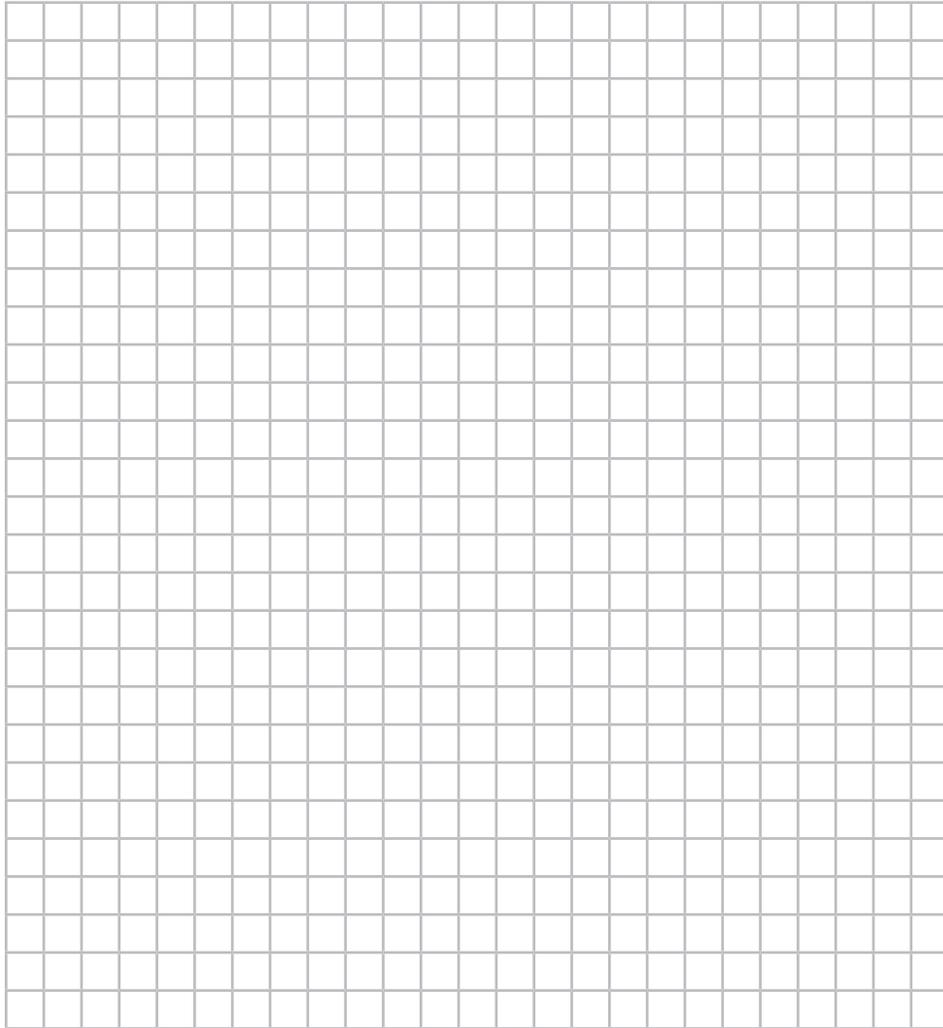


Notizen:



Veranstalter



ANTI-PRISM-PARTY

4. Staffel



- STATION NR. 0 -
SICHERE E-MAIL AM PC UND MIT DEM SMARTPHONE

SICHERE E-MAIL AM PC UND MIT DEM SMARTPHONE

Welches Problem wird gelöst?

- E-Mails sind noch immer DAS Kommunikationsmittel im Internet.
- E-Mails können gut und gerne durch 4 Länder, 3 Provider, zwei Unterseekabel und einmal um die Welt geleitet werden – auch wenn Sie diese nur an Ihren Nachbarn senden.
- Eine unverschlüsselte E-Mail ist wie eine Postkarte.
- Man kann E-Mails aber auch „sicher“ versenden, so dass der Inhalt vertraulich bleibt und der Empfänger sicher sein kann, von wem die Nachricht versandt wurde.
- Erfahren Sie an der Station 0, wie man in vier Schritten sichere E-Mail einrichtet
 - für einen Laptop oder PC (egal mit welchem der folgenden drei Betriebssysteme Sie arbeiten: Windows, MacOS, Linux); oder
 - für ein Smartphone unter Android oder iOS.

Wo gibt es gute Anleitungen im Netz?

- <https://support.mozillamessaging.com/de/home>

Anleitungen

- http://www.thunderbird-mail.de/wiki/Mailverschl%C3%BCsselung_mit_S/MIME
- S/MIME mit X509-Zertifikaten:
<http://computer.david-froehlich.de/smime/>

Liste von freien Softwarealternativen (auch zur Verschlüsselung)

- <https://prism-break.org/>

11 Minuten Turbo-Zeichnung für Zweifler und Gleichgültige

- <https://www.youtube.com/watch?v=iHlzURb0WI>

Wie heißt die Lösung? Wo kann sie bezogen werden? Welche Alternativen gibt es?

E-Mail-Client Thunderbird

- Thunderbird (<http://www.mozilla.org/de/thunderbird/>)
 - für Windows, MacOS, Linux
 - kostenlos und Open-Source

Optionales Thunderbird Add-on (Erweiterung)

- Encrypt-if-Possible: Automatisch wird „Verschlüsseln“ eingestellt, wenn man von allen Empfängern deren Zertifikat mit dem öffentlichen Schlüssel hat.
(<https://addons.mozilla.org/de/thunderbird/addon/encrypt-if-possible/>)

Alternative zu Thunderbird: Outlook:

- Mailclient von Microsoft für Windows mit fast gleicher Bedienung und ebenfalls eingebauter S/MIME-Funktionalität.

Alternative zu S/MIME:

- Open PGP

Was sind die Grenzen der Lösung?

- Jeder Kommunikationsteilnehmer braucht ein Zertifikat und einen E-Mail-Client [anstatt mit Web-Browsern zu mailen].
- Zertifikate gibt es kostenlos, aber man muss alle ein bis drei Jahre wieder ein neues beantragen.
- Geht eine E-Mail an mehrere Empfänger, kann man nur verschlüsseln, wenn man von allen Empfängern ein Zertifikat hat.
- Man muss dem (Open-Source-)Hersteller vertrauen, dass keine Hintertüren eingebaut sind. [Dann gelangt korrekterweise nur der öffentliche Schlüssel ins Internet, z.B. wenn man ein Zertifikat beim Trustcenter beantragt.]
- Die Benutzerfreundlichkeit der aktuellen Lösungen für sichere E-Mail lässt leider sehr zu wünschen übrig. Deshalb gibt es auf der Downloadseite der Anti-Prism-Party eine Schritt-für-Schritt-Anleitung, mit der Sie es z.B. für den E-Mail-Client Thunderbird in einer 1/4 h selbst einrichten können.



Alle Links finden Sie auch unter:
www.anti-prism-party.de/downloads