MOCA 2008

Introduzione all'uso dei remailer anonimi

Leandro Noferini - lnoferin@cybervalley.org

Di cosa parleremo

- Cosa sono i remailer anonimi
- Come funzionano
- Come si usano
- Altri servizi

Non parleremo della gestione di un remailer anonimo

Qual'è il problema

L'uso della cifratura nella posta elettronica non elimina completamente i problemi relativi alla privacy perché in ogni caso restano visibili

la quantità dei messaggi

la dimensione dei messaggi

data e ora di spedizione e ricevimento

partecipanti alla discussione

Cos'è un remailer anonimo

Un remailer anonimo è un programma che filtra i messaggi di posta elettronica che riceve per eliminare tutti gli header che permetterebbero l'identificazione del mittente del messaggio

Permette l'invio di:

messaggi di posta elettronica

articoli sui newsgroups (usando i gateway)

Nym

Tipi di remailer

- tipo I - cypherpunk
- tipo II - mixmaster
- tipo III - mixminion

Qui parleremo fondamentalmente dei remailer di tipo II mixmaster perché sono quelli attualmente maggiormente diffusi e affidabili

Caratteristiche comuni

Funzionano con la tecnica delle chiavi pubblica/privata

Usano la tecnica del trasporto di cipolle

onion routing

Si basano sull'

uso di tutta la rete dei remailer

Assicurano l'anonimato anche rispetto all'operatore del remailer stesso

(seguendo correttamente le norme)

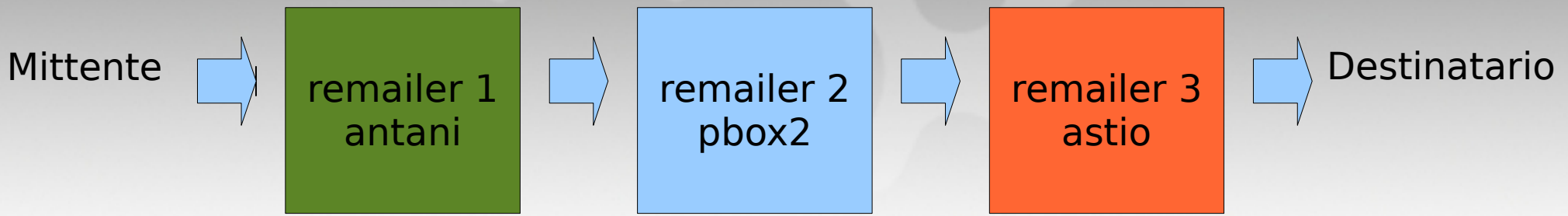
Funzionamento (tipi I e II)

- riceve il messaggio
- eventualmente lo decifra
- opera sul messaggio
- reinvia il messaggio

Funzionamento quasi tutto in automatico

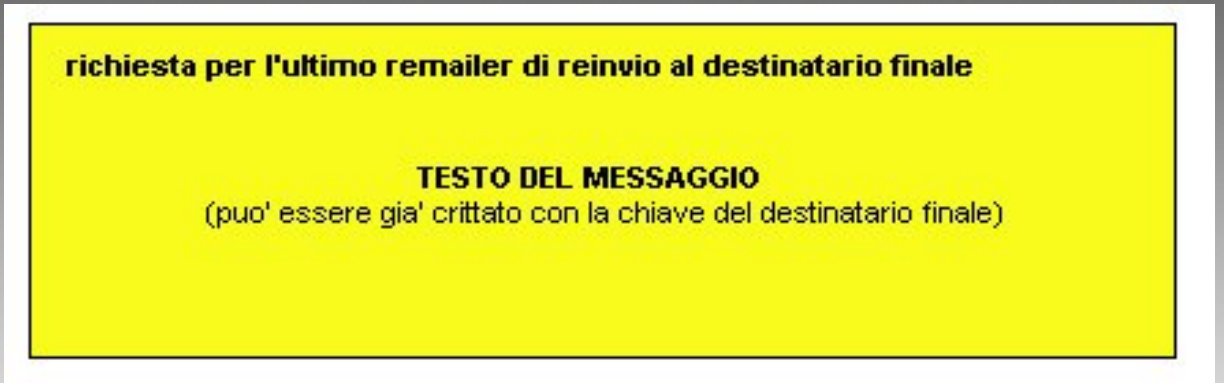
Uso – linee generali

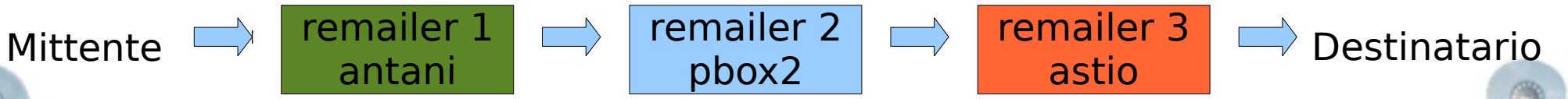
Il mittente sceglie la catena e ne scarica le chiavi pubbliche



Uso – linee generali

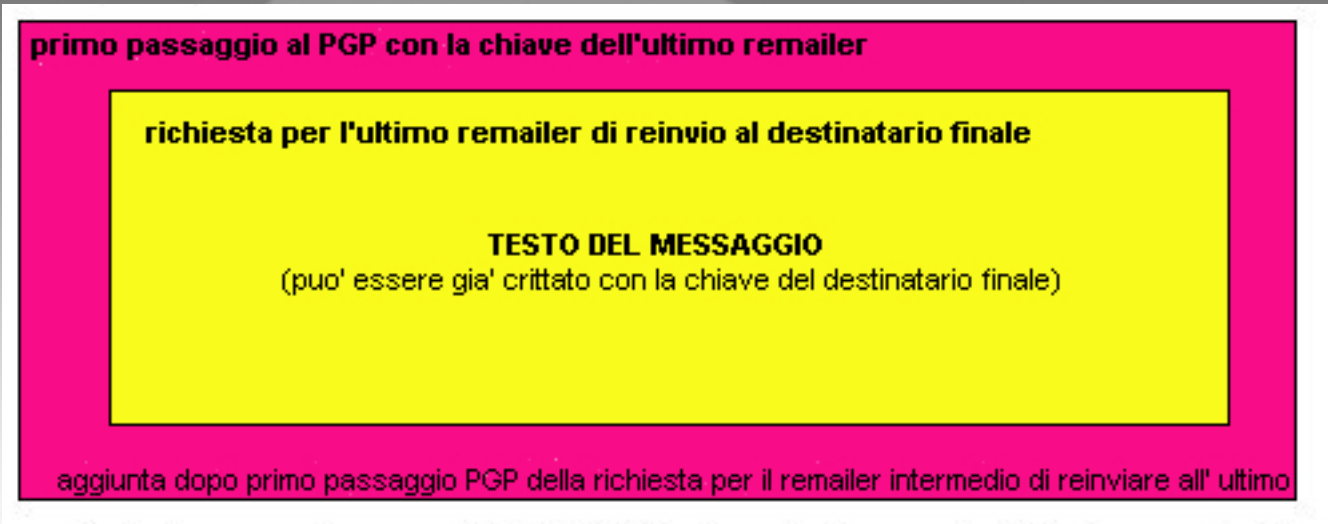
Il mittente prepara il testo per il destinatario





Uso – linee generali

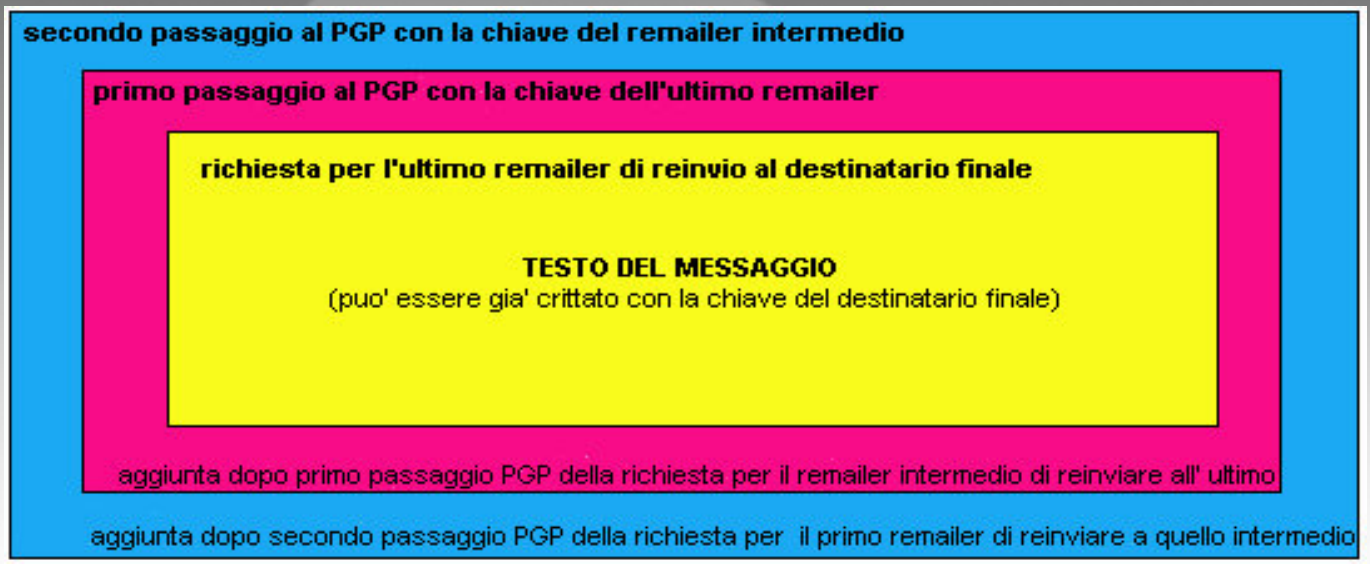
Il mittente cifra il testo usando la chiave dell'ultimo remailer



Mittente → remailer 1 antani → remailer 2 pbox2 → remailer 3 astio → Destinatario

Uso – linee generali

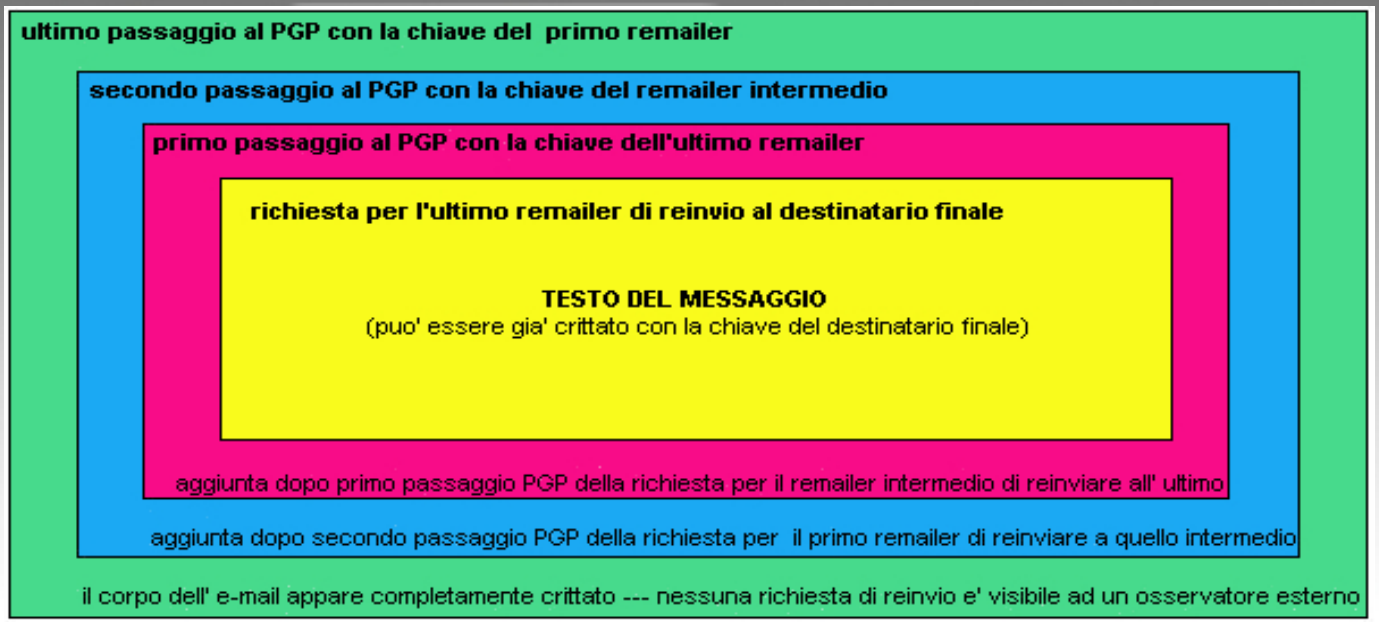
Il mittente cifra il messaggio ottenuto usando la chiave del remailer intermedio



Mittente → remailer 1 antani → remailer 2 pbox2 → remailer 3 astio → Destinatario

Uso – linee generali

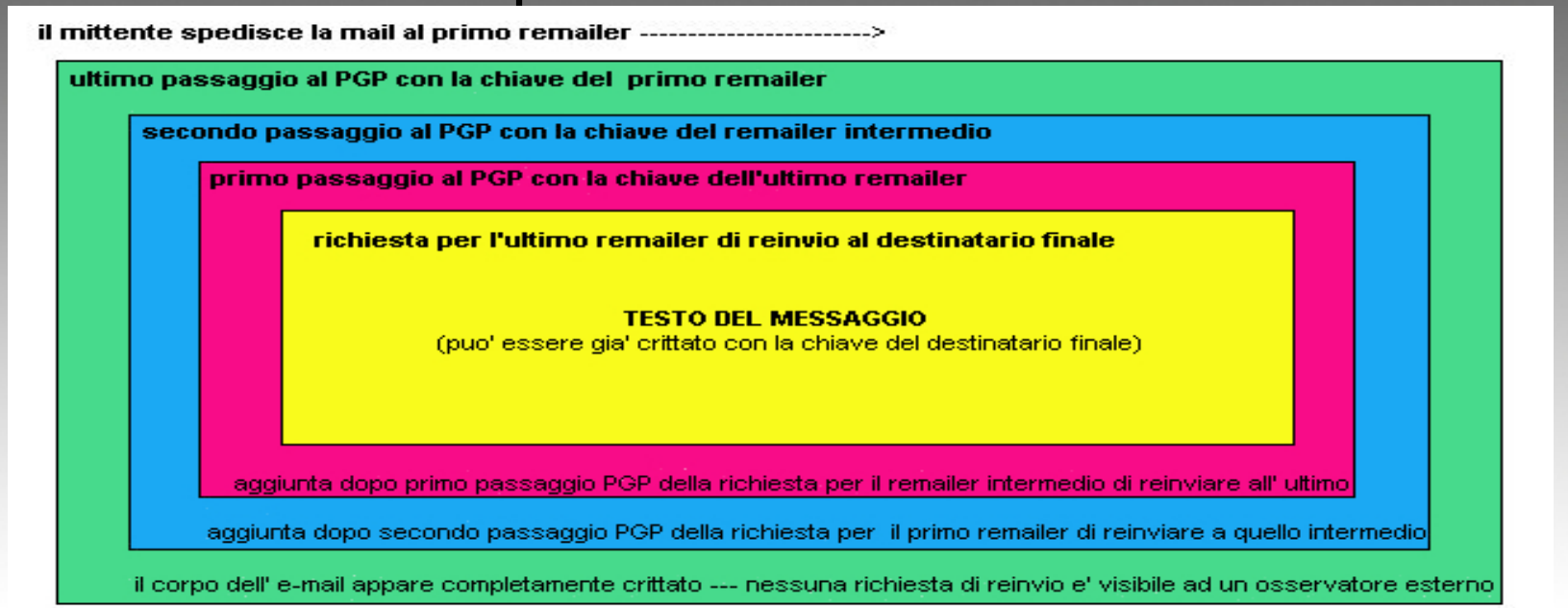
Il mittente cifra il messaggio ottenuto usando la chiave del primo remailer



Mittente → remailer 1 antani → remailer 2 pbox2 → remailer 3 astio → Destinatario

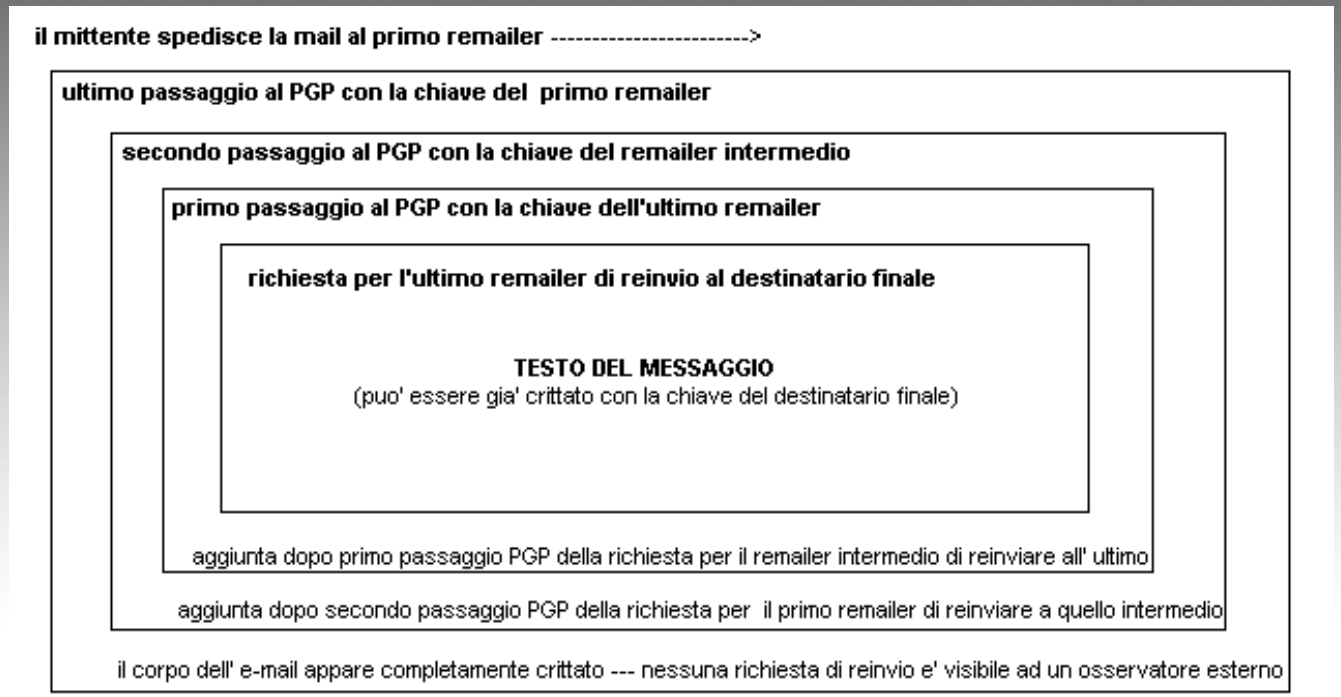
Uso – linee generali

Il mittente spedisce il messaggio ottenuto verso il primo remailer



Mittente → remailer 1 antani → remailer 2 pbox2 → remailer 3 astio → Destinatario

Questa è l'immagine originale dal libro Kriptonite



MOCA 2008

Aspetto dei messaggi
Messaggio normale

Received: by best123bingo.com (PowerMTA(TM) v3.5r6) id hfd8g80kg0kj for
<lnoferin@cybervalley.org>; M\
on, 14 Jul 2008 09:13:35 -0400 (envelope-from <promotion@best123bingo.com>)
Date: Mon, 14 Jul 2008 08:44:02 -0400 (EDT)
From: Prism <promotion@best123bingo.com>
Reply-To: promotion@best123bingo.com
To: lnoferin@cybervalley.org
Message-ID: <86309451123451330 56.1216039442333.EMail.promotion@best123bingo.com>

Subject: Diamond Forever
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-Mailer-MsgId: bG5vZmVyaW5AY3liZXJ2YWxsZXkub3Jn
X-Mailer-CSID: 17_909

```
<html>
   <head>
      <title></title>
   </head>
   <body topmargin=3D"0">
      <table cellspacing=3D"0" cellpadding=3D"0" width=3D"550" align=3D"c=
```

LFG

MOCA 2008

Aspetto dei messaggi
Messaggio da remailer

From: Borked Pseudo Mailed <nobody@pseudo.borked.net>
Comments: This message did not originate from the Sender address above.
        It was remailed automatically by anonymizing remailer software.
        Please report problems or inappropriate use to the
        remailer administrator at <admin@pseudo.borked.net>.
To: e-privacy@firenze.linux.it
Message-ID: <9ec16233d60412f46b7ac4b5b9850a8f@pseudo.borked.net>
Date: Fri, 11 Jul 2008 03:36:04 -0600 (MDT)
X-Mailman-Approved-At: Sat, 12 Jul 2008 15:55:41 +0200
Subject: [e-privacy] Open WiFi Owners Off the Hook In Germany
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Sender: e-privacy-bounces@firenze.linux.it
Errors-To: e-privacy-bounces@firenze.linux.it

http://news.slashdot.org/article.pl?sid=3D08/07/11/0346233
http://arstechnica.com/news.ars/post/20080710-open-wifi-network-viable-defe=
nse-against-infringement-chargeat-least-in-germany.html

Quanto detto fino ad adesso vale per i remailer di tipo I – cypherpunks

Vale solo in linea generale per i remailer di tipo II e III

Per questi è necessario l'utilizzo di un'interfaccia apposita

Uso dei remailer di tipo II mixmaster

Le interfacce possibili sono di due tipi

- per windows esistono due programmi che fanno da interfaccia grafica
- per gli altri sistemi operativi si deve usare il programma per il server usato in modo client

Uso dei remailer di tipo II mixmaster

Interfacce per Windows

- **Jack B. Nimble**
- **Quicksilver**
- **Reliable** il quale funziona anche come server

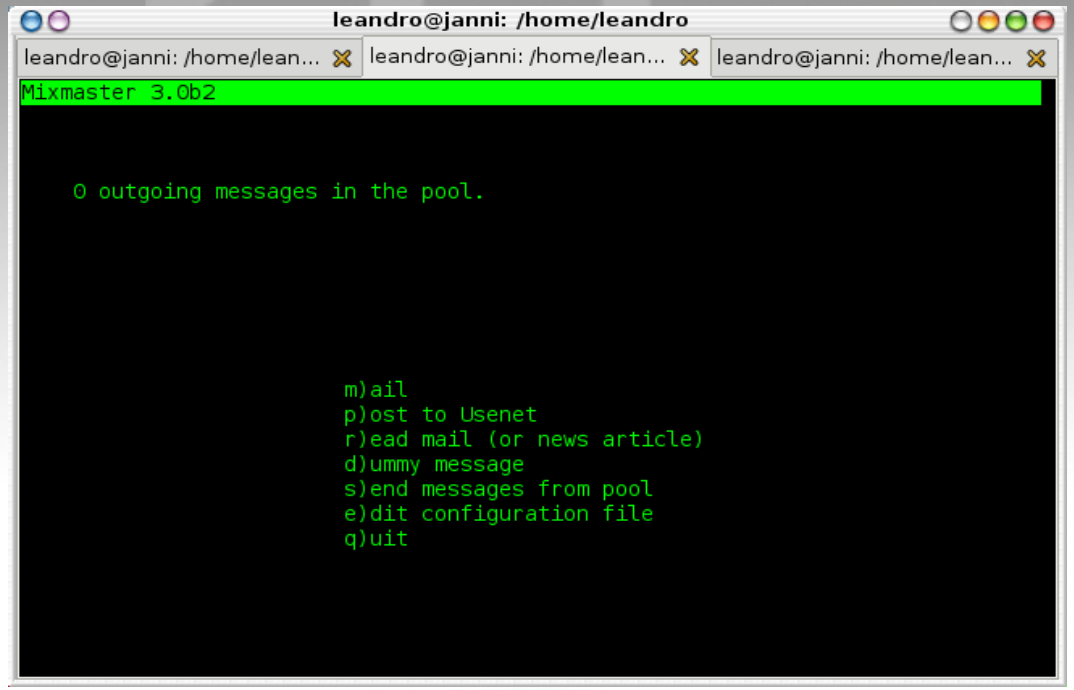
(anche se tempo fa fu pubblicato uno studio che ne rivelava le molte vulnerabilità)

Non li conosco per cui non mi ci dilungherò di più

Uso dei remailer di tipo II mixmaster

Uso del client mixmaster

codice portabile per cui gira su quasi tutti i sistemi operativi
interfaccia fatta con ncurses (per cui molto spartana)



Uso dei remailer di tipo II mixmaster

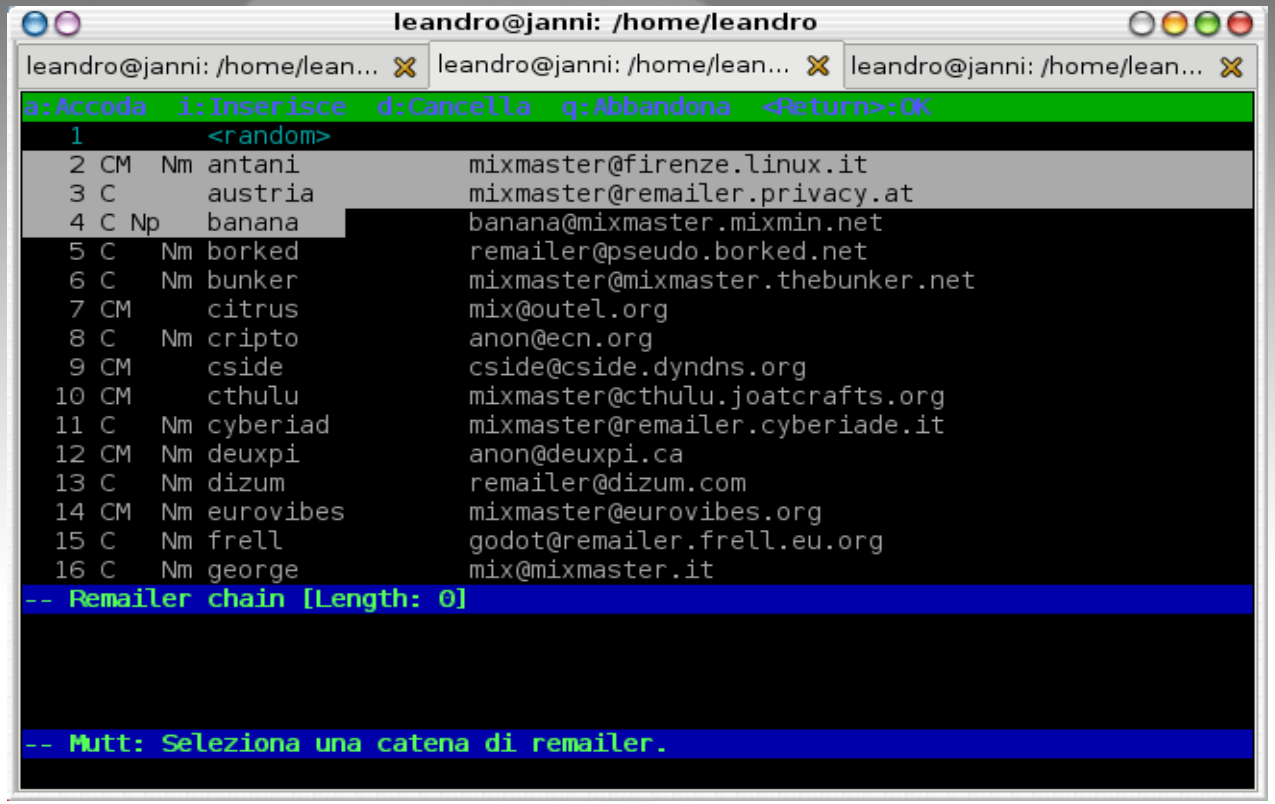
Uso del client mixmaster con mutt

mutt è un programma di posta elettronica molto ben realizzato e con molte possibilità di configurazione comprende anche una propria gestione del client mixmaster direttamente usando la versione compilata con il supporto
la versione distribuita con debian ha il supporto per mixmaster

MOCA 2008

Uso dei remailer di tipo II mixmaster

Uso del client mixmaster con mutt



LFG

Uso dei remailer di tipo II mixmaster

I pinger

•programmi che elencano e mettono a disposizione le caratteristiche della rete dei remailer

• chiavi dei remailer

• statistiche di funzionamento

• catene interrotte (broken chains)

Devono essere usati dagli utenti per scaricare queste informazioni che così possono essere usate dai client

Stato della rete mixmaster

Attualmente la rete dei remailer non è in buono stato

- sono funzionanti realmente pochi remailer (una decina)
- molti non sono seguiti con attenzione
- lo sviluppo dei remailer di tipo III è fermo
- vengono usati troppo poco

Fonti informative

newsgroups alt.privacy.anon-server e alt.privacy

lista di posta elettronica e-privacy@firenze.linux.it

sito del Progetto Winston Smith
http://www.winstonsmith.info

alcuni siti collegati ai remailer http://www.dizum.com
http://www.panta-rhei.eu.org

guide del sito degli autistici http://www.autistici.org/guide
libro Kriptonite http://www.ecn.org/kriptonite

Fonti informative

newsgroups alt.privacy.anon-server e alt.privacy

lista di posta elettronica e-privacy@firenze.linux.it

sito del Progetto Winston Smith
http://www.winstonsmith.info

alcuni siti collegati ai remailer http://www.dizum.com
http://www.panta-rhei.eu.org

guide del sito degli autistici http://www.autistici.org/guide
libro Kriptonite http://www.ecn.org/kriptonite