Untraceable Elctronic Mail, Return Addresses, and Digital Pseudonyms

Discussion of a paper by David Chaum

Albert-Ludwigs-Universität Freiburg

UNI FREIBURG

Milan David Oberkirch

Proseminar "Algorithmen für Rechnernetze"
bei Prof. Christian Schindelhauer, Sommersemester 2012

Motivation

Topic of this presentation

- untraceable mail with return-addresses
- robust pseudonyms
- immun against traffic analysis
- no absolute authority needed

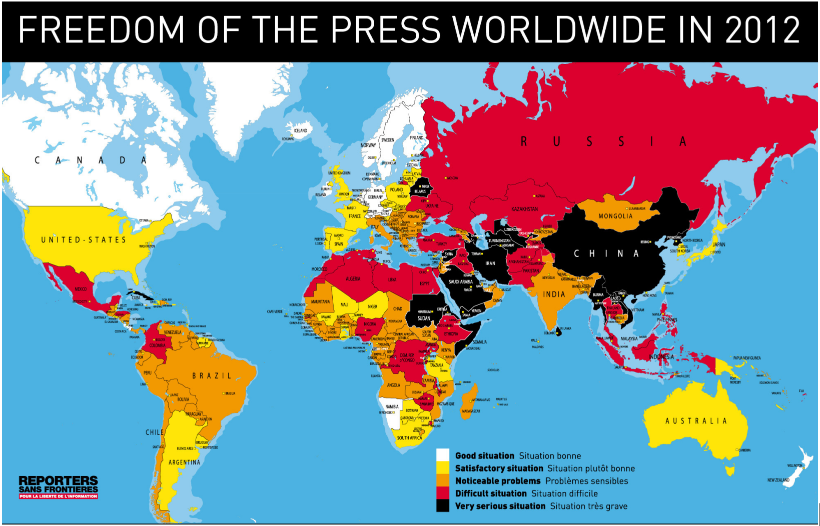
Motivation
Practical use

Why is this topic so important?

- Whistleblower
- Journalists
- Many counties have no freedem of speach

Motivation

Anonymous communication means freedom in a restricted world



[1](croped)

The paper dicussed is an important inspiration for

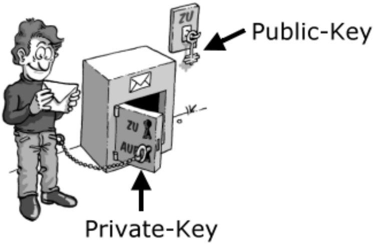
[5] [3]

Contents

RSA

a public key cryptosystem by Rivest, Shamir and Adleman[8]

- public key (K)
- private key (K^{-1})

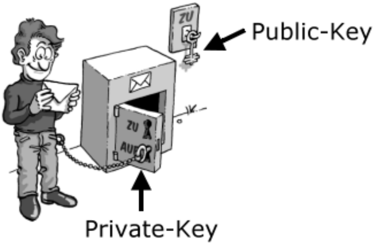


[4]

RSA

a public key cryptosystem by Rivest, Shamir and Adleman[8]

- public key (K)
  - encrypt:
    $X \rightarrow K(X)$
- private key (K^{-1})

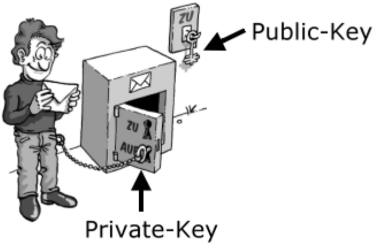


[4]

RSA

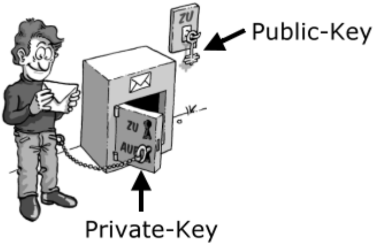
a public key cryptosystem by Rivest, Shamir and Adleman[8]

- public key (K)
  - encrypt:
    $X \rightarrow K(X)$
- private key (K^{-1})
  - decrypt:
    $K^{-1}(K(X)) = X$



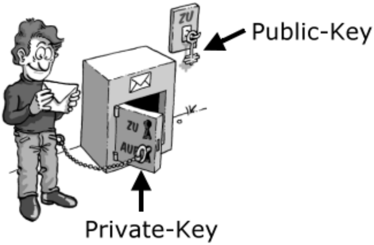
[4]

- public key (K)
  - encrypt: $X \to K(X)$
- private key (K^{-1})
  - decrypt: $K^{-1}(K(X)) = X$
  - sign messages: $X \to K^{-1}(X)$



[4]

- public key (K)
  - encrypt: $X \rightarrow K(X)$
  - verify a signature: $K(K^{-1}(X)) = X$
- private key (K^{-1})
  - decrypt: $K^{-1}(K(X)) = X$
  - sign messages: $X \rightarrow K^{-1}(X)$



[4]

Problem:

$$K(Y) = K(X) \Rightarrow Y = X$$

UNI FREIBURG

Problem:

$K(Y) = K(X) \Rightarrow Y = X$

Solution:

Use a random string R to encrypt:
$X \rightarrow K(R, X)$ (X is *sealed* with K)

1. Encrypted Mail

Alice $\xrightarrow{K_{Bob}(R, m)}$ Bob

1. Encrypted Mail

Alice $\xrightarrow{K_{Bob}(R,\, m)}$ Bob

2. hide Allice's identity from anyone but Joe

Alice $\xrightarrow{K_{Joe}(R_1,\, K_{Bob}(R_0,\, m),\, A_{Bob})}$ Joe $\xrightarrow{K_{Bob}(R,\, m)}$ Bob

1. Encrypted Mail

Alice $\xrightarrow{K_{Bob}(R,\, m)}$ Bob

2. hide Allice's identity from anyone but Joe

Alice $\xrightarrow{K_{Joe}(R_1,\, K_{Bob}(R_0,\, m),\, A_{Bob})}$ Joe $\xrightarrow{K_{Bob}(R,\, m)}$ Bob

3. Untreacable Mail

Alice $\rightarrow M_n \rightarrow M_{n-1} \rightarrow \cdots \rightarrow M_2 \rightarrow M_1 \rightarrow$ Bob

Untreaceable Mail

Alice $\rightarrow M_n \rightarrow M_{n-1} \rightarrow \cdots \rightarrow M_2 \rightarrow M_1 \rightarrow$ Bob

Allice prepares message m before sending:

1. encrypt m for Bob:
   $K_{Bob}(R,\ m)$

Untreaceable Mail

Alice $\rightarrow M_n \rightarrow M_{n-1} \rightarrow \cdots \rightarrow M_2 \rightarrow M_1 \rightarrow$ Bob

Allice prepares message m before sending:

1. encrypt m for Bob:
   $K_{Bob}(R, m)$
2. encrypt m for M_1:
   $K_{M_1}(R_1, K_{Bob}(R_0, m), A_{Bob})$

Allice prepares message m before sending:

1. encrypt m for Bob:
   $K_{Bob}(R, m)$
2. encrypt m for M_1:
   $K_{M_1}(R_1, K_{Bob}(R_0, m), A_{Bob})$
3. kepp on encrypting for the rest of the cascade:
   $K_{M_n}(R_n, K_{M_{n-1}}(R_{n-1}, \ldots K_{M_1}(R_1, K_{Bob}(R_0, m), A_{Bob}) \ldots))$

Untreaceable Mail

Alice $\rightarrow M_n \rightarrow M_{n-1} \rightarrow \cdots \rightarrow M_2 \rightarrow M_1 \rightarrow$ Bob

Sending the message to Bob:

[2]

Alice $\rightarrow M_n \rightarrow \cdots \rightarrow M_2 \rightarrow M_1 \rightarrow$ Bob

Currently we may have

- correspondences between size and time of in- and output
- items send twice being represented as two identical packets on the output

UNI FREIBURG

Currently we may have

- correspondences between size and time of in- and output
- items send twice being represented as two identical packets on the output

Solution

1. wait for a defined amount of items and order them lexikoraphically
2. seal the ordered batch with a unique random string

Untreaceable Mail

Conclusion

- There is no observable relation between in- and output of a mix
- Since Allice can send the message looking like the output of a mix, none can identify the sender
- Since one mix only finds out the adress of the next mix none can reconstruct the whole cascade

Korollar

Any single constituent mix is able to provite the secrecy of the entire cascade of mixes.[7]

Give Bob a return address:

[2](modified)

Alice $\rightarrow A_n \rightarrow A_{n-1} \rightarrow \cdots \rightarrow A_2 \rightarrow A_1 \rightarrow$ Bob

[2](modified)

[2](modified)

Problem

1. Allice does not know who send/modyfied the answer.
2. Bobs Answer is visible to anybody.

[2](modified)

Problem

1. Allice does not know who send/modyfied the answer.
2. Bobs Answer is visible to anybody.

Solution

1. Sign.
2. Encrypt.

Still not perfect

blocking all but one message

The “n-1-attack”[6]

1. block all messages but one, replacing the others
2. watch your output and see where the unknown item disappears

There exists no general applicable method, in order to prevent this attacks. (. . .)The MIX has [to] ensure that the messages he receives are sent by enough different users and so the attacker doesn’t control a majority of them. [6]

A solution to the traffic analysis problem has been presented that allows any single intermediary to provide security for those messages passing through it. In addition, the solution allows messages to be sent or received anonymously [or pseudonymsly].[7]

A solution to the traffic analysis problem has been presented that allows any single intermediary to provide security for those messages passing through it. In addition, the solution allows messages to be sent or received anonymously [or pseudonymsly].[7]

`Thank you for your attention! Are there any questions?`

References I

[1] Freedom of the press worldwide in 2012. http://en.rsf.org/IMG/jpg/carte2012-2.jpg (June the 26th, 2012).

[2] Heirat in russland, deutschland oder dänemark. http://www.frauen-osteuropa.info/heiraten-wo.html (June the 26th, 2012).

[3] Jondo – ip changer proxy programm. http://anonymous-proxy-servers.net/en/jondo.html (June the 26th, 2012).

[4] Personal web ground of silvan schmid: Gnupg. http://www.silvanschmid.com/gnupg.php (June the 26th, 2012).

References II

[5] Tor project: Anonymity online. https://www.torproject.org/ (June the 26th, 2012).

[6] Oliver Berthold, Andreas Pfitzmann, and Ronny Standtke. The disadvantages of free mix routes and how to overcome them. In **International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability**, pages 30–45. Springer-Verlag New York, Inc., 2001.

[7] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. **Communication of ACM**, 24(2):84–90, February 1981.

[8] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. **Communication of ACM**, 26(1):96–99, January 1983.