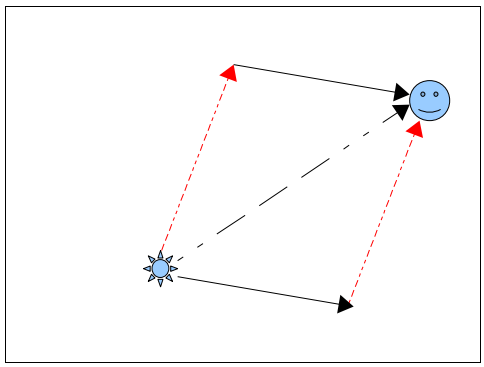
Diffie - Hellmann

Eines der wichtigen Probleme bei der Verschlüsselung ist die sichere Übermittlung des Schlüssels: Was nützt die beste Verschlüsselung, wenn der Angreifer den Schlüssel abfangen kann? Eine Möglichkeit, dieses Problem zu umgehen, ist die Verwendung von asymetrischen Verfahren wie RSA, bei dem der Empfänger unserer message uns die öffentlichen Schlüssel zur Verschlüsselung zusendet und wir nun prinzipiell sicher sein können, dass nur er sie entschlüsseln kann.
Bei symmetrischen Verfahren geht das natürlich nicht. Hier müsste man also geschützt übermitteln. Eine prinzipiell sichere Vigenére – Verschlüsselung mit einem Schlüssel, der so lang ist wie der zu übermittelnde Text, scheitert praktisch eben genau an diesem Problem.
Eine mögliche Lösung besteht darin, dass überhaupt kein Schlüssel übermittelt wird. Das Verfahren nennt man Diffie – Hellmann – Schlüsselaustausch und wie man aus dem ersten Satzteil schließen kann, ist das letzte Wort darin eigentlich falsch. Was bei diesem Verfahren ausgetauscht wird, ist sozusagen ein halber Schlüssel. Benutzen wir zum Verständnis zunächst ein Bild. Wenn bei einer Schatzsuche jeder der beiden Suchenden nur die Richtung und Länge eines der beiden Teilstücke des Weges kennt, kann keiner von beiden ohne die Mithilfe des anderen zum Schatz finden. So ähnlich ist es bei unserem Verfahren und doch auch wieder an einer entscheidenden Stelle ganz anders.



Diffie – Hellmann

- beide Partner einigen sich auf eine Primzahl p und irgendeine andere Zahl g, die zwischen 2 und p – 2 liegen muss.[1]
  Beide Zahlen müssen nicht geheim sein.
- Jeder von beiden Partnern generiert sich nun – dies muss nun wirklich so geschehen, dass sie geheim bleiben – eine eigene Zahl, die wir a nennen wollen und beim Partner b.
  Sie müssen im selben Zahlenraum liegen und sollten nicht zu klein sein, damit ein Angreifer sie nicht mit Probieren finden kann.
- Diese Zahlen setzt nun nämlich jeder bei sich in unsere bekannte Potenz-modulo-Funktion ein, der eine berechnet also $g^a \bmod p$ und der andere $g^b \bmod p$.
  Ihre Werte übermitteln sie – durchaus offen – ihrem Partner und der wiederholt das Verfahren bei sich mit der erhaltenen Zahl. Wegen
  $(g^b \bmod p)^a \bmod p = (g^a \bmod p)^b \bmod p \rightarrow key$
  ist beiden – aber eben nur diesen beiden – nun derselbe Wert bekannt, den sie also als Schlüssel verwenden können.

Warum dies Verfahren sicher ist, kann man mit dem o.a. Bild nicht verstehen, denn danach könnte ja auch jemand anders als die Beteiligten die beiden Pfeile wieder zusammensetzen, wenn er sie aus den übermittelten Werten erhalten kann.
Hierin liegt aber genau das Problem für den Angreifer: Da wir die Potenz-modulo-Funktion verwenden, die den verwendeten Zahlenraum bei der Berechnung „wirr“ durchspringt, kann aus dem übermittelten Wert nicht wieder auf die Ausgangszahl zurück geschlossen werden.

1 Das kann natürlich auch einer von beiden machen oder jemand anders.

a und b müssen groß genug sein, um einen Angriff durch einfaches Ausprobieren abzuwehren.
Wie man leicht sieht, hat man bei a=1 als übermittelten Wert die ungeschützte Zahl g, die von jedem Angreifer sofort erkannt werden kann. Ebenso gut könnte er durch Probieren niedriger Zahlen von a und Vergleich mit dem übermittelten Wert das a herausbekommen.
Wir erinnern uns aber: Die Anzahl der möglichen Zahlen wächst exponentiell mit der Zahl der Stellen[1].
Ein Beispiel mit – eben viel zu kleinen – Zahlen:

p = 1021, g sei z.B. 4 [kann jeder kennen]
Ein Partner wählt a = 500 [darf nur er kennen]
berechnet $4^{500} \ mod \ 1021 = 227$ und übermittelt diese Zahl.
Der andere Partner wählt a = 400 [darf nur er kennen]
berechnet $4^{400} \ mod \ 1021 = 521$ und übermittelt diese Zahl.
Der erste rechnet weiter mit dieser Zahl 521 und erhält 340.
Der zweite rechnet weiter mit der Zahl 227 und erhält auch 340.

1 Untersuchen Sie einmal, wie durch das Weglassen aller Zahlen mit halber Stellenzahl sich die Anzahl der möglichen Zahlen verändert!
Vergleichen Sie dabei einmal die Ergebnisse für zehnstellige, zwanzigstellige ... hundertstellige Zahlen.