Förderverein Bürgernetz

(eMail-)Verschlüsselung

Rüdiger Zwarg

Nach diesem Vortrag werden Sie...

- den Unterschied zwischen symmetrischer, asymmetrischer und hybrider Verschlüsselung kennen.
- eine Idee haben, was es mit den Verschlüsselungsverfahren AES und RSA auf sich hat.
- Programme kennen, mit denen Sie…
  - Zertifikate/Schlüsselpaare erzeugen können
  - eMails verschlüsselt versenden können
  - Dateien verschlüsseln können

Immer geht es dabei...

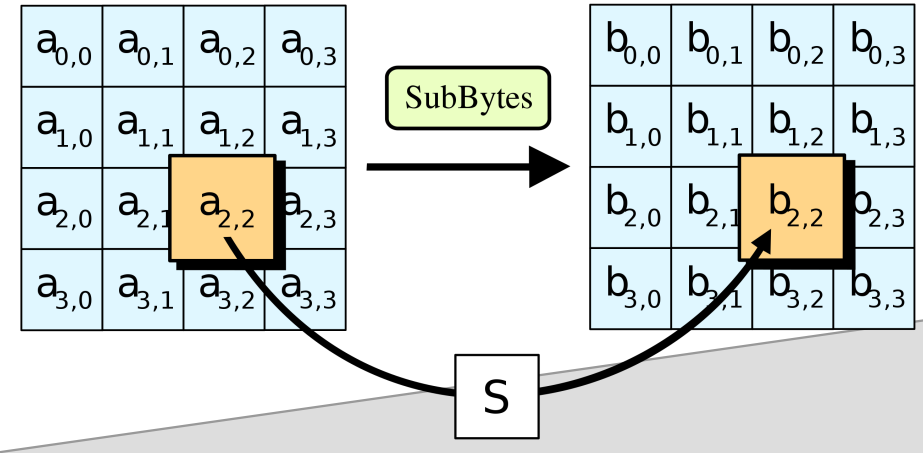
- **um das Versenden an andere Personen**
- nicht um das Verschlüsseln von Speicherdaten auf dem eigenen PC
  - Empfehlung zur Speicherung vertraulicher Daten/Dokumente:
    - Keepass XC » wegen der Ordnung/Systematik
      (ansonsten gibt es eine Vielzahl kostenloser Verschlüsselungsprogamme)

Immer geht es dabei...

- **um das Versenden an andere Personen**
- nicht um das Verschlüsseln von Speicherdaten auf dem eigenen PC
  - Empfehlung zur Speicherung vertraulicher Daten/Dokumente:
    - Keepass XC » wegen der Ordnung/Systematik
      (ansonsten gibt es eine Vielzahl kostenloser Verschlüsselungsprogamme)

Symmetrische Verschlüsselung

- Der Advanced Encryption Standard (AES) ist seit 2002 Nachfolger des Data Encryption Standard (DES) und gilt als pragmatisch sicher. Für höchsten Geheimhaltungsgrad zugelassen
- Der Algorithmus wurde von Joan Daemen und Vincent Rijmen unter der Bezeichnung Rijndael entwickelt.
- AES ist eine Blockchiffre



Eigenschaften von AES

- sicher
- schnell
- Standard!

Problem:

- Der Schlüsselaustausch erfordert einen Medienbruch, um sicher zu sein.
- Und ein Schlüsselaustausch muss überhaupt erstmal verabredet und durchgeführt werden

Eigenschaften von RSA

- sicher bei entsprechender Schlüssellänge
- einfacher Schlüsselaustausch
  (Best Practice: grundsätzlich öffentlichen Schlüssel in Signatur angeben)
- Standard!

Nachteile:

- eher langsam
- verschlüsselbare Daten auf weniger als die Schlüssellänge begrenzt
  (Daher meist/immer als hybride Verschlüsselung realisiert)

Was ist RSA?

- Assymetrische Verschlüsselung besteht aus einem öffentlichen und einem privaten Schlüssel. Die Idee ist (relativ) neu.
- 1976 veröffentlichen Whitfield Diffie und Martin Hellman eine Theorie zur Public-Key-Kryptografie
- Den drei Mathematikern Rivest, Shamir und Adleman gelingt es, Annahmen von Diffie und Hellman zu widerlegen. Im Rahmen dieser wissenschaftlichen Arbeit am MIT stießen sie auf ein Verfahren, bei dem sie keinerlei Angriffspunkte fanden. Hieraus entstand 1977 RSA, das erste veröffentlichte asymmetrische Verschlüsselungsverfahren.
- Bereits Anfang der 1970er Jahre war von den Briten Ellis, Cocks und Williamson ein ähnliches asymmetrisches Verfahren entwickelt worden, welches aber aus Geheimhaltungsgründen nicht wissenschaftlich publiziert wurde. RSA konnte also patentiert werden (2000 abgelaufen).
- Grundsätzlich beruht das Verfahren auf der Zerlegung einer sehr großen Zahl in zwei sehr große Primzahlen

Fragen?

...vor Beginn des Praxisteils

Beginn des Praxisteils

Woher der öffentliche Schlüssel?

Eher unpraktisch:

- Klartext in der Signatur jeder Mail
- Textdatei als Anhang jeder Mail

ganz OK:

- Senden auf Anforderung (Austausch ohne Sicherheitsrisiken)

Besser:

- Eintrag in ein öffentliches Verzeichnis (d.h. Link in der Signatur)
- Speichern in der eigenen Website (d.h. Link in der Signatur)

Schlüsselverzeichnisse

- https://keys.openpgp.org (keine Namenssuche)
- https://keyserver.ubuntu.com
- https://pgp.mit.edu
- https://keyserver.pgp.com
- http://cryptonomicon.mit.edu/
- http://pgp.net.nz:11371/
- http://zuul.rediris.es:11371/
- http://pgp.cyberbits.eu:11371/
- http://sks.pod02.fleetstreetops.com:11371/
- http://sks.pod02.fleetstreetops.com:11371/

Beim Eintrag sollte man nicht nur die Bekanntheit des Servers in Betracht ziehen, sondern sich z.B. auch überlegen, ob man mit Namen oder nur mit eMail gefunden werden will.

öffentlicher Schlüssel

https://keys.openpgp.org/vks/v1/by-fingerprint/46A9621A7A34899538DDC402A5406889EDCDA92C

46A9621A7A34899538DDC402A5406889EDCDA92C.asc

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: 46A9 621A 7A34 8995 38DD  C402 A540 6889 EDCD A92C
Comment: Alice Smith (test key) <dcc-support@sib.swiss>

xsFNBGK7A9sBEADa52UzP0XM0i1wVVxbVCJx87xqEoYY02niOdG2QQEi0bq4d62g
/UwIP68lqUgsrmeEjpJJE8H8NOXmdkJk6dbT1JgHeLh34xS5ykpbVls53GFxIVnT
Fyye9DZMF6cvV95J3HgaSTSJdDa8Twh0htHoKsATZpt+pXI+sahjD0hb+r0pjXe2
UyN/bY1Ux9F6L9eoILcYyY81G0Ft24ybpjDSwi0I4uwybcQzjv84aOGJswvJx+Xr
QTRtQ1QOszDaPjsOCS1NOStnQ5HB5c7jSey0SliJ6duVojTHL9YU53rybs1RaBY5
w3ZcW3kycR/SRc+cEbDs0aZsW8lu+zjpbMBz05MQ9IkaOtKLo3i7Z9Pdx5vyblBX
8ldHL0ylXP7xyqqv7V7riuJ5CBhqh6FxgXlw8QvYfQ3c5n+eTONTjeMS5CdUTbr3
EleuvlvMrEyD9kpsY9Y6tIMaSqgny8SDfC1D8meJgS8ALePCPCxCVrYkwTAhEkqR
JQyClu8qOF7008k/ul04RdUowXdogYLQ/yQ92E1S3jBqhDpyJvOV+yzDpNhV3dB8
+bJqM3xdn0NITto36YWB6/hiQfA4sgVgcaysllsPuUvToU39Q/DBboq70Ndu4dNg
FqAdiUleWLNDAh4vBeEB2qswWtUeLUldQ5CLtYBQjvmTHaAsFnOFuCZaPQARAQAB
zS5BbGljZSBTbW10aCAodGVzdCBrZXkpIDxkY2Mtc3VwcG9ydEBzaWIuc3dpc3M+
wsGOBBMBCgA4FiEERqliGno0iZU43cQCpUBoie3NqSwFAmK7A9sCGwMFCwkIBwIG
FQoJCAsCBBYCAwECHgECF4AACgkQpUBoie3NqSyi9BAAhTPl9Y3XCtev6HNdbuRy
pyRs+aLcYXFlXthiCCScMrnXygXGMoLqWPzzb6x8KLV96a4nWbE3HXaqRyTqrPiQ
UYxqz9qzJdtMBSdDP21TWnQMRflkmax+pEQHkyU8+aeBdWbKoNfkWaDnxaJD899i
te3r6y5eJEogjkhtGC0vSPVqCxLubv3/qqsPfv8XWKLhlaLUCdS+k3i/cdN8AoSA
oCjlxbew3MN0KG+Y7q0Zh74sOlLl8BqzYmwpF3lK817JPzng6bCao0m/HpmKWuPI
GEumwXagiBMJbTtmvS7maHqn88pTdRd+G5yVCzPt5LtcZM2lwnbvxgqiO3CRylPJ
/SvQjNEh8zCWifsrlG96B5D5Yj4Bgmq5J9ApZw2JjhOTmYHkt3qtfimbDgwTeKKV
UvfJLfKrT660EEpKU7TJPOQMmcXYlgiCn8aki4qBokBCa09BNg5bUptgBtq6Hzrw
CGfBXcMcB3Y6ZSzEck73O5VwP2r/GTI8ioda7bOFbaipLWxDpxNa5kZH03h41tEt
lAYlqWW5dA8m2WEbvNkbm4S2GqqVXmLFVf2vdAxf6PTa+GpWb2N16wTIZOXipPrr
611l32cH1ZrWYI5fGyj7J0GGeLYuKSCXCX8nFjpRlQ3sEAR2S1TP3bFCCRmn2fy0
gawiiBUmFAy7vOMBcuiYYpS1fXYWr8RM4BDvmlu5kdV9BVXZrwp7lnZkrlBPoztk
bZ5qy/ZE8x2V/a5VsnQUsHgMaGCmVt2UaOrabluWDiGVYjqRf6f7cTQZX1Brv+IQ
yvY7vwQR3FbmSk7m2RTKqKVnBTEB/TkMb7Rg4VggOMe9wf6yicoqqA+lChNDruL+
9OqqezPLsYzitf76bVWvrhbyuV+7xG6BrxknGnTKS6AQrjgfE1U+IGJg2dyDo679
rs2I6M8QDgAiCliwWaQXvFbShMYXUlI2wlhMUOAk7wQsYzQ9i5NlivlemctmiFgH
AbD+x2wlfkvjuCpWpQNXT+DCh9inNaLfKo9RXzR/XHbHCVvpzVU8ER8iE+GVUanG
K+hM3MRx7Y8nvGSnJI6tlrm6Y8I8HvnBufr4M84oozhQWvdVynHrMwVKQ+lFiZo9
GI8Z4t2UlbQjnetDABEBAAHCwXYEGAEKACAWIQRGqWIaejSJ1TjdxAKlQGiJ7c2p
LAUCYrsD2wIbDAAKCRClQGiJ7c2pLM9kEACeQR6JdpcxlESOzR+BPVUFfuT7oOpQ
olGfZBWzT937q2iyrTVybS5xnC9Mml2thBjXwM5KX+tr5lQpdRxM5pvnvc4KwMlM
afSlwg+Tcl3gjuFGgntj64XdpPSWAKdIz9Wb7gIqfX59reIbPrZekqH9h6y7eAIk
5I/nKvk2V0ylB+qk+93n+Jy42c/GVcloXOhKe+lfEEJnv5a3ASLiVcfeuzlqXihR
rCeQcbaQsoXM2BSBtxitThRwgNlXMN3/aFLVEzcrWKCfB7TJalfYzduyqnfW//CZ
Ts6NCU1lKqsK/V8TCnvaxDHfvXqELh+d3Q4RpN1PBwbzEYwoEauXXctyuJm6P5M+
H/PzywzBYsJv5XrO9AHx7Ibne+PpTY3I5Z8hWyWZlENBRiMXJhR1tl+OGrYMfRzs
UlqwvasdWbkLg9ZM/uJf2O5VAbtMLiVnXfKBqhXTHuBuQxUDTR9wkBLfWeuAYXoC
QftN8knB0JwQLYfIpiTkBTQtMlcfIafb6p+WuAPJGftai3zOS95PSyFawylHNie4
THHp2SNfqkP5ml7TdK6yxDu6047dZlaPVBo2MEE3V98AqPcGU7M+t6wOLNQeOd94
ElW78oNkwUJRrcMr/rrX+Z/DIZw+LMD7vAqtsfMy50lOaaeKLVBHMB/fN1KCfo6n
czxH0wwuD7Yhbg==
=ycK8
-----END PGP PUBLIC KEY BLOCK-----
```

öffentlichen Schlüssel verifizieren

Fingerabdruck:

- Der Fingerabdruck ist nicht nur ein Hashcode des Schlüssels. Zusätzlich fließen noch Metadaten, Zeitstempel etc. ein. Es wäre extrem schwierig, einen solchen Fingerabdruck zu fälschen.
- Den Fingerabdruck kann/sollte man in der eMail-Signatur angeben

Schlüssel-ID:

- Das sind nur die letzten paar Blöcke des Fingerabdrucks. Die Schlüssel-ID ist also nicht so aussagekräftig/sicher wie der Fingerabdruck

Muss man das?

- Zunächst einmal ist ein gefälschter Schlüssel einfach nur nutzlos und verwirrend.
- Zur Gefahr kann es nur werden, wenn zusätzlich Mails abgefangen werden.

Welche (kostenlose) Software?

Schlüsselerstellung/-verwaltung:

- Kleopatra: https://gpg4win.org/download.html
- Fortra: https://www.goanywhere.com/products
- PGPTool: https://pgptool.github.io/
- WinGPG: https://scand.de/produkte/wingpg/

eMail-Versand:

- Thunderbird (jetzt eingebaut)
- Enigmail (Client Add-On)
- Mailvelope (Browser Add-On)

Dateiverschlüsselung:

- s.o. Fortra, PGPTool, WinGPG

(kostenlose) eMail-Anbieter

- Protonmail: https://proton.me/mail/pricing
- Tuta: https://tuta.com/de/pricing
- Canarymail: https://canarymail.io/pricing.html?ref=Website
- Mailfence: https://mailfence.com/#pricing

es gibt natürlich etliche Bezahl-Anbieter und Varianten mit Mailvelope:

- z.B. Posteo (ab 1€/Monat)

Was ist eigentlich mit S/MIME?

Die kurze Antwort lautet:

Das Problem mit S/MIME ist, dass das mit den Zertifikaten/Schlüsseln nicht so einfach ist. PGP ist für den gelegentlichen, privaten Nutzer die bessere Wahl.

- S/MIME beruht auf einer Zertifikatskette an deren Spitze eine „Certificate Authority“, eine nichtstaatliche Behörde, steht.
- S/MIME und PGP sind nicht kompatibel, beruhen aber auf demselben Konzept mit asymmetrischer Verschlüsselung und öffentlichen Schlüsseln.
- Thunderbird unterstützt auch S/MIME
- Es gibt wenige CAs die (zeitlich begrenzte) Zertifikate ausstellen:
  https://www.actalis.com/s-mime-certificates.aspx (1 Jahr » Sicherheitsbedenken wg. Passwortvergabe)
  https://wiseid.com/ (3 Monate)
  http://wiki.cacert.org/CAcertInShort-de (Mitgliedschaft)

kurzes Video (Link)

mailvelope tutorial - Google Search

15.04.24
Autor: R.Zwarg