



openHPI – Sicherheit im Internet
Verschlüsselungsmethoden

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Funktionsprinzip der 1-Schlüssel Verschlüsselung

Stellen zunächst vor, wie die **1-Schlüssel Verfahren** der **symmetrischen Kryptographie** funktionieren ...

- Das Ver- und Entschlüsseln einer Nachricht erfolgt mit gleichem und geheim zu haltenden Schlüssel – „**Secret Key**“
 - Beide, Sender und Empfänger, benötigen diesen Schlüssel
 - Problematisch: Sicherer Schlüsselaustausch
 - Auch als symmetrische Verschlüsselung bekannt
- Formale mathematische Beschreibung:

$$f_{\text{entschlüsseln}}(\text{Schlüssel}, f_{\text{verschlüsseln}}(\text{Schlüssel}, \text{Text})) = \text{Text}$$

■ Verschlüsselungsprinzipien:

- Diffusion
 - Eine Stelle des Klartextes soll möglichst viele Stellen des Geheimtextes beeinflussen, so dass geringe Änderungen im Klartext viele Änderungen im Geheimtext nach sich ziehen
- Konfusion:
 - Zusammenhang zwischen Geheimtext und Schlüssel so komplex wie möglich, um Rückschlüsse zu erschweren
- Gebräuchliche Verfahren verwenden **rundenbasierten Ansatz**
 - Um Komplexität zu steigern, werden Klartext und Schlüssel pro Runde immer wieder „umsortiert“

Bekannte Verfahren der 1-Schlüssel Verschlüsselung

DES – Data Encryption Standard

- Seit 1976 offizieller Verschlüsselungsstandard der US-Regierung
- Besitzt Schlüssellänge von 56 Bit und sollte deshalb nicht mehr verwendet werden, da Anzahl der prinzipiell möglichen Schlüssel nicht hoch genug ist, um Brute Force standzuhalten
- Triple-DES führt den DES Algorithmus dreimal aus und erreicht dadurch ein höheres Sicherheitsniveau

AES – Advanced Encryption Standard

- Verfahren, das im Jahr 2000 einen Kryptographie-Wettbewerb gewann
- Gilt seitdem als Verschlüsselungsstandard und DES-Nachfolger
- Besitzt verschiedene Schlüssellängen: 128, 192, 256 Bit

Schlüsselaustauschproblem bei 1-Schlüssel Verschlüsselung

Bevor Kommunikation mittels 1-Schlüssel Verschlüsselung geschützt werden kann, müssen Kommunikationspartner („Teilnehmer“) einen geheimen Schlüssel verabreden ...

- Schlüssel darf nicht unverschlüsselt über offenes Internet gesendet werden, ansonsten kann Angreifer den Schlüssel beim Transport über das Internet abhören und anschließend die verschlüsselten Inhalte entschlüsseln
- Schlüsselaustausch ist grundsätzliches Problem der 1-Schlüssel Verschlüsselung
 - Möglicher Lösungsansatz ist die Anwendung des Diffie-Hellmann-Schlüsselaustauschverfahrens
- Bei Verwendung von **2-Schlüssel** Verschlüsselungsverfahren besteht dieses Problem nicht

Funktionsprinzip der 2-Schlüssel Verschlüsselung

Betrachten nun **2-Schlüssel Verschlüsselungsverfahren**:

- Einsatz von Schlüsselpaaren zur Ver- bzw. Entschlüsselung:
 - **Privater Schlüssel**, engl. **Private Key**:
 - ist vor jedem anderen Teilnehmer geheim zu halten
 - **Öffentlicher Schlüssel**, engl. **Public Key**:
 - wird allen anderen Teilnehmern zugänglich gemacht
- Nachricht, die mit öffentlichem Schlüssel verschlüsselt wird, kann nur mit zugehörigem privaten Schlüssel entschlüsselt werden
- Nachricht, die mit privatem Schlüssel verschlüsselt wird, kann nur mit zugehörigem öffentlichen Schlüssel entschlüsselt werden

Wichtig: Aus öffentlichem Schlüssel lässt sich der private Schlüssel (praktisch) **nicht berechnen**

2-Schlüsselverfahren: Verschlüsselung und Entschlüsselung

Voraussetzung:

- Jeder Teilnehmer besitzt:
 - geheim zu haltenden, privaten Schlüssel (S_{privat})
 - frei zugänglichen, öffentlichen Schlüssel ($S_{\text{öffentlich}}$)
- Der öffentliche Schlüssel kann seinem Besitzer zweifelsfrei und sicher zugeordnet werden

Verschlüsselung einer Nachricht mit dem **öffentlichen** Schlüssel eines Teilnehmers erlaubt es nur diesem selbst, die Nachricht mit seinem privaten Schlüssel zu entschlüsseln

$$f_{\text{entschlüsseln}}(S_{\text{privat}}, f_{\text{verschlüsseln}}(S_{\text{öffentlich}}, \text{Text})) = \text{Text}$$

- **Vertraulichkeit** der Nachricht kann so sichergestellt werden

2-Schlüsselverfahren: Verschlüsselung und Entschlüsselung

Verschlüsselung einer Nachricht mit dem **privaten** Schlüssel eines Teilnehmers erlaubt es jedem anderen, zu überprüfen, ob Nachricht wirklich vom Absender stammt, nämlich genau dann, wenn sich Nachricht mit dessen öffentlichen Schlüssel entschlüsseln lässt

$$f_{\text{entschlüsseln}}(S_{\text{öffentlich}}, f_{\text{verschlüsseln}}(S_{\text{privat}}, \text{Text})) = \text{Text}$$

- **Verbindlichkeit** und **Integrität** der Nachricht kann so sichergestellt werden

Bedingung: Funktioniert beides aber nur, wenn:

- öffentliche Schlüssel nicht kompromittiert sind und
- private Schlüssel geheim gehalten wurden

Bekanntes Verfahren der 2-Schlüssel Verschlüsselung

RSA

- Entwickelt von **R**ivest, **S**hamir und **A**dleman
- Die meisten Webserver verwenden das RSA Verfahren zur Absicherung der Verbindungen
- RSA unterstützt verschiedene Schlüssellängen, heutzutage sollten verwendete Schlüssel mindesten **2048 Bit** lang sein
- Sicherheit von RSA basiert auf dem nur sehr aufwendig zu lösenden mathematischen Problem der Faktorisierung (Primfaktorzerlegung) riesig großer Zahlen
→ mehr dazu wird in einem Exkurs erläutert

Hybride Verschlüsselung

Hybride Verschlüsselungsverfahren kombinieren Vorteile der 1-Schlüssel und der 2-Schlüssel Verschlüsselung und gleichen die Nachteile aus

Warum ist Kombination sinnvoll?

- 1-Schlüssel Verschlüsselungen sind sehr effizient, erfordern aber eine sichere Verteilung des geheimen Schlüssels
- 2-Schlüssel Verschlüsselungen brauchen keinen sicheren Schlüsselaustausch, sind aber sehr aufwendig in der Berechnung und daher für große Datenmengen nicht geeignet

Hybride Verfahren kombinieren Effizienz von 1-Schlüssel Verschlüsselungsverfahren mit initialer Sicherheit von 2-Schlüssel Verschlüsselungsverfahren

Hybride Verschlüsselung: Funktionsprinzip

Kommunikationspartner verabreden

- 1-Schlüsselverfahren **X** und
- 2-Schlüsselverfahren **Y**
- 1) Generierung eines zufälligen geheimen Sitzungsschlüssels **S** für spätere Anwendung der 1-Schlüssel Verschlüsselung **X**
- 2) Vermittels des 2-Schlüssel Verschlüsselungsverfahrens **Y** wird Sitzungsschlüssel mit öffentlichem Schlüssel des Empfängers verschlüsselt und an ihn übertragen
- 3) Empfänger entschlüsselt mit seinem privaten Schlüssel empfangenen Sitzungsschlüssel **S**
- 4) Eigentliche Kommunikation kann nun mit verabredetem 1-Schlüsselverfahren **X** mit dem sicher ausgetauschten Sitzungsschlüssel **S** abgesichert werden

Hybride Verschlüsselung: Anwendungen im Internet

Hybride Verschlüsselung kommt im Internet an vielen Stellen zum Einsatz zur Absicherung der Kommunikation:

- Netzwerkprotokoll-Suite **IPsec**
 - Absicherung auf der Übermittlungsebene von Internet-Datenpaketen
- **TLS/SSL** – Transport Layer Security/Secure Sockets Layer
 - Absicherung von Internetverbindungen z.B. bei Webanwendungen (Online-Banking)
- Verschlüsselung von Emails:
 - **PGP** – Pretty Good Privacy
 - **GPG** – GNU Privacy Guard