# EMAIL-VERSCHLÜSSELUNG

Emails bieten einen komfortablen Weg der Kommunikation, zum Austausch von Texten, zur Abmachung von Plena, Terminen, Aktionen. Doch Emails haben einen grossen Nachteil: sie sind wie Postkarten, also das was draufsteht, kann von jedem Menschen gelesen werden, der die Postkarte in die Hand bekommt. Und so wie Postkarten von einem Menschen zum nächsten weitergereicht werden, werden auch Emails von einem Server zum nächsten weitergereicht. Eine Möglichkeit, die Informationen in den Emails zu schützen, ist Email-Verschlüsselung. Dabei wird der Inhalt der Emails so verschlüsselt, dass nur die Person mit dem passenden Schlüssel die Informationen wieder entschlüsseln kann. Wenn die Repressionsbehörden dann irgendwo versuchen, in das Email hineinzuschauen, wenn es gerade auf dem Weg zu der Person ist, sehen sie nur einen langen Buchstaben- und Zahlensalat.

### Public-Key Verfahren

Als Public-Key Verfahren (Verfahren mit öffentlichem Schlüssel) oder asymmetrischer Verschlüsselung wird ein System bezeichnet, bei der jede Person, die verschlüsselt kommunzieren will, zwei zusammengehörige Schlüssel, einen öffentlichen (public) & einen geheimen (secret) besitzt. Ein Schlüssel ist in diesem Zusammenhang eine Datei mit einer langen Buchstaben- & Zahlenkombination. Der eine Schlüssel ist zum Verschlüsseln von Daten. Dieser Schlüssel kann & soll weitergegeben werden, um anderen Personen das Verschlüsseln zu ermöglichen und ist somit der öffentliche Schlüssel. Der andere Schlüssel ist zum Entschlüsseln da. Dies ist der geheime Schlüssel und der ist passwortgeschützt. Wenn nun Daten mit dem öffentlichen Schlüssel verschlüsselt werden, können sie nur noch mit dem geheimen Schlüssel entschlüsselt werden.

### Anna & Arthur verschlüsseln

Anna & Arthur beschliessen zu verschlüsseln. Beide erstellen sich ein Schlüsselpaar und schicken sich dann gegenseitig die öffentlichen Schlüssel per Email zu. Um zu überprüfen, ob die Schlüssel auf dem Weg nicht verändert wurden und ob der Schlüssel wirklich von der betreffenden Person ist, treffen sie sich und geben sich gegenseitig den Fingerabdruck des Schlüssels. Der Fingerabdruck ist eine Zeichenkette, die für jeden Schlüssel eindeutig ist. Damit überprüfen sie den öffentlichen Schlüssel des/der anderen auf Übereinstimmung mit dem Fingerabdruck. Nun schreibt Anna ein Testmail und verschlüsselt dieses mit dem öffentlichen Schlüssel von Arthur. Sobald sie das getan hat, kann das Email nur noch von Arthur entschlüsselt werden. Arthur bekommt das Mail und entschlüsselt es mit seinem geheimen Schlüssel. Nun schreibt er zurück und verschlüsselt das Mail an Anna mit dem öffentlichen Schlüssel, den er von Anna bekommen hat. Sobald er das getan hat, kann das Email nur von noch Anna entschlüsselt werden. Er schickt ihr das Email und Anna entschlüsselt es mit ihrem geheimen Schlüssel.

Jedoch Achtung, es wird nur der Inhalt der Email verschlüsselt, nicht jedoch die Adressfelder oder die Betreffzeile. Für die Repressionsbehörden ist es mittels Überwachung weiterhin möglich herauszufinden, wer wann wem ein Email geschickt hat. Sie wissen halt nur nicht, was drin steht.

### Anna & Arthur signieren

Das Public-Key Verfahren bietet aber noch einen weiteren Vorteil. Bei Emails ist es ja so, dass der/die AbsenderIn nicht wirklich überprüft werden kann. Ihr könnt ja auch einfach bei einem Mail von euch einen anderen Absender angeben. Es kann auch jeder & jede eine Emailadresse für ein Pseudonym erstellen, das von jemand anderem verwendet wird und sich so als jemand anderes ausgeben. Mit dem privaten Schlüssel kann das Email signiert werden. Dabei wird an den Text der Email eine Signatur angehängt, eine kurze Kette aus Zahlen & Buchstaben, die aus dem Inhalt der Email und dem privaten Schlüssel errechnet wird. Somit kann die Empfängerin der Email überprüfen, ob das Email während des Transportes verändert wurde und ob das Email wirklich von der AbsenderIn kommt.




### Anna vertraut Arthur vertraut Anton vertraut Akira

Natürlich ist es kaum möglich, sich persönlich mit allen, mit denen mensch weltweit per Email kommuniziert, auch persönlich zu treffen um Fingerabdruücke auszutauschen. Deswegen gibt es ein 'Web Of Trust', ein Netz des Vertrauens. Das bedeutet folgendes: Anna vertraut der Signatur von Arthur. Sie signiert nun seinen öffentlichen Schlüssel (und umgekehrt). Arthur vertraut wiederum Anton und signiert dessen öffentlichen Schlüssel (und umgekehrt). Und Anton vertraut Akira und signiert ihren öffentlichen Schlüssel (und umgekehrt). Somit kann auch Anna darauf vertrauen, dass die Signatur von Akira wirklich die von Akira ist.

### Keyserver

Da es mühsam ist, immer erst wegen des öffentlichen Schlüssels anzufragen, um einer Person ein verschlüsseltes Email schicken zu können, haben sich mit der Zeit sogenannte 'Keyserver', also Schlüsselserver, verbreitet. Grössere Organisationen oder Gruppen haben solche Schlüsselserver, wo jeder & jede dann den eigenen öffentlichen Schlüssel hochladen kann, damit ihn andere runterladen können. Teilweise bilden diese Schlüsselserver auch ein Netzwerk und tauschen die hochgeladenen Schlüssel untereinander aus, damit die BenutzerInnen nicht so viel suchen müssen (zum Beispiel die sks-keyserver, siehe Link am Ende des Flyers).

Am Keyserver könnt ihr einfach mal nach Schlüsseln suchen, da seht ihr auch, welche Schlüssel von welchen anderen Schlüsseln signiert wurden.

### Revocation/Zurückziehen von Schlüsseln

Am Anfang, wenn ihr euch euer Schlüsselpaar generiert, macht euch bitte auch ein Widerrufszertifikat. Das braucht ihr, falls euer Schlüssel kompromittiert wurde (also wenn die Bullen den Schlüssel haben oder ihr das Passwort verloren habt oder ähnliches). Dieses Zertifikat bitte auch irgendwo sicher verwahren (verschlüsselt auf einer extra Festplatte z.B.). Im Falle des Falles ladet ihr das Widerrufszertifikat auf einem Keyserver hoch. Wenn andere AktivistInnen dann ihren Schlüsselbund über einen Keyserver aktualisieren, wird euer Schlüssel automatisch deaktiviert. Um zu sehen ob andere etwas an ihren Schlüsseln verändert haben, solltet ihr wöchentlich euren Schlüsselbund aktualisieren (alle eure Schlüssel gemeinsam heissen Schlüsselbund).

### Tipps zu Email Verschlüsselung

Schützt euren privaten Schlüssel. Legt ihn nur auf eurem privaten Laptop ab, von dem ihr ja sicherlich die Festplatte verschlüsselt habt und macht irgendwo eine Sicherungskopie die ihr möglichst zugriffsgeschützt aufbewahrt. Verwendet eine starke Passphrase.

Verwendet gewöhnliche Betreffzeilen & verschlüsselt auch Emails, deren Inhalte nicht geheim sein müssen! Setzt euch mit FreundInnen gemeinsam zusammen und signiert gegenseitig eure Keys (das nennt sich dann Keysigining-Party). Macht euch kleine Papierschnipsel, wo euer Schlüsselfingerabdruck draufsteht, die ihr dann immer mithaben könnt um sie auszutauschen. Aber Achtung: falls ihr für die politische Arbeit ein eigenes Pseudonym mit eigener Email Adresse verwendet, kann eine Verbindung zwischen euch & eurem Pseudonym geschaffen werden, wenn ihr mit dem Fingerabdruck des Schlüssels in Verbindung gebracht werdet. Deswegen z.B. den Fingerabdruck nicht über Telephon sagen, wenn die Möglichkeit besteht, dass ihr abgehört werdet.

Euer Geheimer Key ist zwar was sehr privates, jedoch ist das kein Grund einen Bund fürs Leben einzugehen. Solche Keys haben ein Ablaufdatum, das ihr beim Erstellen setzen könnt. Wählt das nicht zu weit in der Zukunft.

### Die Software

Als Standard zum Verschlüsseln hat sich im Laufe der Zeit OpenPGP herauskristallisiert. Unter den meisten Betriebssystemen gibt es das Programm GPG (Gnu Privacy Guard), das diesen Standard implementiert. Wenn ihr das Email Programm Thunderbird verwendet, dann gibt es dafür eine Erweiterung namens Enigmail, die dafür da ist, euch das Ver/Entschlüsseln, Signieren von Emails und das Verwalten von Schlüsseln zu vereinfachen.

Es gibt auch verschlüsselte Mailinglisten. Eine Software, die so etwas mittels GPG möglich macht, ist 'Schleuder'. Falls ihr verschlüsselte Mailinglisten verwenden wollt, könnt ihr euch an das Technikkollektiv immerda.ch oder an nadir wenden, die bieten Schleuderlisten an, auch das Kollektiv tachanka.org wird das bald anbieten.

Keyserver des Mayfirst Kollektives:
**https://zimmermann.mayfirst.org/**
Keyserver des Indymedia Netzwerkes:
**https://keys.indymedia.org**
Text vom Riseup Kollektiv zu Email Verschlüsselung (Englisch):
**https://help.riseup.net/security/encrypted-email/**
OpenPGP Best Practices der Riseup Labs Privacy and Authenticity Outreach Workgroup (Englisch)
**https://we.riseup.net/riseuplabs+paow/openpgp-best-practices**
Technikkollektiv immerda
**https://www.immerda.ch**
Liste der sks Keyserver
**http://sks-keyservers.net/status/**

tear the system down - bit. by. bit. mailto:bitbybit@riseup.net
technologie in linksradikalen kontexten irc://irc.indymedia.org/#bitbybit