LU05g - Diffie Hellman Schlüsselaustausch

siehe auch *Diffie-Hellman-Schlüsselaustausch*

Bei modernen Verschlüsselungsverfahren sind die Algorithmen allgemein bekannt. Daher ist der geheime Austausch des Schlüssels von grosser Bedeutung.

Sofern sich beide Partner persönlich kennen, kann dies z.B. über einen Memorystick erfolgen. Bei der verschlüsselten Kommunikation mit einem Webserver wird dies aber schwieriger:

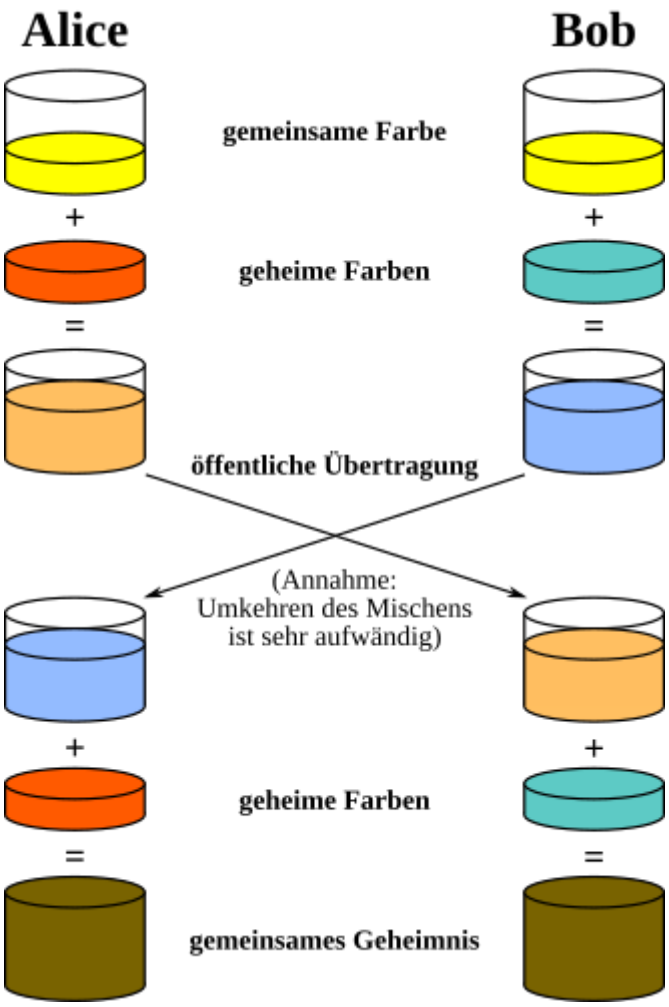
- Die beiden Kommunikationspartner (z.B. Web-Server und Web-Browser) müssen den Schlüssel im Klartext vereinbaren.
- Jeder Angreifer kann mitlesen, wenn der Schlüssel vereinbart wird.

Mit diesem Verfahren können zwei Partner über eine unsichere Leitung einen gemeinsamen, geheimen Schlüssel vereinbaren. Ein potentieller Lauscher kann die ganze Kommunikation mitlesen. Trotzdem kann der Lauscher den geheimen Schlüssel nicht ermitteln.

Veranschaulichung mit Farben

Die Funktionsweise lässt sich gut anhand von Farben erläutern. Dabei gehen wir davon aus, dass

- ... es einfach ist, zwei Farben zu mischen
- ... es sehr schwierig ist, aus einer Farbmischung die ursprünglichen Farben zu filtern.



Quelle: https://upload.wikimedia.org/wikipedia/commons

Umsetzung in der Informatik

In der Informatik basieren die meisten Verfahren auf dem Division/Rest-Verfahren (modulo). Dabei gilt:

- Die Berechnung von Modulo ist sehr einfach. Zum Beispiel: **175348 mod 29 = 14** kann jeder bessere Taschenrechner.
- Die Umkehrung von Modulo kann nicht berechnet werden. Zum Beispiel: **x mod 29 = 14** lässt sich nicht berechnen, man müsste viele verschiedene Zahlen ausprobieren.

1. Alice und Bob einigen sich auf eine grosse Primzahl **p** und eine natürliche Zahl **g**. Die Zahl **g** muss kleiner sein, als die Primzahl **p**.
2. Alice erzeugt eine geheime Zufallszahl **a** und Bob erzeugt eine geheime Zufallszahl **b**.
3. Alice berechnet: $\mathbf{A = g^a \bmod p}$ und sendet **A** an Bob.
4. Bob berechnet: $\mathbf{B = g^b \bmod p}$ und sendet **B** an Alice.
5. Beide können nun den geheimen Schlüssel berechnen:
    - Alice rechnet: $\mathbf{K = B^a \bmod p}$
    - Bob rechnet: $\mathbf{K = A^b \bmod p}$.

Beispiel (Quelle: Wikipedia):

Das folgende Beispiel dient zur Veranschaulichung und benutzt deshalb sehr kleine Zahlen. In der tatsächlichen Anwendung werden dagegen Zahlen mit mindestens mehreren hundert Stellen benutzt.

Alice	**Bob**
Beide einigen sich auf die beiden öffentlichen Schlüssel p=13 und g=2.	
Wählt die Zufallszahl a=5 als geheimen Schlüssel.	Wählt die Zufallszahl b=8 als geheimen Schlüssel.
Rechnet **$A = 2^5 \bmod 13 = 6$** und sendet A an Bob.	Rechnet **$B = 2^8 \bmod 13 = 9$** und sendet B an Alice.
Berechnet **$K = 9^5 \bmod 13 = 3$**.	Berechnet **$K = 6^8 \bmod 13 = 3$**.

Beide erhalten das gleiche Ergebnis. Die Lauscherin Eve kann zwar die Zahlen 13, 2, 6 und 9 mithören, das eigentliche gemeinsame Geheimnis von Alice und Bob K=3 bleibt ihr aber verborgen.

The times they are a-changin'

Wie schon Bob Dylan sang: Die Zeiten ändern sich.

Mit der Einführung von Quanten-Computern könnten viele der heutigen Verschlüsselungstechnologien unsicher werden. Anstatt Jahrhunderte braucht ein Quanten-Computer vermutlich nur Sekunden um eine Verschlüsselung basierend auf Modulo zu knacken.

Siehe auch https://www.boxcryptor.com/de/blog/post/quantum_computing_vs_encryption/

---

m114-A0G