Diffie-Hellman-Merkle-Schlüsselaustausch[1]


Merkle, Hellman, Diffie

Dr. Whitfield 'Whit' Diffie (geboren am 5.Juni 1944) ist ein amerikanischer Experte für Kryptographie. Diffie

studierte bis 1965 Mathematik am Massachusetts Institute of Technology (MIT). Diffie arbeitete zunächst an der Entwicklung von Mathlab (einem Programm zur symbolischen Manipulation mathematischer Ausdrücke) mit und beschäftigte sich dann an der Universität Stanford mit dem Problem des Beweisens der Korrektheit von Programmen. Anschließend wandte er sich dem Thema Kryptografie zu und entdeckte 1975 zusammen mit Martin Hellman und Ralph Merkle die Verwendbarkeit von Falltürfunktionen als Grundlage der Public Key Cryptography, also der Verschlüsselung von Nachrichten mit öffentlichen Schlüsseln. Ähnliche Methoden wurden unabhängig davon allerdings bereits durch James Ellis im englischen Geheimdienst untersucht.

Vorabinformation

Berechnen Sie mit Ihrer Nachbarin oder Ihrem Nachbarn einen Schlüssel nach dem Diffie-Hellman-Merkle-Verfahren.
Zuerst müssen sich die Kommunikationspartner auf zwei Zahlen einigen:
Eine Primzahl p und eine natürliche Zahl g werden gemeinsam festgelegt. Für unser Beispiel wählen wir p=11 und g=7. Diese werden später in die Einwegfunktion $g^z \mod p$ eingesetzt, wobei z eine Zufallszahl zwischen 1 und p-1 darstellt (vgl. Verfahren für Alice und Bob weiter unten)
Die beiden Werte p und g können über einen unsicheren Kanal übertragen werden!

Durchführung

Die Kommunikationspartner seien Alice und Bob[2]. Das Beispiel benutzt sehr kleine Zahlen. In der tatsächlichen Anwendung werden Zahlen mit mehreren hundert Stellen benutzt.
Bestimmen Sie wer von Ihnen die Rolle von Alice bzw. Bob übernimmt und führen Sie die unten aufgeführten Anweisungen für die zugewiesene Rolle aus. Führen Sie Ihre Berechnungen alleine aus! Sie können dazu den Rechner von Windows benutzen. Den Rechner finden Sie unter Zubehör. Um die Modulo-Werte zu berechnen, müssen Sie den Rechner auf wissenschaftlich umstellen.

Alice	**Bob**
1. Wählen Sie eine Zahl (<p) zwischen 1 und 10 und nennen Sie Ihre Zufallszahl a. Diese bleibt geheim!	1. Wählen Sie eine Zahl (<p) zwischen 1 und 10 und nennen Sie Ihre Zufallszahl b. Diese bleibt geheim!
2. Setzen Sie Ihre Zahl in die Einwegfunktion $7^a \mod 11$ ein und nennen Sie Ihr Ergebnis A. **A** =	2. Setzen Sie Ihre Zahl in die Einwegfunktion $7^b \mod 11$ ein und nennen Sie Ihr Ergebnis B. **B** =
3. Teilen Sie Bob das Ergebnis A mit. 4. Nennen Sie den von Bob erhaltenen Wert B und setzen sie den Wert in die Funktion $B^a \mod 11$ ein. Das Ergebnis ist der Schlüssel. **Schlüssel** =	3. Teilen Sie Alice das Ergebnis B mit. 4. Nennen Sie den von Alice erhaltenen Wert A und setzen sie den Wert in die Funktion $A^b \mod 11$ ein. Das Ergebnis ist der Schlüssel. **Schlüssel** =
5. Vergleichen Sie den Schlüssel mit Bob.	5. Vergleichen Sie den Schlüssel mit Alice.

Wählen Sie für p und g andere, größere Zahlen und führen Sie das Verfahren wiederholt durch. Bekommen Sie weiterhin beide den gleichen Schlüssel?

---

1 Nach Material vom OSZ Handel (Johann Penon) und Simon Singh: Geheime Botschaften, Carl Hanser Verlag 2000. Bilder von http://www.at-mix.de/druckversion-lexikon-diffie.htm

2 In der Beschreibung von Verschlüsselungsverfahren hat sich die Konvention durchgesetzt, die beiden Kommunikationspartner mit Alice und Bob zu bezeichnen.