4.2 Diffie-Hellman-Schlüsselaustausch

Übertragen werden soll ein Schlüssel für eine symmetrische Chiffrierung. Dazu haben Diffie und Hellman 1976 das folgende Verfahren vorgeschlagen, das auf der Exponentialfunktion in endlichen Körpern, also einer (mutmaßlichen) Einweg-Funktion beruht:

1. A (Alice) und B (Bob) einigen sich (öffentlich) über eine Primzahl p und eine zugehörige Primitivwurzel a.
2. A erzeugt eine Zufallszahl x, bildet $u = a^x \bmod p$ und sendet u an B.
3. B erzeugt eine Zufallszahl y, bildet $v = a^y \bmod p$ und sendet v an A.
4. A berechnet $k = v^x \bmod p$, und B berechnet $k = u^y \bmod p$.

Die Zahl k ist der gemeinsame geheime Schlüssel (oder dient zu dessen Bestimmung nach einem öffentlich bekannten Verfahren). Dass sowohl A als auch B den gleichen Schlüssel haben, liegt an der Gleichung

$$v^x \equiv a^{xy} \equiv u^y \pmod{p}.$$

Ein Lauscher kann nur die Zahlen p, a, u und v abfangen, die ihm nicht gestatten, k oder x oder y effizient zu berechnen.

Damit hat man also auch so etwas wie ein hybrides Verschlüsselungsverfahren; es unterscheidet sich von einem „echten“ asymmetrischen Verfahren aber insofern, als A nicht an B spontan eine Nachricht senden kann, sondern eine Synchronisation herstellen muss.

Wenn ein Angreifer effizient diskrete Logarithmen berechnen kann, kann er auch das Diffie-Hellman-Verfahren effizient brechen. Ob auch die umgekehrte Implikation gilt, ist unbekannt.

Beim britischen Geheimdienst CESC war das Verfahren schon 1974 entdeckt, aber natürlich geheim gehalten worden.