Einführung in Diffie-Hellman und RSA-Verschlüsselung

Mathe-AG

October 6, 2024

1 Diffie-Hellman Schlüsselaustausch

Der Diffie-Hellman-Schlüsselaustausch ist ein Verfahren, das es zwei Parteien ermöglicht, einen gemeinsamen geheimen Schlüssel über einen unsicheren Kanal zu erzeugen, ohne dass ein vorheriger geheimer Austausch notwendig ist.

1.1 Grundidee

Die Grundidee ist, dass jeder Teilnehmer eine private Zahl wählt, aber nur eine berechnete Zahl öffentlich teilt. Am Ende können beide Teilnehmer denselben geheimen Schlüssel berechnen.

1.2 Mathematischer Ablauf

- Wähle eine große Primzahl p und eine zugehörige Basis g (oft auch als Generator bezeichnet). Diese Werte sind öffentlich.
- Alice wählt eine geheime Zufallszahl a und berechnet $A = g^a \mod p$, dann sendet sie A an Bob.
- Bob wählt ebenfalls eine geheime Zufallszahl b und berechnet $B = g^b \mod p$, dann sendet er B an Alice.
- Alice berechnet nun den gemeinsamen Schlüssel $K_A = B^a \mod p$.
- Bob berechnet den gemeinsamen Schlüssel $K_B = A^b \mod p$.
- Da $K_A = K_B$, teilen sich Alice und Bob nun denselben geheimen Schlüssel: $K = g^{ab} \mod p$.

Wichtig: Ein Angreifer, der nur g, p, A und B kennt, kann nicht so leicht a oder b berechnen, da das Problem, den diskreten Logarithmus zu berechnen, als schwierig gilt.

1.3 Beispiel

- Wähle $p = 23$ und $g = 5$.
- Alice wählt $a = 6$ und berechnet $A = 5^6 \mod 23 = 8$. Sie sendet A an Bob.
- Bob wählt $b = 15$ und berechnet $B = 5^{15} \mod 23 = 19$. Er sendet B an Alice.
- Alice berechnet $K_A = 19^6 \mod 23 = 2$.
- Bob berechnet $K_B = 8^{15} \mod 23 = 2$.

Beide haben nun den gemeinsamen Schlüssel $K = 2$.

2 RSA-Verschlüsselung

Das RSA-Kryptosystem basiert auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen. Es wird sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet.

2.1 Schlüsselerzeugung

- Wähle zwei große Primzahlen p und q.
- Berechne das Produkt $n = p \times q$. Dies ist der Modul für beide Schlüssel.
- Berechne $\phi(n) = (p-1)(q-1)$.
- Wähle eine Zahl e, die teilerfremd zu $\phi(n)$ ist (oft wird $e = 65537$ verwendet).
- Berechne den privaten Schlüssel d, sodass $d \cdot e \equiv 1 \mod \phi(n)$ (dies ist der modulare Inverse von e).

Der öffentliche Schlüssel ist (n, e), und der private Schlüssel ist (n, d).

2.2 Verschlüsselung

Um eine Nachricht m zu verschlüsseln, verwendet der Sender den öffentlichen Schlüssel (n, e) und berechnet:

$$c = m^e \mod n$$

wobei c der chiffrierte Text ist.

2.3 Entschlüsselung

Um die Nachricht zu entschlüsseln, verwendet der Empfänger den privaten Schlüssel (n, d) und berechnet:

$$m = c^d \mod n$$

wobei m die ursprüngliche Nachricht ist.

2.4 Beispiel

- Wähle $p = 61$ und $q = 53$. Dann ist $n = 61 \times 53 = 3233$ und $\phi(n) = (61 - 1)(53 - 1) = 3120$.
- Wähle $e = 17$. Dann berechne $d = 2753$, da $17 \cdot 2753 \equiv 1 \mod 3120$.
- Der öffentliche Schlüssel ist $(3233, 17)$ und der private Schlüssel ist $(3233, 2753)$.
- Um die Nachricht $m = 65$ zu verschlüsseln, berechne $c = 65^{17} \mod 3233 = 2790$.
- Um die Nachricht zu entschlüsseln, berechne $m = 2790^{2753} \mod 3233 = 65$.

3 Tipps für den Unterricht

- Erkläre die zugrunde liegenden mathematischen Konzepte: Primzahlen, Modulo-Rechnung und das Konzept des diskreten Logarithmus.
- Verwende konkrete Zahlenbeispiele, um den Ablauf nachvollziehbar zu machen.
- Diskutiere die Sicherheit der Verfahren und warum das Faktorisierungsproblem bzw. das diskrete Logarithmusproblem schwer zu lösen sind.
- Stelle auch Anwendungen in der Praxis vor, z.B. HTTPS, VPNs und digitale Signaturen.
- Optional: Verwende Programme oder Online-Tools, um die Berechnungen durchzuführen und zu veranschaulichen.