Kryptologie = Kryptografie + Kryptoanalyse

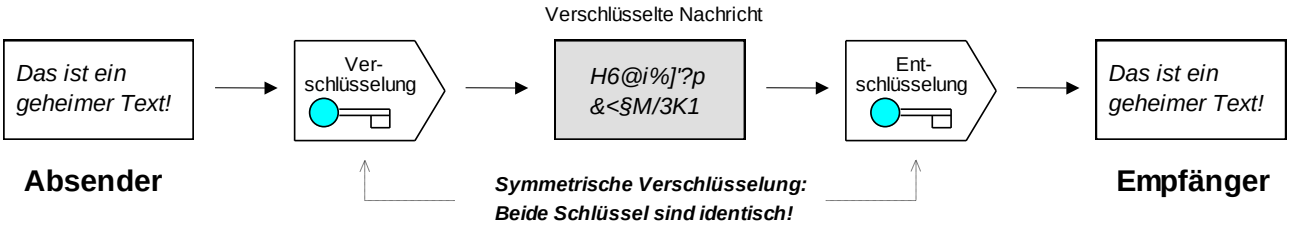
Die Kryptologie (aus dem Griechischen *kryptós* = verborgen bzw. *logos* = Lehre) ist die Wissenschaft, die sich mit technischen Verfahren für die Informationssicherheit beschäftigt und sich in die beiden Gebiete Kryptografie und Kryptoanalyse unterteilt. Die Kryptographie beschäftigt sich mit der Entwicklung und Anwendung der einzelnen Verfahren, d.h. mit der Sicherheit der eigenen geheimen Kommunikation gegen unbefugte Entschlüsselung. Die Kryptoanalyse, quasi als Gegenspielerin, hat die Informationsgewinnung aus verschlüsselten fremden Nachrichten, also das Brechen der geheimen Kommunikation zum Ziel.

Ziele der Datenverschlüsselung (Kryptografie)

- **Vertraulichkeit** der Inhalt der Nachricht ist geheim, nur Berechtigte haben Zugriff
- **Integrität** der Inhalt der Nachricht wurde nicht verändert
- **Authentizität** die Nachricht ist eindeutig vom angegebenen Absender
- **Verbindlichkeit** der Empfänger kann nachweisen, dass die Nachricht vom Absender stammt

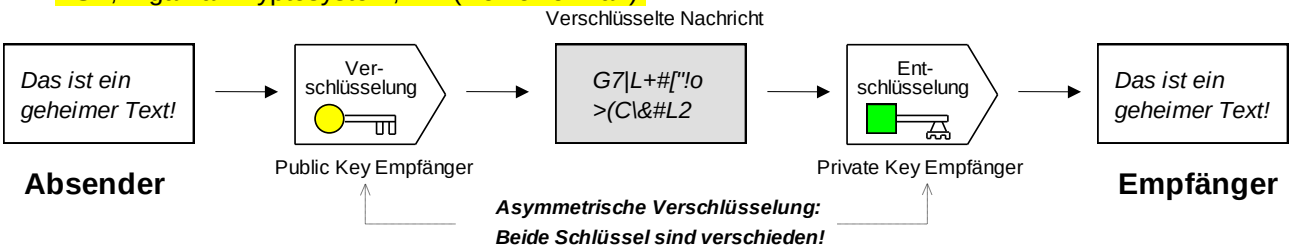
Symmetrische Verschlüsselung

Verschlüsselungsverfahren, bei denen jeweils der selbe Schlüssel für Ver- und Entschlüsselung verwendet wird z.B. DES, 3DES, IDEA, RC4/5, AES.



Asymmetrische Verschlüsselung - Public/Private-Key-Verfahren

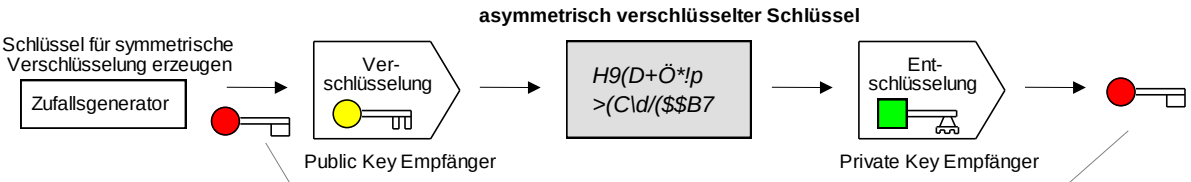
Verschlüsselungsverfahren, bei denen sich die Schlüssel für Ver- und Entschlüsselung unterscheiden. Meist wird der öffentliche *Public Key* zum Verschlüsseln, der geheime *Private Key* zum Entschlüsseln verwendet z.B. RSA, Elgamal-Kryptosystem, DH (DeffieHellman).



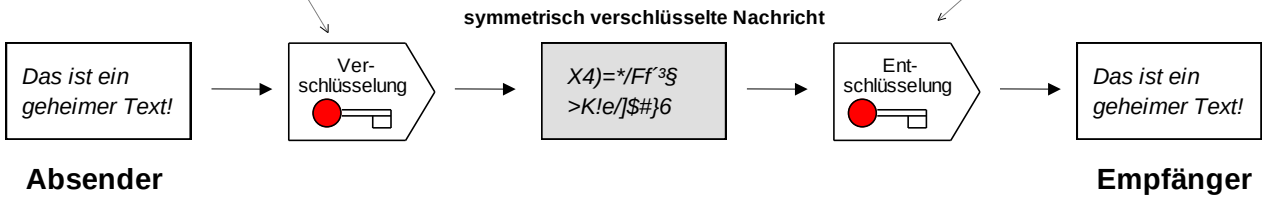
Hybride Verfahren

kombinieren die symmetrische und die asymmetrische Verschlüsselung und vermeiden jeweils deren Nachteile. Die zu übertragende Nachricht wird symmetrisch verschlüsselt. Der dafür nötige Schlüssel wird vorher asymmetrisch verschlüsselt übertragen (z.B. SSH, IPsec, HTTPS, SSL/TLS).

1. Schritt: Schlüssel für symmetrische Verschlüsselung erzeugen und diesen mit asymmetrischer Verschlüsselung übertragen



2. Schritt: Nachricht wird mit symmetrischer Verschlüsselung übertragen



Vergleich von symmetrischer und asymmetrischer Verschlüsselung

	Symmetrische Verschlüsselung	Asymmetrische Verschlüsselung
Vorteile	- nach Schlüsselübermittlung **sehr sicher** - schnell, Hardware-Lösungen erreichen über 1GBit/s	- öffenlicher und privater Schlüssel sind unabhängig voneinander, d.h. der private kann nicht berechnet werden, wenn man im Besitz des öffentlichen ist - **Schlüsselverteilungsproblem ist gelöst**, da der Transport des öffentlichen Schlüssels über einen unsicheren Kanal (z.B. Internet) unkritisch ist
Nachteile	- alle Kommunikationspartner müssen über den gleichen Schlüssel verfügen - **Schlüsselverteilungsproblem** Wie kann man einen sicheren Schlüssel über einen unsicheren Kanal (Internet?) übertragen? - für jede Übertragung zu Personen, Gruppen oder Unternehmen muss ein eigener Schlüssel angelegt werden	- 1000 ... 10000 mal **langsamer** als symmetrische Verfahren - sehr **rechen- und zeitintensiv** - Angreifer versuchen aus dem Public Key den Private Key zu berechnen, deshalb sind bei asymm. Verfahren Schlüssel mit min. 1024 Bit nötig (entspicht dann etwa der gleichen Sicherheit wie 70 Bit bei symm. Verfahren)

Schlüsselraum

Von der Länge des Schlüssels, also der Zahl der Bitstellen ergibt sich die Menge der Möglichkeiten, aus denen ein Schlüssel ausgewählt werden kann. Diese Menge nennt man *Schlüsselraum*.
Um eine hohe Sicherheit zu gewährleisten, sollte der Schlüsselraum möglichst groß gewählt werden.
Beispiel: Mit einer Schlüssellänge von 40 Bit erhält man $2^{40} = 1{,}1 \times 10^{12}$ Möglichkeiten.
Mit leistungsstarken Prozessoren oder durch den Zusammenschluss vieler Rechner (z.B. Cloud, Cluster) lassen sich mehr als 10^{11} Schlüssel pro Sekunde testen. Alle Möglichkeiten bei 40 Bit Schlüssellänge auszuprobieren, würde dann lediglich 11 Sekunden dauern.
(siehe auch www.cryptool.org/images/ct1/presentations/CrypToolPresentation-de.pdf, Seite 18)

Aufgaben

1.) Begründen Sie, warum der Public-Key bei asymmetrischen Verfahren nicht geheim gehalten werden muss. Weil man damit nur Verschlüsseln kann.

2.) Stellen Sie einige Vor- und Nachteile von symmetrischen, asymmetrischen und hybriden Verfahren gegenüber.

3.) Geben Sie die üblichen Schlüssellängen bei den oben angegebenen Verschlüsselungsverfahren an.

4.) Ein Verschlüsselungsverfahren benutzt eine Schlüssellänge von 64 Bit.

a) Wie lange bräuchte man maximal mit einem leistungsstarken Rechensystem, das 10^{11} Schlüssel pro Sekunde testen kann, um das System zu knacken?

b) Laden Sie sich das Programm LCP (www.lcpsoft.com/download/lcp504en.rar) herunter. Starten Sie das Programm und importieren Sie unter *Import--> PwDump File* die Datei PwDump03.txt. Deaktivieren Sie unter *Session -> Options* alle Methoden außer *Brute force*. Wählen Sie unter *Brute force --> character set* das Set *A-Z, 0-9* aus. Starten Sie den Angriff und geben Sie die erreichte Geschwindigkeit in Schlüssel/s an:
_____ keys/s
Wie lange würde mit dieser Geschwindigkeit das Entschlüsseln eines 1024-Bit Schlüssels maximal dauern?

5.) (APr-FQ) Ein 64-Bit-Schlüssel wird von einem Rechner in 60 Minuten entschlüsselt. Durch die Verwendung eines 78-Bit-Schlüssels soll die Zeit zur Entschlüsselung bei gleicher Rechenleistung auf mehrere Wochen erhöht werden. Ermitteln Sie die Entschlüsselungszeit in Wochen. Der Rechenweg ist anzugeben.

6.) (Kopfrechnen) Um wieviel Bit muss die Schlüssellänge mindestens erhöht werden, wenn die maximale Entschlüsselungszeit mindestens um den Faktor 100 verlängert werden soll?

Lösungen Aufgaben

1.) Begründen Sie, warum der Public-Key bei asymmetrischen Verfahren nicht geheim gehalten werden muss.

Mit dem Public-Key verschlüsselte Daten können NICHT mit dem Public-Key enschlüsselt werden

2.) Stellen Sie die Vor- und Nachteile von symmetrischen, asymmetrischen und hybriden Verfahren gegenüber.

- sym./asym. siehe Blatt!
- hybride Verfahren sind elegant aber komplizierter, evtl. mehr Softwarefehler

3.) Geben Sie die üblichen Schlüssellängen bei den oben angegebenen Verschlüsselungsverfahren an.

symmetrische	asymmetrische
DES : 56 ***3DES : 168, 112 oder 56*** ***IDEA : 128*** ***RC4 : 40 - 2048*** ***RC5 : 0 - 2040 (std: 128)*** ***AES : 128, 192 oder 256***	***RSA : 1024 - 4096***

4.) Ein Verschlüsselungsverfahren benutzt eine Schlüssellänge von 64 Bit.

a) Wie lange bräuchte man maximal mit einem leistungsstarken Rechensystem, das 10^{11} Schlüssel pro Sekunde testen kann, um das System zu knacken?

in Jahren:

*(2^64/10^11)/(60*60*24*365)=5,8Jahre*

b) Laden Sie sich das Programm LCP (www.lcpsoft.com/download/lcp504en.rar) herunter. Starten Sie das Programm und importieren Sie unter *Import--> PwDump File* die Datei PwDump03.txt. Deaktivieren Sie unter *Session -> Options* alle Methoden außer *Brute force*. Wählen Sie unter *Brute force --> character set* das Set *A-Z, 0-9* aus. Starten Sie den Angriff und geben Sie die erreichte Geschwindigkeit in Schlüssel/s an:

_____

Wie lange würde mit dieser Geschwindigkeit das Entschlüsseln eines 1024-Bit Schlüssels maximal dauern?

5.) (APr-FQ) Ein 64-Bit-Schlüssel wird von einem Rechner in 60 Minuten entschlüsselt. Durch die Verwendung eines 78-Bit-Schlüssels soll die Zeit zur Entschlüsselung bei gleicher Rechenleistung auf mehrere Wochen erhöht werden. Ermitteln Sie die Entschlüsselungszeit in Wochen. Der Rechenweg ist anzugeben.

Dreisatz: 2^64 == 60Minuten
2^78 == (60/2^64)*2^78
ca 98 Wochen

6.) Um wieviel Bit muss die Schlüssellänge mindestens erhöht werden, wenn die maximale Entschlüsselungszeit mindestens um den Faktor 100 verlängert werden soll?

7 Bit

ZEUG

in Firefox die unterschiedlichen Farben der Sicherheit beobachten
symm-Verschlüsselung
mit welchem Verfahren und welcher Schlüssellänge wird symm. verschlüsselt?

https://addons.mozilla.org/
https://www.facebook.com/login.php
https://www.bsi.bund.de/
https://webdav-ca0585-muenchen.musin.de/

Camellia: https://hisbus.his.de/hisbus/docs/hisbus21.pdf

easy filesharing webserver z.B. https://192.168.47.174/

Sperrliste http://csc3-2004-crl.verisign.com/CSC3-2004.crl

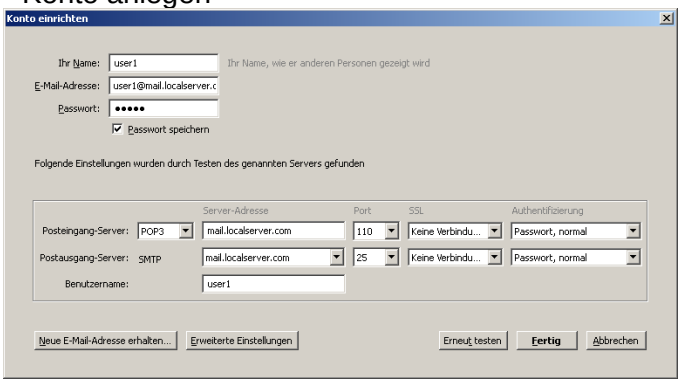
Thunderbird Portable, Enigmail and GnuPG
https://securityinabox.org/en/thunderbird_main

Portable Thunderbird with GPG and Enigmail

- Thunderbird Portable in beliebiges Verzeichnis installieren
- GPG for Thunderbird Portable in dasselbe Verzeichnis installieren
- Enigmail-Plugin (enigmail-xxx.xpi) herunterladen und mit der Maus in den geöffneten Thunderbird Portable hineinziehen

4.2 How to Generate Key Pairs and Configure Enigmail to Work with Your Email Accounts

- Konto anlegen



- Keys erzeugen
- Public-Key als Attachment jeweils an alle Anderen senden
- Public-Key importieren