Diffie-Hellman-Schlüsselaustausch

Ein zentrales Problem der Kryptographie ist die Verteilung der verwendeten Schlüssel. Mit Hilfe des *Diffie-Hellman-Schlüsselaustausch-verfahrens* erzeugen zwei Kommunikationspartner einen geheimen Schlüssel, den nur diese beiden kennen. Dieser Schlüssel wird üblicherweise verwendet, um verschlüsselte Nachrichten mittels eines symmetrischen Kryptosystems zu übertragen.

Ein solches Verfahren muss zum Einsatz kommen, wenn man PFS („Perfect Forward Secrecy“) erreichen möchte.

Funktionsweise

Die Funktionsweise erklärt die folgende Präsentation ab Folie 7, der Originalcomic findet sich dort, das Bild zu Diffie-Hellman Verfahren ist dieses.

[n/a: Keine Treffer]

Problemstellung

Alice und Bob möchten miteinander verschlüsselt kommunizieren. Dazu möchten sie gern die Schlüssel für den Verschlüsselungsvorgang miteinander austauschen. Leider besteht keine gesicherte Verbindung zwischen beiden (z.B. das Internet) und ein persönliches Treffen als sicherste Alternative ist nicht möglich. Also wählen sie die folgende Vorgehensweise:

Vorbereitungen

- Zunächst denkt sich einer von beiden eine[1)] Primzahl **P** sowie eine Zahl **g** aus. Für die Zahl g muss gelten, dass sie kleiner als P ist. [2)]
- Diese beiden Zahlen (P und g) werden offen an den anderen Partner gesendet, so dass Alice und Bob sich also auf diese beiden Zahlen „geeinigt haben“.

Schlüsselberechnung

Nun denkt sich jeder der beiden eine **geheime** Zahl aus; Alice nimmt **a**, Bob wählt **b**. a und b sind die geheimen Schlüssel, diese werden niemals über den unsicheren Kanal gesendet!

Jetzt berechnen beide den zu Ihrem geheimen Schlüssel gehörigen öffentlichen Schlüssel:

Alice:	$S_a=g^a \bmod P$
Bob:	$S_b=g^b \bmod P$

Diese öffentlichen Schlüssel tauschen Sie nun aus, so dass Alice S_b kennt und Bob S_a. Aus diesen öffentlichen Schlüsseln errechnen beid nun unter Verwendung Ihrer „geheimen“ Zahl [3)], den gemeinsamen Schlüssel, mit dem Sie jetzt Ihre Nachrichten verschlüsseln können.

Alice:	$G=S_b^a \bmod P$
Bob:	$G=S_a^b \bmod P$

Anmerkung: „mod“ bezeichnet die Berechnung des Restes bei ganzzahliger Division. (7 mod 3 = 1, da 7:3=2 Rest 1)

Aufgaben

1) Vollziehe den Schlüsselaustausch mit deinem Nebensitzer mit Papier und Bleistift (und einem Taschenrechner) und kleinen Zahlen nach. Mache dir klar, dass der geheime Schlüssel niemals über die unsichere Leitung übertragen werden muss.

2) Bonus: Programmiere ein kleines Programm, mit dem der Schlüsselaustauch veranschaulicht wird. (PHP/Java/Python)

1)

in der Praxis möglichst große

2)

Tatsächlich gibt es noch eine weitere Einschränkung, die wir aber hier vernachlässigen; bei weiterem Interesse sei auf die einschlägige Literatur

3)

dem jeweiligen geheimen Schlüssel