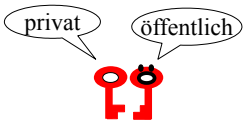
IuD: Asymmetrische Verschlüsselung

Verschlüsselungsverfahren, bei denen beim Ver- und Entschlüsseln derselbe Schlüssel verwendet wird, nennt man **symmetrische** Verfahren.

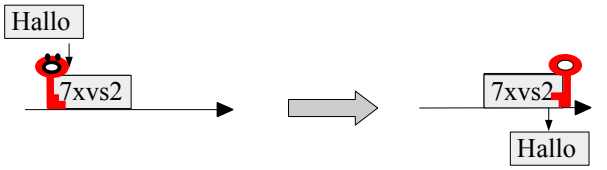
Verschlüsselungsverfahren, bei denen beim Ver- und Entschlüsseln verschiedene Schlüssel zum Einsatz kommen, nennt man **asymmetrische** Verfahren.

Prinzip der asymmetrischen Verschlüsselungsverfahren



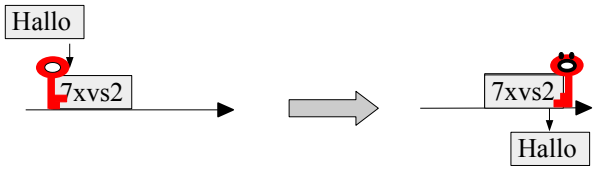
Man erzeugt ein Schlüsselpaar und behält den privaten Schlüssel. Den öffentlichen Schlüssel kopiert man und verteilt ihn an jedem, der mit einem kommunizieren möchte.

Verschlüsseln mit dem öffentlichem Schlüssel



Entschlüsseln mit dem privatem Schlüssel

Anwenden des privaten Schlüssels

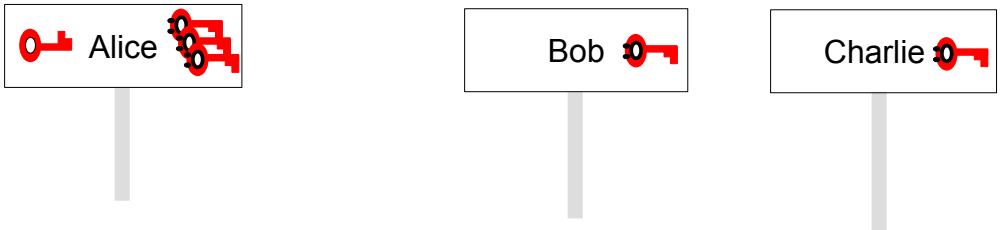


Anwenden des öffentlichen Schlüssels

Aufgaben:

1. *Erkläre, was an der asymmetrischen Verschlüsselung im Vergleich zu der symmetrischen Verschlüsselung asymmetrisch ist.*

2. *Alice hat ein Schlüsselpaar, kopiert den öffentlichen Schlüssel und gibt ihn an ihre Freunde Bob und Charlie weiter. Wer kann jetzt mit welchem Schlüssel Nachrichten verschlüsseln? Wer kann sie dann lesen? Spielt dazu alle möglichen Szenarien durch und notiert sie in einem Sequenzdiagramm. Was fällt euch auf?*



Beantworte anhand deiner Szenarien folgende Fragen:

a) Wer kann geheime Nachrichten an Alice (A) schreiben?

b) An wen kann Alice geheime Nachrichten schreiben?

c) Können Bob (B) und Charlie (C) geheim kommunizieren?

3. *a) Betrachte die Kommunikation von einer beliebigen Person hin zu A. Gib an,welches Krypto-Ziel mit diesem Verfahren gewährleistet wird.*

   b) Betrachte die Kommunikation von A zu einer beliebigen Person, z.B. Bob. Bob bekommt eine Nachricht, die Alice mit ihrem privatem Schlüssel verschlüsselt hat. Kann Bob sicher sein, dass niemand sonst die Nachricht gelesen hat?

   Kann Bob sicher sein, dass die Nachricht von Alice kommt?

   Gib an, welches Krypto-Ziel bei diesem Nachrichtenweg gewährleistet wird?

4. *5 Personen [n Personen] wollen sicher miteinander kommunizieren. Sie tauschen dazu Schlüssel aus:*

   (A) mit einem asymmetrischen Verfahren

   (B) mit einem symmetrischen Verfahren.

   Erstelle eine Gegenüberstellung:

   a) Wie viele Schlüssel werden bei den beiden Verfahren insgesamt benötigt?

   b) Wie viele Schlüssel muss jeder Einzelne jeweils verwalten?

5. *Verschlüsseln mit asymmetrischer Verschlüsselung [1]* *(Aufgabe mit Chat-Tool)*

   Startet pro Gruppe einmal das Programm ChatServerGUI.jar und startet den Server. Dann startet jeder das Programm ChatClient.jar.

   a) Wähle einen kurzen Namen und verbinde dich mit dem Server.

   b) Zunächst brauchst du ein Schlüsselpaar. (Rechtsklick in den Schlüsselspeicher). Du kannst zwischen verschiedenen Sicherheitsstufen wählen. Kürzere Schlüssel gehen schneller. Längere sind sicherer, benötigen aber auch mehr Zeit bei der Generierung und der Verschlüsselung.

   c) Teile deinen öffentlichen Schlüssel allen mit. Du kannst den Schlüssel verschicken, indem du ihn auf die Nachrichteneingabezeile ziehst.

   d) Wenn du einen Schlüssel bekommst, dann kannst du die Schlüsselnachricht auf den Schlüsselspeicher ziehen, um den Schlüssel zu sichern.

   e) Schicke an einen/mehrere Personen eine verschlüsselte Nachricht. Gib dazu zunächst die Nachricht ein. Schicke sie nicht unverschlüsselt ab, sondern ziehe zuerst den richtigen Schlüssel auf die Nachricht. Versende die verschlüsselte Nachricht.

   Verwendeter Schlüssel: _____

   f) Wenn du eine verschlüsselte Nachricht empfängst, musst du auch den richtigen Schlüssel auf diese Nachricht ziehen.

   Verwendeter Schlüssel: _____

   g) Unterschreibe/Signiere eine Nachricht und versende sie an alle.

   Nenne den Schlüssel, den du dazu verwendest: _____

   h) Wenn du eine solche Nachricht empfängst, könntest du denken „Ich brauche gar keinen Schlüssel, weil ich die Nachricht ja lesen kann.“

   Welchen Schlüssel verwendet man bei einer solchen Nachricht und warum ist das Anwenden dieses Schlüsseln sinnvoll?

   _____

1 Thomas Schaller, JK-Informatik