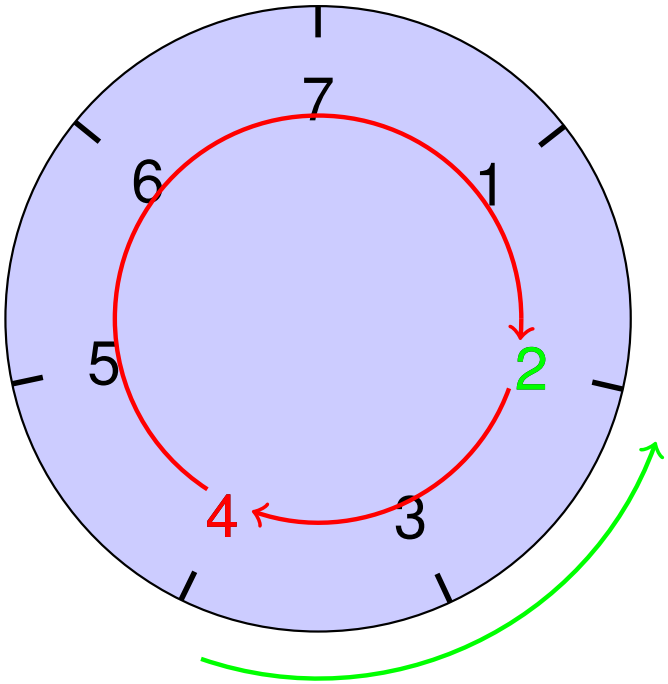
Verschlüsselung
Schlüssel: 2 Stunden plus

Ein Beispiel - Die Uhr



Verschlüsselung
Schlüssel: 2 Stunden plus
Entschlüsselung
Schlüssel: 2 Stunden minus

Ein Beispiel - Die Uhr



Verschlüsselung
Schlüssel: 2 Stunden plus
Entschlüsselung
Schlüssel: 2 Stunden minus
Schlüssel: 5 Stunden plus

Schlüssellänge

Die Länge/Größe des Schlüssels (in Bit) bestimmt

- Die Größe der verwendeten Zahlen
- und damit den Rechenaufwand (für alle!)
- Wenn nichts dagegen spricht, immer die größtmögliche Zahl nehmen
- An die Zukunft denken!

Schlüssellänge

Die Länge/Größe des Schlüssels (in Bit) bestimmt

- Die Größe der verwendeten Zahlen
- und damit den Rechenaufwand (für alle!)
- Wenn nichts dagegen spricht, immer die größtmögliche Zahl nehmen
- An die Zukunft denken!

Schlüssellänge

Die Länge/Größe des Schlüssels (in Bit) bestimmt

- Die Größe der verwendeten Zahlen
- und damit den Rechenaufwand (für alle!)
- Wenn nichts dagegen spricht, immer die größtmögliche Zahl nehmen
- An die Zukunft denken!

Schlüssellänge

Die Länge/Größe des Schlüssels (in Bit) bestimmt

- Die Größe der verwendeten Zahlen
- und damit den Rechenaufwand (für alle!)
- Wenn nichts dagegen spricht, immer die größtmögliche Zahl nehmen
- An die Zukunft denken!

Schlüssel und Passphrase

- Der Schlüssel (die großen Zahlen) dienen der Mathematik des Algorithmus
- Trick: Die Zahlen auf Festplatte speichern, aber gesondert verschlüsselt
- ... mit der Passphrase (und deshalb kann die auch geändert werden)
- Verschlüsselt wird nur der private Teil des Schlüssels

Schlüssel und Passphrase

- Der Schlüssel (die großen Zahlen) dienen der Mathematik des Algorithmus
- Trick: Die Zahlen auf Festplatte speichern, aber gesondert verschlüsselt
- ... mit der Passphrase (und deshalb kann die auch geändert werden)
- Verschlüsselt wird nur der private Teil des Schlüssels

Schlüssel und Passphrase

- Der Schlüssel (die großen Zahlen) dienen der Mathematik des Algorithmus
- Trick: Die Zahlen auf Festplatte speichern, aber gesondert verschlüsselt
- ... mit der Passphrase (und deshalb kann die auch geändert werden)
- Verschlüsselt wird nur der private Teil des Schlüssels

Schlüssel und Passphrase

- Der Schlüssel (die großen Zahlen) dienen der Mathematik des Algorithmus
- Trick: Die Zahlen auf Festplatte speichern, aber gesondert verschlüsselt
- ... mit der Passphrase (und deshalb kann die auch geändert werden)
- Verschlüsselt wird nur der private Teil des Schlüssels

Gute Passphrases

Eine ’gute’, d.h. schwer zu knackende Passwörter/ -phrases haben folgende Eigenschaften:

- stehen nicht in einem Wörterbuch
- sind keine Variationen von echten Wörtern (HALLO <-> h4110)
- sind lang genug, um ein Durchprobieren aller Möglichkeiten zu überstehen

Gute Passphrases

Eine ’gute’, d.h. schwer zu knackende Passwörter/ -phrases haben folgende Eigenschaften:

- stehen nicht in einem Wörterbuch
- sind keine Variationen von echten Wörtern (HALLO <-> h4110)
- sind lang genug, um ein Durchprobieren aller Möglichkeiten zu überstehen

Gute Passphrases

Eine ’gute’, d.h. schwer zu knackende Passwörter/ -phrases haben folgende Eigenschaften:

- stehen nicht in einem Wörterbuch
- sind keine Variationen von echten Wörtern (HALLO <-> h4110)
- sind lang genug, um ein Durchprobieren aller Möglichkeiten zu überstehen

Verfallsdatum

Bob kann seinem public key ein Verfallsdatum einschreiben.

- Das Verfallsdatum schlägt zu, auf wenn Bob eine Kompromitierung seines privaten Schlüssels nicht mitbekommen hat.
- oder er nicht alle erreicht, die seinen öffentlichen Schlüssel haben
- regelmässiger Wechsel der Schlüssel

Verfallsdatum

Bob kann seinem public key ein Verfallsdatum einschreiben.

- Das Verfallsdatum schlägt zu, auf wenn Bob eine Kompromitierung seines privaten Schlüssels nicht mitbekommen hat.
- oder er nicht alle erreicht, die seinen öffentlichen Schlüssel haben
- regelmässiger Wechsel der Schlüssel

Verfallsdatum

Bob kann seinem public key ein Verfallsdatum einschreiben.

- Das Verfallsdatum schlägt zu, auf wenn Bob eine Kompromitierung seines privaten Schlüssels nicht mitbekommen hat.
- oder er nicht alle erreicht, die seinen öffentlichen Schlüssel haben
- regelmässiger Wechsel der Schlüssel

Fingerprints

Woher weiss Alice, dass der öffentliche Schlüssel, den sie nutzt um Bob eine Mail zu schicken, auch der von Bob ist?

- Alice und Bob berechnen und vergleichen Prüfsumme (fingerprint)
- Key fingerprint = 4744 73DE 6ED4 BBE5 D897 D3F2 B8FA F345 ECC6 FD81
- Dafür brauchen Bob und Alice einen 2ten Kanal!
- Telefon, persönlich, Antifa-Info-Blatt

Fingerprints

Woher weiss Alice, dass der öffentliche Schlüssel, den sie nutzt um Bob eine Mail zu schicken, auch der von Bob ist?

- Alice und Bob berechnen und vergleichen Prüfsumme (fingerprint)
- Key fingerprint = 4744 73DE 6ED4 BBE5 D897 D3F2 B8FA F345 ECC6 FD81
- Dafür brauchen Bob und Alice einen 2ten Kanal!
- Telefon, persönlich, Antifa-Info-Blatt

Fingerprints

Woher weiss Alice, dass der öffentliche Schlüssel, den sie nutzt um Bob eine Mail zu schicken, auch der von Bob ist?

- Alice und Bob berechnen und vergleichen Prüfsumme (fingerprint)
- Key fingerprint = 4744 73DE 6ED4 BBE5 D897 D3F2 B8FA F345 ECC6 FD81
- Dafür brauchen Bob und Alice einen 2ten Kanal!
- Telefon, persönlich, Antifa-Info-Blatt

Fingerprints

Woher weiss Alice, dass der öffentliche Schlüssel, den sie nutzt um Bob eine Mail zu schicken, auch der von Bob ist?

- Alice und Bob berechnen und vergleichen Prüfsumme (fingerprint)
- Key fingerprint = 4744 73DE 6ED4 BBE5 D897 D3F2 B8FA F345 ECC6 FD81
- Dafür brauchen Bob und Alice einen 2ten Kanal!
- Telefon, persönlich, Antifa-Info-Blatt

Übersicht

Generierung eines Schlüsselpaares

- Passphrase
- Kommentar
- Gültigkeit
- Schlüsselstärke / Algorithmus

Generierung eines Widerrufs-Zertifikats

- Sein Schlüsselpaar als ungültig/kompromittiert markieren.
- Andere können dann keine Mails mehr an mich schicken.
- Am Besten auf CD brennen und bei Freunden deponieren.

Öffentl. Schlüssel verschicken

- Thunderbird: ’Meinen öffentlichen Schlüssel anhängen’

Öffentl. Schlüssel importieren

- Thunderbid: Rechtsclick auf Anhang -> ÖpenPGP Schlüssel importieren"

1. verschlüsselte Testmail

- Subject / Betreff wird nicht verschlüsselt !

Fingerabdruck ?

- Verschlüsselt ja, aber von wem ?
- Man-in-the-middle Attacke
- Fingerabdruck: Prüfsumme des öffentlichen Schlüssels, den beide haben

Fingerabdruck vergleichen

- Auf einem anderen Weg, nicht per Email
- Telefon
- In Printmedien veröffentlichen, z.B. Antifa Infoblatt
- Ausdrucken
- Webseite, z.b. https://systemausfall.org/node/9
- Persönlich, z.B. auf "Key signing parties"
- Thunderbird: OpenPGP -> Schlüssel verwalten
  - Rechtsclick auf Schlüssel -> Schlüsseleigenschaften

Signieren

- Damit man das Fingerabdruck-Vergleichen nur einmal machen muss
- Thunderbird: OpenPGP -> Schlüssel verwalten
  - Rechtsclick auf Schlüssel -> Unterschreiben
  - Lokal unterschreiben

Signatur

Woher weiss Bob, dass die Mail tatsächlich von Alice war?

- Authenzität: Die Mail ist wirklich von Alice
- Integrität: Die Mail ist unverändert
- Echtheitszertifikat
- Signatur ist unabhängig von der Verschlüsselung (geht mit und ohne)

Signatur

Woher weiss Bob, dass die Mail tatsächlich von Alice war?

- Authenzität: Die Mail ist wirklich von Alice
- Integrität: Die Mail ist unverändert
- Echtheitszertifikat
- Signatur ist unabhängig von der Verschlüsselung (geht mit und ohne)

Signatur

Woher weiss Bob, dass die Mail tatsächlich von Alice war?

- Authenzität: Die Mail ist wirklich von Alice
- Integrität: Die Mail ist unverändert
- Echtheitszertifikat
- Signatur ist unabhängig von der Verschlüsselung (geht mit und ohne)

Signatur

Woher weiss Bob, dass die Mail tatsächlich von Alice war?

- Authenzität: Die Mail ist wirklich von Alice
- Integrität: Die Mail ist unverändert
- Echtheitszertifikat
- Signatur ist unabhängig von der Verschlüsselung (geht mit und ohne)

Web of Trust

Signierte Schlüssel.

- Echtheitszertifikat für Schlüssel
- Beliebig viele Zertifikate
- Zertifikate werden Teil des öffentlichen Schlüssels und so weiterverteilt

Web of Trust

Signierte Schlüssel.

- Echtheitszertifikat für Schlüssel
- Beliebig viele Zertifikate
- Zertifikate werden Teil des öffentlichen Schlüssels und so weiterverteilt

Web of Trust

Signierte Schlüssel.

- Echtheitszertifikat für Schlüssel
- Beliebig viele Zertifikate
- Zertifikate werden Teil des öffentlichen Schlüssels und so weiterverteilt

Web of Trust

Warnung: Die Signaturen im Web-of-Trust veröffentlichen den social-graph!

- Wer kennt wenn, oder ist ihm/ihr schon mal begegnet
- und wann war das
- sind weitere Signaturen zeitnah erfolgt
- Vertrauensbeziehungen

Web of Trust

Warnung: Die Signaturen im Web-of-Trust veröffentlichen den social-graph!

- Wer kennt wenn, oder ist ihm/ihr schon mal begegnet
- und wann war das
- sind weitere Signaturen zeitnah erfolgt
- Vertrauensbeziehungen

Web of Trust

Warnung: Die Signaturen im Web-of-Trust veröffentlichen den social-graph!

- Wer kennt wenn, oder ist ihm/ihr schon mal begegnet
- und wann war das
- sind weitere Signaturen zeitnah erfolgt
- Vertrauensbeziehungen

Web of Trust

Warnung: Die Signaturen im Web-of-Trust veröffentlichen den social-graph!

- Wer kennt wenn, oder ist ihm/ihr schon mal begegnet
- und wann war das
- sind weitere Signaturen zeitnah erfolgt
- Vertrauensbeziehungen

Schlüssel entwerten

shit happens

- Problem: Entschlüsseln - Bob will, dass sein öffentlicher Schlüssel nicht mehr zum Verschlüsseln verwendet wird.
- Problem: Signatur - Bob will, dass sein öffentlicher Schlüssel nicht mehr zur Überprüfung von Signaturen taugt.

Schlüssel entwerten

shit happens

- Problem: Entschlüsseln - Bob will, dass sein öffentlicher Schlüssel nicht mehr zum Verschlüsseln verwendet wird.
- Problem: Signatur - Bob will, dass sein öffentlicher Schlüssel nicht mehr zur Überprüfung von Signaturen taugt.

Revokation

Bob will der Welt mitteilen, dass sein public key nicht mehr gültig ist.

- Bob erzeugt ein Widerrufs-Zertifikat
- Anhand der Signatur kann erkannt werden, dass der Widerruf echt ist
- Bob verteilt das Widerrufs-Zertifikat, wenn er seinen key ungültig machen will
- Das Zertifikat muss er erzeugt haben, solange er seinen privaten Schlüssel hat!
- Nur der öffentliche Schlüssel wird ungültig, mit dem privaten können weiterhin alte Mails entschlüsselt werden.

Revokation

Bob will der Welt mitteilen, dass sein public key nicht mehr gültig ist.

- Bob erzeugt ein Widerrufs-Zertifikat
- Anhand der Signatur kann erkannt werden, dass der Widerruf echt ist
- Bob verteilt das Widerrufs-Zertifikat, wenn er seinen key ungültig machen will
- Das Zertifikat muss er erzeugt haben, solange er seinen privaten Schlüssel hat!
- Nur der öffentliche Schlüssel wird ungültig, mit dem privaten können weiterhin alte Mails entschlüsselt werden.

Revokation

Bob will der Welt mitteilen, dass sein public key nicht mehr gültig ist.

- Bob erzeugt ein Widerrufs-Zertifikat
- Anhand der Signatur kann erkannt werden, dass der Widerruf echt ist
- Bob verteilt das Widerrufs-Zertifikat, wenn er seinen key ungültig machen will
- Das Zertifikat muss er erzeugt haben, solange er seinen privaten Schlüssel hat!
- Nur der öffentliche Schlüssel wird ungültig, mit dem privaten können weiterhin alte Mails entschlüsselt werden.

Revokation

Bob will der Welt mitteilen, dass sein public key nicht mehr gültig ist.

- Bob erzeugt ein Widerrufs-Zertifikat
- Anhand der Signatur kann erkannt werden, dass der Widerruf echt ist
- Bob verteilt das Widerrufs-Zertifikat, wenn er seinen key ungültig machen will
- Das Zertifikat muss er erzeugt haben, solange er seinen privaten Schlüssel hat!
- Nur der öffentliche Schlüssel wird ungültig, mit dem privaten können weiterhin alte Mails entschlüsselt werden.

Revokation

Bob will der Welt mitteilen, dass sein public key nicht mehr gültig ist.

- Bob erzeugt ein Widerrufs-Zertifikat
- Anhand der Signatur kann erkannt werden, dass der Widerruf echt ist
- Bob verteilt das Widerrufs-Zertifikat, wenn er seinen key ungültig machen will
- Das Zertifikat muss er erzeugt haben, solange er seinen privaten Schlüssel hat!
- Nur der öffentliche Schlüssel wird ungültig, mit dem privaten können weiterhin alte Mails entschlüsselt werden.

Übersicht

Schlüsselserver

- Vereinfacht den Schlüsselaustausch
- Thunderbird: OpenPGP -> Schlüssel verwalten
  - Schlüsselserver -> Schlüssel suchen
  - z.B. info@systemausfall.org
  - In der Regel: neueren Schlüssel nehmen - oder nochmal nachfragen
- Soll ich meinen öffentlichen Schlüssel zu einem Schlüsselserver hochladen ?
- Photo-ID: z.B. bei Schlüssel 0x7A7115F1

Mail signieren

- Thunderbird: Im Mail verfassen Fenster -> OpenPGP -> Nachricht unterschreiben

Etc

- Backup: Wohin mit Schlüsselpaar / Widerrufszertifikat ?
- Was tun wenns brennt ?
- Reisen / ohne Laptop unterwegs: Webmail und GPG ?
- ...noch Fragen ?

Was ist eine Schleuder?

- Eine Schleuder ist eine verschlüsselte Mailingliste zur Gruppenkommunikation
- man schreibt nicht wie auf einer normalen Mailingliste unverschlüsselte Mails an die Gruppenmitglieder
- man muss nicht einzeln an alle Gruppenmitglieder verschlüsseln
- man schreibt an die Schleuder, die dafür sorgt, dass alle Mails immer verschlüsselt werden

Was ist eine Schleuder?

- Eine Schleuder ist eine verschlüsselte Mailingliste zur Gruppenkommunikation
- man schreibt nicht wie auf einer normalen Mailingliste unverschlüsselte Mails an die Gruppenmitglieder
- man muss nicht einzeln an alle Gruppenmitglieder verschlüsseln
- man schreibt an die Schleuder, die dafür sorgt, dass alle Mails immer verschlüsselt werden

Was ist eine Schleuder?

- Eine Schleuder ist eine verschlüsselte Mailingliste zur Gruppenkommunikation
- man schreibt nicht wie auf einer normalen Mailingliste unverschlüsselte Mails an die Gruppenmitglieder
- man muss nicht einzeln an alle Gruppenmitglieder verschlüsseln
- man schreibt an die Schleuder, die dafür sorgt, dass alle Mails immer verschlüsselt werden

Was ist eine Schleuder?

- Eine Schleuder ist eine verschlüsselte Mailingliste zur Gruppenkommunikation
- man schreibt nicht wie auf einer normalen Mailingliste unverschlüsselte Mails an die Gruppenmitglieder
- man muss nicht einzeln an alle Gruppenmitglieder verschlüsseln
- man schreibt an die Schleuder, die dafür sorgt, dass alle Mails immer verschlüsselt werden

Wie funktioniert eine Schleuder?

- Eine Schleuder hat einen eigenes Schlüsselpaar
- Sie verwaltet die öffentlichen Schlüssel der einzelnen Mitglieder
- Man braucht nur den öffentlichen Schlüssel der Schleuder, um an alle Mitglieder Mails zu schicken
- Ausnahmen: man kann eine Schleuder auch so einrichten, dass unverschlüsselte/unsignierte Mails versendet werden können, um diese Variante kümmern wir uns aber jetzt nicht...

Wie funktioniert eine Schleuder?

- Eine Schleuder hat einen eigenes Schlüsselpaar
- Sie verwaltet die öffentlichen Schlüssel der einzelnen Mitglieder
- Man braucht nur den öffentlichen Schlüssel der Schleuder, um an alle Mitglieder Mails zu schicken
- Ausnahmen: man kann eine Schleuder auch so einrichten, dass unverschlüsselte/unsignierte Mails versendet werden können, um diese Variante kümmern wir uns aber jetzt nicht...

Wie funktioniert eine Schleuder?

- Eine Schleuder hat einen eigenes Schlüsselpaar
- Sie verwaltet die öffentlichen Schlüssel der einzelnen Mitglieder
- Man braucht nur den öffentlichen Schlüssel der Schleuder, um an alle Mitglieder Mails zu schicken
- Ausnahmen: man kann eine Schleuder auch so einrichten, dass unverschlüsselte/unsignierte Mails versendet werden können, um diese Variante kümmern wir uns aber jetzt nicht...

Wie funktioniert eine Schleuder?

- Eine Schleuder hat einen eigenes Schlüsselpaar
- Sie verwaltet die öffentlichen Schlüssel der einzelnen Mitglieder
- Man braucht nur den öffentlichen Schlüssel der Schleuder, um an alle Mitglieder Mails zu schicken
- Ausnahmen: man kann eine Schleuder auch so einrichten, dass unverschlüsselte/unsignierte Mails versendet werden können, um diese Variante kümmern wir uns aber jetzt nicht...

Die Schleuder benutzen

- Vor Verschicken von Mails über die Schleuder: einmalig eine unverschlüsselte Mail an testliste-sendkey@nadir.org schicken, Betreff und Inhalt sind egal
- Man bekommt dann eine Mail mit dem öffentlichen Schlüssel zurück und muss ihn importieren
- Mail an die Schleuder schicken: immer verschlüsselt, signiert und nicht im html-Format

Die Schleuder benutzen

- Vor Verschicken von Mails über die Schleuder: einmalig eine unverschlüsselte Mail an testliste-sendkey@nadir.org schicken, Betreff und Inhalt sind egal
- Man bekommt dann eine Mail mit dem öffentlichen Schlüssel zurück und muss ihn importieren
- Mail an die Schleuder schicken: immer verschlüsselt, signiert und nicht im html-Format

Die Schleuder benutzen

- Vor Verschicken von Mails über die Schleuder: einmalig eine unverschlüsselte Mail an testliste-sendkey@nadir.org schicken, Betreff und Inhalt sind egal
- Man bekommt dann eine Mail mit dem öffentlichen Schlüssel zurück und muss ihn importieren
- Mail an die Schleuder schicken: immer verschlüsselt, signiert und nicht im html-Format

Beispiel

From: anna
To: list

Liste entschlüsselt
und verschlüsselt

From: list
To: arthur

From: list
To: anton

From: list
To: andrea

Beispiel

From: anna
To: list

Liste entschlüsselt und verschlüsselt

From: list
To: arthur

From: list
To: anton

From: list
To: andrea

Beispiel

From: anna
To: list

Liste entschlüsselt
und verschlüsselt

From: list
To: arthur

From: list
To: anton

From: list
To: andrea

Beispiel

From: anna
To: list

Liste entschlüsselt und verschlüsselt

From: list
To: arthur

From: list
To: anton

From: list
To: andrea

Beispiel

From: anna
To: list

Liste entschlüsselt und verschlüsselt

From: list
To: arthur

From: list
To: anton

From: list
To: andrea

Befehle für Admins zur Schleuderverwaltung

- Es gibt Spezialkommandos, mit der einE Admin die Schleuder verwalten kann
- Die Kommandos werden per Mail (im Body) direkt an die Schleuderadresse geschickt

Befehle für Admins zur Schleuderverwaltung

- Es gibt Spezialkommandos, mit der einE Admin die Schleuder verwalten kann
- Die Kommandos werden per Mail (im Body) direkt an die Schleuderadresse geschickt

Adminbefehle zur Schleuderverwaltung

- Eine Mail als Kopie an ein Nichtmitglied schicken (dafür muss der Schlüssel der Adresse importiert sein)

X-RESEND: NICHTMITGLIED@nadir.org

Adminbefehle zur Schleuderverwaltung

- Um die aktuellen Schleuder-Mitglieder aufgelistet zu bekommen:

X-GET-MEMBERS:

Adminbefehle zur Schleuderverwaltung

- Um ein neues Schleuder-Mitglied einzutragen:

X-SAVE-MEMBERS:
- email: altes-Mitglied-1@nadir.org
- email: altes-Mitglied-2.org
- email: altes-Mitglied-3@nadir.org
- email: NEUE-ADRESSE@nadir.org

- Wichtig: X-SAVE-MEMBERS überschreibt aktuelle Mitglieder, deshalb immer vollständige Membersliste eintragen und neue Adresse(n) unten anfügen!

Adminbefehle zur Schleuderverwaltung

- Um ein neues Schleuder-Mitglied einzutragen:

```
X-SAVE-MEMBERS:
- email: altes-Mitglied-1@nadir.org
- email: altes-Mitglied-2.org
- email: altes-Mitglied-3@nadir.org
- email: NEUE-ADRESSE@nadir.org
```

- Wichtig: X-SAVE-MEMBERS überschreibt aktuelle Mitglieder, deshalb immer vollständige Membersliste eintragen und neue Adresse(n) unten anfügen!

Befehle für Admins zur Schleuderverwaltung

- Listet alle bekannten öffentlichen Schlüssel auf:

X-LIST-KEYS:

Adminbefehle zur Schleuderverwaltung

- Vollständigen öffentlichen Schlüssel importieren:

```
X-ADD-KEY:
——BEGIN PGP PUBLIC KEY BLOCK——
Version: GnuPG v1.4.9 (GNU/Linux)
mQGiBEjVO7oRBADQvT6wtD2IzzIiK0NbrcilCKCp4M2
(...)
JZIcfhO1zEbwc1ZKF3JuQ9X5GRmY62hz9SBUnOL08NB
=xTv3
——END PGP PUBLIC KEY BLOCK——
```

Adminbefehle zur Schleuderverwaltung

- Einen Schlüssel entfernen mit der keyId:

```
X-DEL-KEY: 0x745F67DB
```

Weitere Infos

- Mehr Infos: schleuder2.nadir.org