Proseminar Kryptographische Protokolle von Christian Ruppert

Diffie-Hellman Schlüsselaustausch

1 Warum Schlüsselaustausch?

Der Transport von Codebüchern oder Streichlisten war immer eines der größten Sicherheitsprobleme in der Kryptographie, vor Allem im militärischen Bereich. Gelang so ein Codebuch dem Feind in die Hände, war das Verschlüsselungssystem hinfällig. Bis 1976 war das persönliche Überbringen oder das Senden einen Boten der einzig sichere und übliche Weg, solche Codes zu verteilen. Das sogenannte Schlüsselverteilungsproblem zu lösen war demnach ein wichtiges militärisches Ziel.

1.1 Geschichte von Diffie - Hellman

Obwohl es in den 70er Jahren praktische keine kommerzielle Anwendung für den Schlüsselaustausch gab und in militärisches Kreisen erhebliche Mittel für die Kryptographie flossen, arbeiteten Martin Hellman und Whitfield Diffie in Stanford, CA an einem Schlüsselverteilungssystem. Ein großer Teil des Konzept geht auch auf den Nanotechniker Ralph Merkle zurück, welcher auch als Erfinder im Patent eingetragen ist. Im November 1976 veröffentlichten Sie 'New Directions in Cryptography', was den Beginn der asymmetrischen Verschlüsselung darstellte. 1 Jahr später wurde RSA entwickelt.

Interessanterweise gab 1997 der britische Nachrichtendienst GCHQ bekannt, ein sehr ähnliches Protokoll bereits einige Jahr zuvor entwickelt zu haben, was jedoch der Geheimhaltung unterlag. Da die Briten keine ökonomische Anwendung für das Verfahren sahen und es zudem militärischer Geheimhaltung unterlag, wurde von ihrer Seite nie ein Patent beantragt.

1.2 Was macht Diffie - Hellman ?

Die Besonderheit von Diffie - Hellman besteht darin, dass über einen unsicheren Kanal ein geheimer Schlüssel vereinbart wird. Die Bezeichnung „Schlüsselaustausch“ ist hier ein bisschen irreführend, da kein bestehender Schlüssel übertragen, sondern ein neuer Schlüssel anhand von öffentlichen und privaten Informationen berechnet wird.

2 Mathematische Grundlagen

Die Korrektheit und Sicherheit von Diffie - Hellman basiert auf

- einer endlichen zyklischen Gruppe, auf dem sich die Operationen bewegen.
- einem Generatorelement dieser Gruppe
- einer schwer umzukehrenden Funktion(Oneway - Trapdoorfunktion)

2.1 Endlicher Körper: Definiton

Diffie-Hellman basiert auf einem Endlichen Körper (oder Galoiskörper, Galoisfeld) F_p über einer Primzahl p. In Diesem sind Addition, Subtraktion, Multiplikation und Division wohl definiert. Diffie Hellman bewegt sich auf der multiplikativen Gruppe F_p^* von F_p. Die Operation dieser Gruppe ist die Multiplikation. Außerdem benötigt man ein Generatorelement a (oder primitive Einheitswurzel). Aus diesem Element können durch Potenzieren alle Elemente der Gruppe erzeugt werden.
Defintion :

Gegeben sei eine Primzahl p und die Trägermenge $M = \{0, ..., p-1\}$ von F_p. Ein Element $a \in$ M heißt primitive Einheitswurzel, wenn gilt :
$\forall m \in \{1, ..., p-1\} : \exists q \in \{0, ..., p-1\}$, so dass $m \equiv a^q \bmod p$.

2.2 Endlicher Körper: Beispiele

Die Primzahl p sei 7. F_7:

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Als primitive Einheitswurzel wählt man zunächst $a = 2$. Man testet, ob a auch wirklich F_p erzeugt, also :

$2^1 = 2 \equiv 2 \bmod 7$	$2^2 = 4 \equiv 4 \bmod 7$	$2^3 = 8 \equiv 1 \bmod 7$
$2^4 = 16 \equiv 2 \bmod 7$	$2^5 = 32 \equiv 4 \bmod 7$	$2^6 = 64 \equiv 1 \bmod 7$

Nein, 3,5,6 werden nicht erzeugt.

Das Gleiche versucht man mit a = 3 :

$3^1 = 3 \equiv 3 \bmod 7$	$3^2 = 9 \equiv 2 \bmod 7$	$3^3 = 27 \equiv 6 \bmod 7$
$3^4 = 81 \equiv 4 \bmod 7$	$3^5 = 243 \equiv 5 \bmod 7$	$3^6 = 729 \equiv 1 \bmod 7$

Ja, 1,...,6 wird erzeugt. Also ist 3 ein passendes Generatorelement.

2.3 Effiziente Berechnung von a

Da fast jedes zweite Element von F_p erzeugend ist, hat man eine gute Chance, es richtig zu „erraten“. Die Verfikation ist jedoch aufwendiger. Indem man p-1 faktorisiert, gibt es effizientere Verfahren.

$\forall a \in N$ gilt : $a^{(p-1)} \equiv 1 \bmod$ p.

Die Ordnung von a ist das kleinste postive x, für das gilt : $a^x = 1\ modp$. Somit ist die Ordnung einer primitive Einheitswurzel p-1, da das Ergebnis von (1*a*a*..)erst bei $p - 1 \equiv 1$ sein darf, da sich sonst die Sequenz ab 1 wiederholen würde. Dann könnte a keine primitive Einheitswurzel sein. Um zu testen ob a Einheitswurzel bzgl. p ist, testet man, ob die Ordnung von a kleiner als p-1 ist. Wenn die Ordnung gleich p-1 ist, ist a primitve Einheitswurzel. Das lässt sich effizient berechnen, indem man p-1 faktorisiert, denn durch eine mögliche kleinere Ordnung f muss p-1 teilbar sein. (Es würde sich dann eine f lange Sequenz von (1*a*a*..) $p - 1/f$ mal wiederholen). Also muss man für jeden Faktor f von p-1 testen, ob :

$a^{(p-1)/f} \not\equiv 1 \bmod$ p

Besonders einfach wird es, wenn $p - 1 = 2r$,wobei r prim ist, gilt. Dann ist a primitve Einheitswurzel, wenn $a^2 \not\equiv 1 \bmod p$ und $a^r \not\equiv 1 \bmod p$.

In der Praxis werden festgelegte Primzahlen der Größe 1024bit - 8192bit genutzt. (Diffie Hellman Gruppen), deren Generatorelement a = 2 bekannt ist, da die Berechnung bzw. Verifizierung Derselben relativ aufwendig ist.

3 Das Diffie - Hellman Verfahren

3.1 Verfahren der Schlüsselvereibarung

Zunächst einigen sich Alice und Bob auf eine große Primzahl p und ein dazu passendes a. Diese Parameter sind nicht geheim und können ungesichert übertragen werden. Alice und Bob wählen sich jeweils eine Zufallszahl X_1 und X_2 mit $1 \leq X_i < p$.

$Y_i = a^{X_i}$ wird von Beiden berechnet. X_i entspricht dem privaten Schlüssel und Y_i dem öffentlichen Schlüssel eines asymmetrischen Kryptosystems. Y_i wird dem anderen Gesprächspartner geschickt, X_i bleibt geheim.

Nun können sich Alice und Bob jeweils den geheimen Schlüssel berechnen.

Alice rechnet : $K_{1,2} = Y_2^{X_1} = a^{X_2^{X_1}} = a^{X_1 X_2}$

Bob rechnet : $K_{2,1} = Y_1^{X_2} = a^{X_1^{X_2}} = a^{X_1 X_2}$

Somit haben beide den identischen Schlüssel berechnet.

3.2 Ein Beispiel

p = 7, a = 3

Alice	Bob
wählt $X_1 = 2$	wählt $X_2 = 6$
berechnet $Y_1 = a^{X_1} = 3^2 = 9 \equiv 2 mod 7$	berechnet $Y_2 = a^{X_2} = 3^6 = 729 \equiv 1 mod 7$
$Y_1 = 2 ->$	$<- Y_2 = 1$
berechnet $K_{1,2} = 1^2 mod 7 = 1$	berechnet $K_{2,1} = 2^6 mod 7 = 1$

4 Sicherheit

4.1 Das „Diffie-Hellman Problem“

Das DH - Verfahren ermöglicht es also, über einen unsicheren Kanal einen geheimen Schlüssel zu vereinbaren. Die Sicherheit basiert auf einer Einwegfunktion mit Falltür. Eine Einwegfunktion ist, wie z.b. auch die Primfaktorisierung, eine Funktion, die komplexitätstheoretisch schwer oder gar nicht umzukehren ist. Eine „Trapdoor“-Einwegfunktion lässt sich umkehren, wenn man im Besitz der geheimen Information ist. Diese ist bei Diffie-Hellman die geheime Zufallszahl X_i. Wenn ein Angreifer jedoch nur im Besitz der öffentlichen Variablen p, a und Y_i ist, muss er das diskrete Logarithmusproblem

$X_i = \log_a Y_i \bmod p$ lösen, um ein X_I und somit den Schlüssel zu berechnen. Das ist jedoch im Vergleich zur Exponentiation wesentlich aufwendiger. Für p = 200 benötigt man 400 Multiplikationen ($K = a^{X_1 X_2}$), $X_I \leq p$, Ein Angreifer müsste $2^{200} = 10^{30}$ Operationen zur Lösung des diskr. Logarithmus ausführen.

4.2 Andere Sicherheitsaspekte

Da das Diffie - Hellman Verfahren keine Authorisierung vornimmt, ist ein Man-in-the-Middle Angriff leicht Möglich. Hier muss anderweitig für Sicherheit gesorgt werden, z.B durch sogenannte Station - to - Station Protokolle. Außerdem sind Timing Attacks möglich.

5 Anwendung von Diffie - Hellman

Üblicherweise wird DH dazu benutzt, Schlüssel für symmetrische Kryptosysteme zu erzeugen.

Das Elgamal - Kryptosystem ist ein auf DH aufbauendes Kryptosystem. In VPN wird Diffie - Hellman verwendet