Sicherer Schlüsselaustausch über einen unsicheren Kanal

Wenn ein symmetrisches Verschlüsselungsverfahren verwendet wird, stellen der Schlüssel, seine Übergabe und Geheimhaltung Hauptangriffspunkte für das Verfahren dar. Im zweiten Weltkrieg konnte z. B. der Angriff auf die von der deutschen Wehrmacht benutzte Enigma durch versenkte U-Boote, in denen sich die Codebücher mit Tagesschlüsseln befanden, erfolgreich gestaltet werden.

Daher ließ – vor allem das Militär – an dem Aspekt der Absicherung eines Verfahrens zum Schlüsselaustausch forschen (der in Großbritannien erteilte Auftrag datiert aus den 60er Jahren). Die britischen Forscher James Ellis, Clifford Cocks und Malcolm J. Williamson äußerten Ideen, die allerdings aus Gründen der Geheimhaltung weder veröffentlicht noch patentiert wurden.

Später – nämlich 1976 – wird von den US-Amerikanern Martin Hellman gemeinsam mit Whitfield Diffie und Ralph Merkle an der Stanford-Universität (Kalifornien) ein Verfahren mit der gleichen Grundidee, wie bei den Briten, entwickelt und veröffentlicht. Das Verfahren zum öffentlichen Schlüsseltausch wird – bis heute – als **Diffie-Hellman-Schlüsselaustausch** bezeichnet.

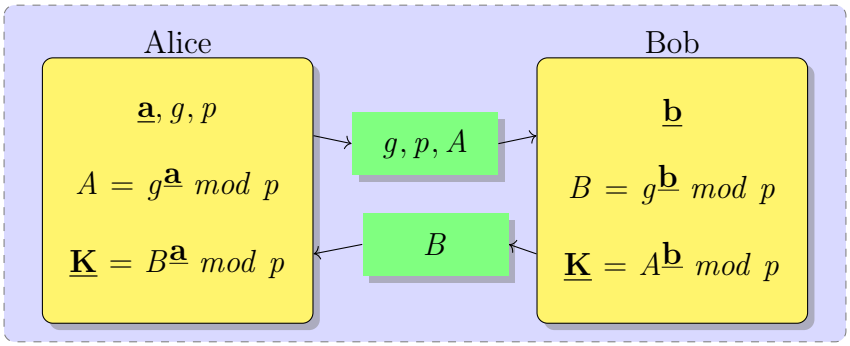


Abbildung 1: Schema des Diff-Hellman-Schlüsseltauschs

Der prinzipielle Ablauf ist in der Abbildung (1) dargestellt – dabei stellen die beiden Boxen in der Mitte den Teil der Kommunikation zwischen Alice und Bob dar, der beobachtet werden kann, da sie über einen unsicheren Kanal (z. B. das Internet) abgewickelt werden.

Obwohl sich Alice und Bob nie treffen, um einen gemeinsamen Schüssel auszutauschen, gelingt ihnen mit diesem Verfahren die Einigung auf einen gemeinsamen Schlüssel.

Die unterstrichenen Elemente werden nicht weitergegeben.

Beispiel zur Illustration – mit kleinen Zahlen

1. Alice schlägt Bob vor: $g = 2$ und $p = 13$.
2. Alice wählt die Zufallszahl $\underline{a} = 5$. Bob wählt die Zufallszahl $\underline{b} = 7$.
3. Alice berechnet $A = 2^5 \mod 13 = 6$ und sendet dieses Ergebnis an Bob.
4. Bob berechnet $B = 2^7 \mod 13 = 11$ und sendet dieses Ergebnis an Alice.
5. Alice berechnet $\underline{K} = 11^5 \mod 13 = 7$.
6. Bob berechnet $\underline{K} = 6^7 \mod 13 = 7$.
7. Beide erhalten das Ergebnis $\underline{K} = 7$.