zurück

Diffie-Hellman-Schlüsselaustausch

Der **Diffie-Hellman-Schlüsselaustausch** (DHKE) ist ein kryptografisches Verfahren zum **sicheren Austausch eines gemeinsamen Schlüssels** über eine unsichere Verbindung. Es dient als Grundlage für viele verschlüsselte Kommunikationsprotokolle (z. B. HTTPS, SSH, VPNs).

Ziel

Zwei Parteien (z. B. Alice und Bob) möchten einen **gemeinsamen geheimen Schlüssel** erzeugen – über eine öffentliche Verbindung –, ohne dass ein Angreifer (z. B. Eve) diesen Schlüssel berechnen kann.

Grundidee

Beide Parteien wählen einen privaten Schlüssel und berechnen daraus einen öffentlichen Schlüssel, den sie austauschen. Mit dem jeweils empfangenen öffentlichen Schlüssel berechnen sie dann denselben geheimen Schlüssel.

Mathematische Grundlage

- Es wird eine große Primzahl p und eine Basis g (mit $1 < g < p$) öffentlich vereinbart.
- Die Berechnungen basieren auf **modularer Exponentiation**: $a^b \mod p$
- Sicherheit basiert auf dem **diskreten Logarithmusproblem** (schwer zu lösen).

Beispielrechnung

Öffentliche Parameter:

- Primzahl $p = 23$
- Basis $g = 5$

Private Schlüssel:

- Alice wählt $a = 6$ (geheim)
- Bob wählt $b = 15$ (geheim)

Öffentliche Schlüssel:

- Alice berechnet: $A = g^a \mod p = 5^6 \mod 23 = 8$
- Bob berechnet: $B = g^b \mod p = 5^{15} \mod 23 = 2$

Austausch:

- Alice sendet $A = 8$ an Bob
- Bob sendet $B = 2$ an Alice

Gemeinsamer geheimer Schlüssel:

- Alice berechnet: $s = B^a \mod p = 2^6 \mod 23 = 18$
- Bob berechnet: $s = A^b \mod p = 8^{15} \mod 23 = 18$

Ergebnis: Beide Seiten besitzen nun denselben geheimen Schlüssel: **$s = 18$**

Sicherheit

Ein Angreifer kennt:

- p, g, A, B

Aber nicht:

- a oder b

Das Berechnen von a aus $A = g^a \mod p$ ist **mathematisch extrem aufwendig** (diskreter Logarithmus). Deshalb kann der gemeinsame Schlüssel nicht einfach abgeleitet werden.

Anwendungsbeispiele

- TLS / HTTPS (z. B. in Browsern)
- SSH
- IPsec VPNs
- PGP/GnuPG
- Signal, WhatsApp, Matrix

Schwächen & Schutzmaßnahmen

- **Nicht authentifiziert**: Anfällig für „Man-in-the-Middle“-Angriffe.
- Lösung: Kombinieren mit Zertifikaten oder digitalen Signaturen.

Varianten

- **ECDH**: Elliptic Curve Diffie-Hellman – gleiche Idee, effizienter, moderner.
- **DHE-RSA**: Authentifizierte Variante mit RSA-Zertifikaten.

Zusammenfassung

Schritt	Beschreibung
1	Öffentliche Werte wählen (p, g)
2	Jeder wählt geheimen Exponenten a, b
3	Öffentliche Schlüssel berechnen: $A = g^a \mod p, B = g^b \mod p$
4	Schlüssel austauschen
5	Gemeinsamen Schlüssel berechnen: $s = B^a \mod p = A^b \mod p$
	Beide Seiten besitzen denselben geheimen Schlüssel