Anonymität im Internet

Matthias Bauer

matthiasb@saeftl.franken.de

Warum Anonymität?

- Natürlicher Zustand im Alltag.

Warum Anonymität?

- Natürlicher Zustand im Alltag.
- Urteil vom BundesVerfassungsGericht.

Warum Anonymität?

- Natürlicher Zustand im Alltag.
- Urteil vom BundesVerfassungsGericht.
- Aufzeigen von Straftaten durch Insider (”Whistleblowing“).

Warum Anonymität?

- Natürlicher Zustand im Alltag.
- Urteil vom BundesVerfassungsGericht.
- Aufzeigen von Straftaten durch Insider (”Whistleblowing“).
- Kritik an semi–legalen Organisationen/Regimekritik.

Warum Anonymität?

- Natürlicher Zustand im Alltag.
- Urteil vom BundesVerfassungsGericht.
- Aufzeigen von Straftaten durch Insider (”Whistleblowing“).
- Kritik an semi–legalen Organisationen/Regimekritik.
- Open Source Entwicklung nach der Einführung von Software Patenten.

Anonymität?

- Alle Benutzer des anonymierenden Dienstes bilden die Anonymitäts–Menge.
- Ein Dienst ist anonymisierend, wenn ein Beobachter von einer abgehörten Nachricht nur sagen kann, dass der Absender in der Anonymitäts–Menge ist.

Protokolle anonymisieren

- HTTP — Hart, weil:

Protokolle anonymisieren

- HTTP — Hart, weil:
  - JavaScript, Java, . . .

Protokolle anonymisieren

- HTTP — Hart, weil:
  - JavaScript, Java, . . .
  - Zahlreiche Eigenschaften des Protokolls vereinfachen Beobachtung.

Protokolle anonymisieren

- HTTP — Hart, weil:
  - JavaScript, Java, . . .
  - Zahlreiche Eigenschaften des Protokolls vereinfachen Beobachtung.
  - Enge Korrelation zwischen Anfragen.

Protokolle anonymisieren

- HTTP — Hart, weil:
  - JavaScript, Java, . . .
  - Zahlreiche Eigenschaften des Protokolls vereinfachen Beobachtung.
  - Enge Korrelation zwischen Anfragen.
  - Mit Proxies allein nur sehr beschränkt zu machen.

Protokolle anonymisieren

- HTTP — Hart, weil:
  - JavaScript, Java, . . .
  - Zahlreiche Eigenschaften des Protokolls vereinfachen Beobachtung.
  - Enge Korrelation zwischen Anfragen.
  - Mit Proxies allein nur sehr beschränkt zu machen.
- Mail — Einfacher, weil:

Protokolle anonymisieren

- HTTP — Hart, weil:
  - JavaScript, Java, . . .
  - Zahlreiche Eigenschaften des Protokolls vereinfachen Beobachtung.
  - Enge Korrelation zwischen Anfragen.
  - Mit Proxies allein nur sehr beschränkt zu machen.
- Mail — Einfacher, weil:
  - Ziemlich Asynchron.

Protokolle anonymisieren

- HTTP — Hart, weil:
  - JavaScript, Java, . . .
  - Zahlreiche Eigenschaften des Protokolls vereinfachen Beobachtung.
  - Enge Korrelation zwischen Anfragen.
  - Mit Proxies allein nur sehr beschränkt zu machen.
- Mail — Einfacher, weil:
  - Ziemlich Asynchron.
  - Normalerweise kein ”Active Content“.

Der unprofessionelle Ansatz

- Webmail–Accounts bei kostenlosen Anbietern.
  Vorteil: Keine spezielle Software oder Infrastruktur nötig.
  Nachteil: Der Webmail–Anbieter kriegt die IP-Adresse (ausser man hat anonymes HTTP).

Der unprofessionelle Ansatz

- Webmail–Accounts bei kostenlosen Anbietern.
  Vorteil: Keine spezielle Software oder Infrastruktur nötig.
  Nachteil: Der Webmail–Anbieter kriegt die IP-Adresse (ausser man hat anonymes HTTP).
- Gegen Strafverfolger oder kriminelle Organisationen kein ausreichender Schutz.

Geschichte des professionellen Ansatz

- Penet.fi Remailer

Geschichte des professionellen Ansatz

- Penet.fi Remailer
- Cypherpunk Remailer

Geschichte des professionellen Ansatz

- Penet.fi Remailer
- Cypherpunk Remailer
- Mixmaster Remailer

Public Key Kryptographie

Public Key Kryptographie: Verschlüsselung mit Schlüsselpaaren,

- einer nur zum Verschlüsseln: öffentlicher Schlüssel (public key) P.

Beispiel: PGP, verfügbar für praktisch jedes Betriebssystem.

Public Key Kryptographie

Public Key Kryptographie: Verschlüsselung mit Schlüsselpaaren,

- einer nur zum Verschlüsseln: öffentlicher Schlüssel (public key) P.
- ein anderer nur zum Entschlüsseln: privater Schlüssel (secret key) S.

Beispiel: PGP, verfügbar für praktisch jedes Betriebssystem.

Chaums Mixe

- Grundliegende Idee der meisten geplanten Anomysierungsdienste.

Chaums Mixe

- Grundliegende Idee der meisten geplanten Anomysierungsdienste.
- von David Chaum, 1988

Chaums Mixe

- Grundliegende Idee der meisten geplanten Anomysierungsdienste.
- von David Chaum, 1988
- *Brief im Briefumschlag im Briefumschlag . . . und jeder macht den äussersten auf und wirft den inneren Brief wieder in den Briefkasten*.

Chaums Mixe / Type I Remailer

A will B die Nachricht *N* schicken. Er verschlüsselt sie mit Bs Public Key :

$$M = E_B(N)$$

Chaums Mixe / Type I Remailer

A stellt einen `To: B` Header davor und verschlüsselt mit dem Key von R_3 :

$$M = (E_{R_3}(\text{"To : B"}, E_B(N)))$$

Chaums Mixe / Type I Remailer

A stellt einen To: R_3 Header davor und verschlüsselt mit dem Key von R_1 :

$$M = (E_{R_1}(\text{"To : R}_3\text{"}, E_{R_3}(\text{"To : B"}, E_B(N))))$$

Chaums Mixe / Type I Remailer

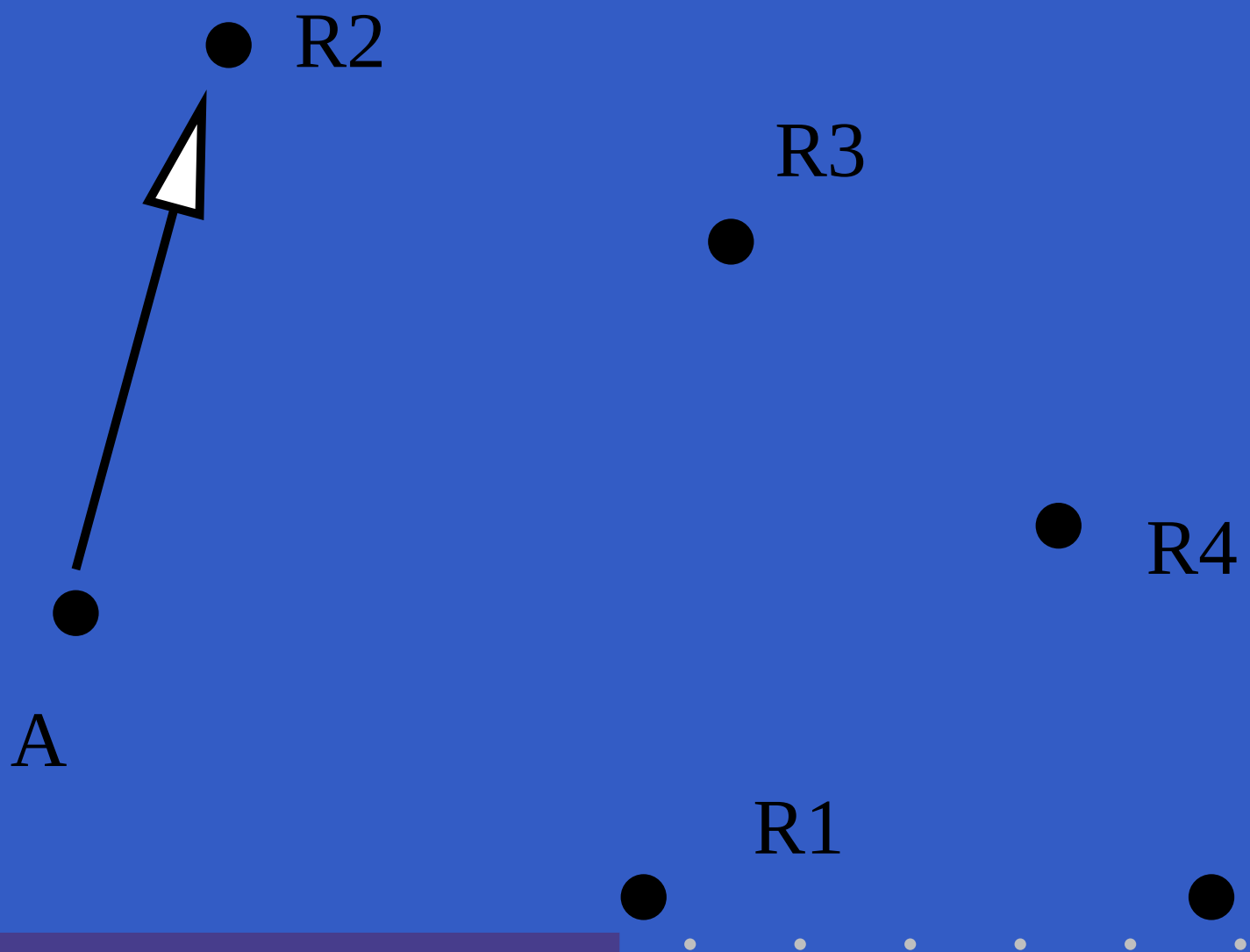
A stellt einen To: R_1 Header davor und verschlüsselt mit dem Key von R_2:

$$M = E_{R_2}(\text{"To : R}_1\text{"}, E_{R_1}(\text{"To : R}_3\text{"}, E_{R_3}(\text{"To : B"}, E_B(N))))$$

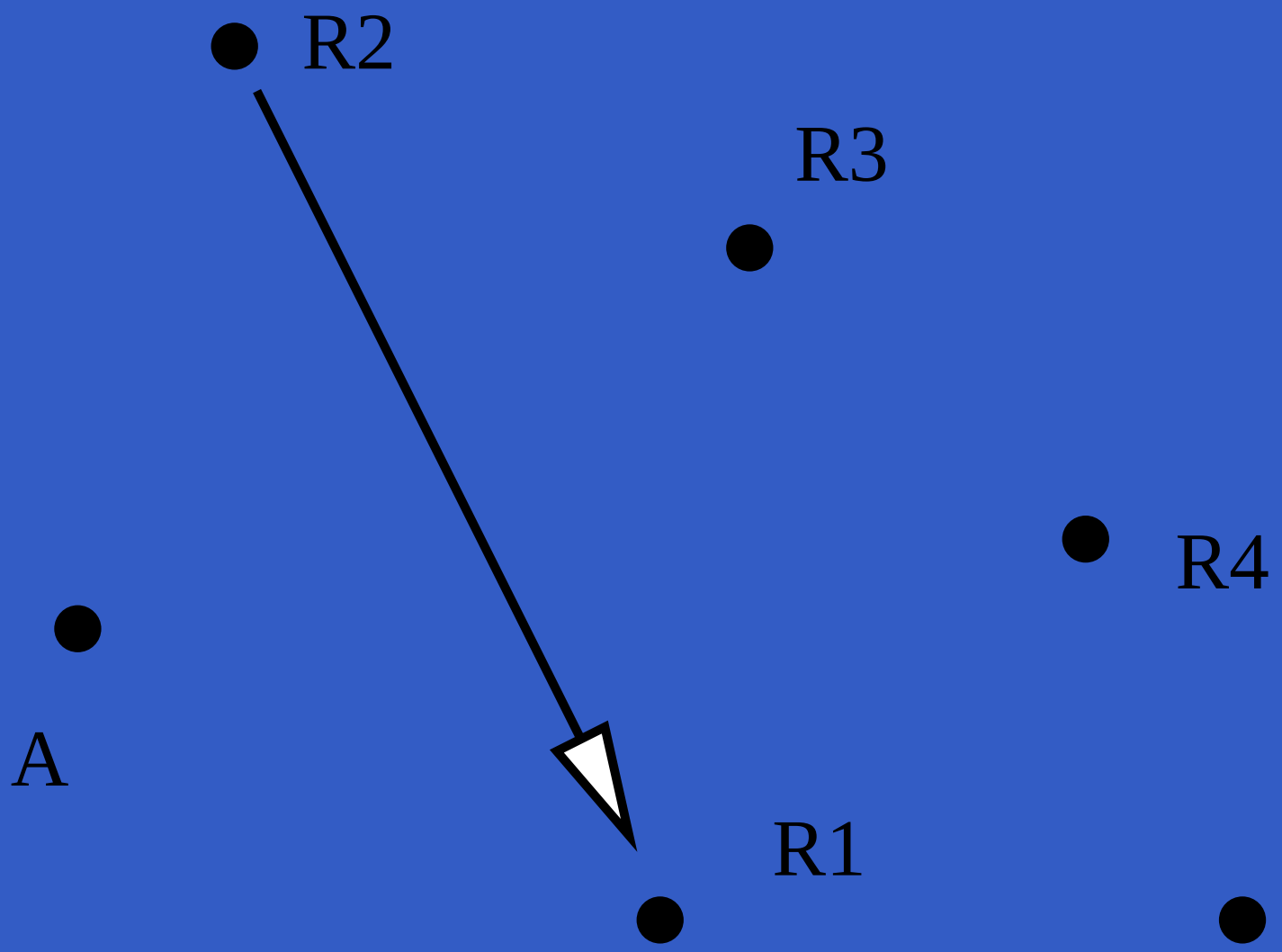
Chaums Mixe / Type I Remailer

A schickt M an R_2 .

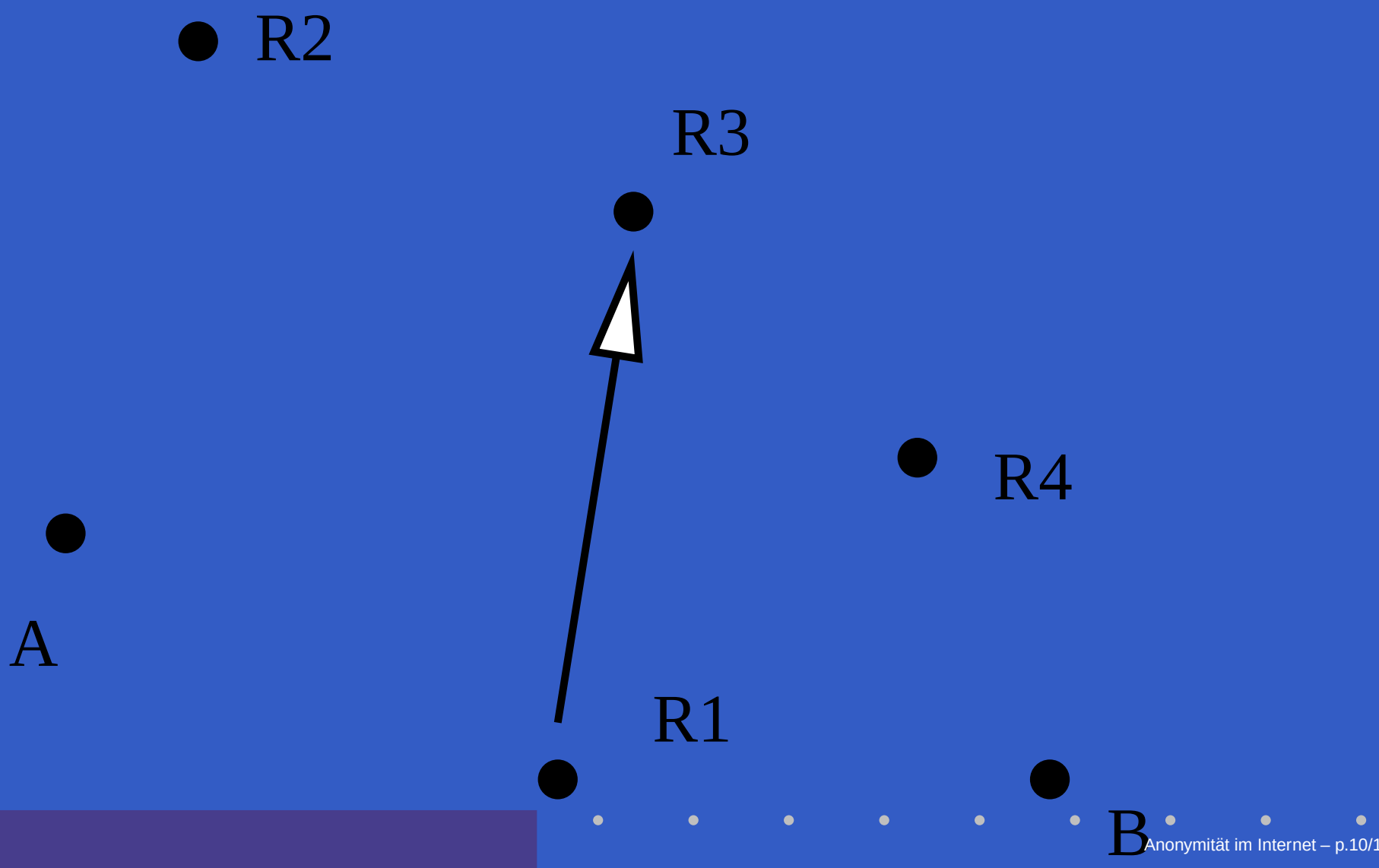
Chaums Mixe (2)



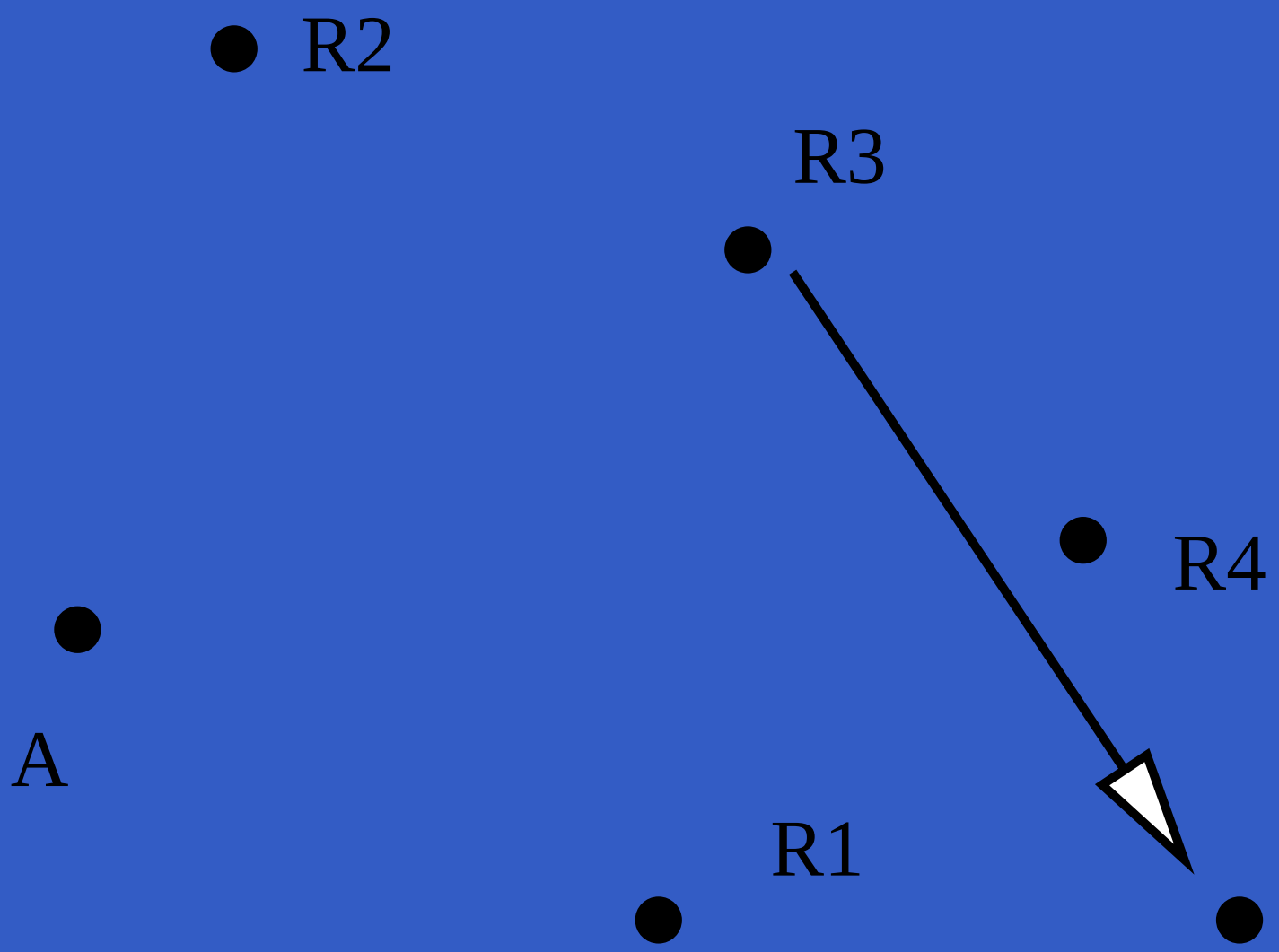
Chaums Mixe (2)



Chaums Mixe (2)



Chaums Mixe (2)



Analyse

Obwohl das gut ausschaut, gibts Attacken, wenn der Angreifer mächtig genug ist :

- Die Remailer funktionieren ”First in – First out“.

Analyse

Obwohl das gut ausschaut, gibts Attacken, wenn der Angreifer mächtig genug ist :

- Die Remailer funktionieren ”First in – First out“.
- Die Längen der Nachrichten sind im Allgemeinen charakteristisch.

Analyse

Obwohl das gut ausschaut, gibts Attacken, wenn der Angreifer mächtig genug ist :

- Die Remailer funktionieren ”First in – First out“.
- Die Längen der Nachrichten sind im Allgemeinen charakteristisch.
- Die Nachrichten werden mit jeder Entschlüsselung kürzer.

Analyse

Obwohl das gut ausschaut, gibts Attacken, wenn der Angreifer mächtig genug ist :

- Die Remailer funktionieren ”First in – First out“.
- Die Längen der Nachrichten sind im Allgemeinen charakteristisch.
- Die Nachrichten werden mit jeder Entschlüsselung kürzer.
- Man kann eine abgefangene Nachricht mehrfach wieder reinschicken.

Analyse

Obwohl das gut ausschaut, gibts Attacken, wenn der Angreifer mächtig genug ist :

- Die Remailer funktionieren ”First in – First out“.
- Die Längen der Nachrichten sind im Allgemeinen charakteristisch.
- Die Nachrichten werden mit jeder Entschlüsselung kürzer.
- Man kann eine abgefangene Nachricht mehrfach wieder reinschicken.
- Mixmaster versucht diese Fehler zu beheben.

Mixmaster oder Type II Remailer

- Nachrichten werden vor dem Versenden in immer gleich grosse Teile zerlegt, die einzeln verschickt werden.

Mixmaster oder Type II Remailer

- Nachrichten werden vor dem Versenden in immer gleich grosse Teile zerlegt, die einzeln verschickt werden.
- Jeder Remailer füllt die Nachricht nach dem Entschlüsseln mit Zufall auf.

Mixmaster oder Type II Remailer

- Nachrichten werden vor dem Versenden in immer gleich grosse Teile zerlegt, die einzeln verschickt werden.
- Jeder Remailer füllt die Nachricht nach dem Entschlüsseln mit Zufall auf.
- Nachrichten werden von Remailern verzögert und gemischt.

Client Software

Mit was kann man anonymisierte Maildienste benutzen?

- Unter Unix und Windows: `mixmaster`.

Client Software

Mit was kann man anonymisierte Maildienste benutzen?

- Unter Unix und Windows: `mixmaster`.
- Unix-Mailer `mutt` hat rudimentäre Einbindung von `mixmaster` (und `pgp/gpg`).

Client Software

Mit was kann man anonymisierte Maildienste benutzen?

- Unter Unix und Windows: `mixmaster`.
- Unix-Mailer `mutt` hat rudimentäre Einbindung von `mixmaster` (und `pgp/gpg`).
- Unter Windows *Jack B. Nymble* von Potatoware, mit graphischem Front-End und guter Doku.

Konfiguration (1)

Public Key Krypto mit völlig Unbekannten: Henne–Ei Problem

- Man kann den Key vom Remailer unauthentifiziert anfragen.
- Es gibt Dienste im Web, die Remailer Keys auflisten.

Konfiguration (2)

Remailer fallen aus, jeder ist aber kritischer Punkt

- Man kann den Remailer selbst nach Statistiken fragen.
- Oder das Web bemühen (remailer-stats, pinger-Skripten).

Empfehlung

Wer anonyme Emails schreiben oder empfangen will, sollte idealerweise selbst einen Remailer betreiben.

Derzeit: 51 Mixmaster Remailer.

`mixmaster@immd1.informatik.uni-erlangen.de`

leitet > 2000 Mails pro Tag weiter.

Server Software

- `mixmaster` (Ulf Möller) für Unix.

Server Software

- `mixmaster` (Ulf Möller) für Unix.
- `Reliable` (Potatoware) für Windows.

Weiterführend

- *JAP* : Java–basierter HTTP-Anonymizer Dienst vom Datenschutzbüro Schleswig und UniDresden.

Weiterführend

- *JAP* : Java–basierter HTTP-Anonymizer Dienst vom Datenschutzbüro Schleswig und UniDresden.
- *Freedom.net*: Genereller TCP/IP Anonymisierer mit Moduln für Mail und HTTP.

Weiterführend

- *JAP* : Java–basierter HTTP-Anonymizer Dienst vom Datenschutzbüro Schleswig und UniDresden.
- *Freedom.net*: Genereller TCP/IP Anonymisierer mit Moduln für Mail und HTTP.
- *NymIP, GnuNet, . . .* Dutzende von OpenSource Projekten verschiedenen Reifegrads.

Weiterführend

- *JAP* : Java–basierter HTTP-Anonymizer Dienst vom Datenschutzbüro Schleswig und UniDresden.
- *Freedom.net*: Genereller TCP/IP Anonymisierer mit Moduln für Mail und HTTP.
- *NymIP, GnuNet, . . .* Dutzende von OpenSource Projekten verschiedenen Reifegrads.
- *Freenet.sourceforge.net, . . .* Einige P2P Protokolle implementieren anonymisierende Dienste.