Chiffrendesign

Will man ein Verschlüsselungsverfahren entwickeln, bieten sich zwei Wege an:

- Man macht das Verfahren möglichst kompliziert und hofft, dass dadurch keine Schwachstellen entstehen – oder dass ein Angreifer diese in der Komplexität nicht findet. Diesen Ansatz nennt man auch "Security by Intricacy" (in etwa "Sicherheit durch Unduchschaubarkeit")
- Man entwirft das Verfahren möglichst durchdacht und versucht, Schwachstellen gar nicht entstehen zu lassen.

Wenig verwunderlich kommt bei ernsthaften Verfahren nur die zweite Variante zum Einsatz.

Was ist eine Schwachstelle eines modernen Verfahrens?

Zunächst muss man sich klarmachen, was man bei modernen Verfahren unter einer Schwachstelle versteht.

Bei einem modernen Verfahren spricht man bereits dann von einer "Schwachstelle", wenn es einen Angriff auf das Verfahren gibt, der besser ist als die vollständige Schlüsselsuche.

Außerdem werden statistische Auffälligkeiten bei einem modernen Verfahren als Schwachstelle betrachtet, da diese als Angriffpunkt dienen können. Ein gutes symmetrischen Verfahren soll ein **Zufallsorakel** sein.

Als Zufallsorakel bezeichnet man eine Funktion, bei der kein erkennbarer Zusammenhang zwischen der Eingabe (Klartext & Schlüssel) und der Ausgabe (Geheimtext) existiert – auch nicht in wenigen Einzelfällen.

- Wenn ein Verschlüsselungsverfahren beispielsweise bei Verwendung des Schlüssels `00…000` stets einen Geheimtext liefert, der als letztes Bit eine `0` hat, ist die Zufallsorakel-Eigenschaft schon verletzt.
- Ebenso hat man kein Zufallsorakel mehr, wenn das Invertieren von Klartext und Schlüssel dazu führt, dass auch der Geheimtext invertiert. Dies ist beim DES der Fall. Unter anderem deshalb ist der DES kein perfektes Zufallsorakel.
- Wenn es Schlüssel gibt, bei denen Verschlüsselung und Entschlüsselung identisch sind - dann führt das zweifache Verschlüsseln wieder zum Klartext. Das ist bei DES bei einigen wenigen Schlüsseln der Fall → kein Zufallsorakel.

Überlegungen zur Schlüssellänge

Schlüssellänge	Anzahl der Schlüssel	Dauer einer vollständigen Schlüsselsuche
40 Bit	$1{,}1 \cdot 10^{12}$	1,3 Sekunden
56 Bit	$7{,}1 \cdot 10^{16}$	24 Stunden
64 Bit	$1{,}8 \cdot 10^{19}$	256 Tage
128 Bit	$3{,}4 \cdot 10^{38}$	$1{,}3 \cdot 10^{19}$ Jahre
192 Bit	$6{,}3 \cdot 10^{57}$	$2{,}4 \cdot 10^{38}$ Jahre
256 Bit	$1{,}2 \cdot 10^{77}$	$4{,}4 \cdot 10^{57}$ Jahre

Das Alter des Universums liegt bei etwa 10^{10} Jahren. Auch "stärkere" Computer lösen das Problem der vollständigen Schlüsselsuche nicht, da diese dazu neigen auch sehr viel mehr Energie zu verbrauchen.

Angewandte Operationen

Oft wird vermutet, dass moderne Verschlüsselungsverfahren komplizierte mathematische Funktionen verwenden - das ist bei praktisch allen modernen Verfahren nicht der Fall. Die Verfahren operieren auf Blöcken von Bits, es kommen daher praktisch nur Bit-Operationen und deren Kombinationen zum Einsatz:

Zeichen	Name	Beispiel
$\oplus$	exklusives Oder	11100 $\oplus$ 10110 = 01010
+	Addition	1110 + 1011 = 1001
-	Subtraktion	1110 - 1011 = 0011
< <	Linksverschiebung	1100 < < 1 = 1000
< < <	Linksrotation	1110 < < < 2 = 1011
> >	Rechtsverschiebung	1110 > > 2 = 0011
> > >	Rechtsrotation	1110 > > > 2 = 1011
v	Oder	1110 v 1011 = 1111
$\wedge$	Und	1110 $\wedge$ 1011 = 1010
||	Konkatenation	1110 || 1011 = 11101011

Konfusion und Diffusion

- Zu verschlüsselnde Daten müssen unkenntlich gemacht werden: **Konfusion**
- Zu verschlüsselnde Daten müssen vermischt werden: **Diffusion**

Das Problem besteht natürlich auch darin, das auf eine solche Weise zu tun, dass der Vorgang bei Kenntnis des korrekten Schlüssels umkehrbar ist.

Zur Konfusion kommen häufig sogenannte S-Boxen zum Einsatz (S-Box), oft handelt es sich hierbei einfach um Ersetzungstabellen, die bestimmte Eingabebitfolgen in aus der S-Box abzuleitende Ausgabebitfolgen transformieren.

Rundenprinzip und Schlüsselaufbereitung

Um Speicherplatz zu sparen, arbeiten alle bekannten symmetrischen Blockchiffren nach dem Rundenprinzip. Eine Verschlüsselung wird dabei in Teilschritte (Runden) aufgeteilt, die im Wesentlichen identisch ablaufen.

In jeder Runde kommen normalerweise 3 Operationen zum Einsatz:

- Konfusion (S-Box)
- Diffusion
- Einbringen eines "Rundenschlüssels" mit einer Bitoperation

Um für jede Runde einen Rundenschlüssel zur Verfügung zu stellen, muss aus dem eigentlichen Schlüssel meist mehr Schlüsselmaterial erzeugt werden, als die Länge des eigentlichen Schlüssels hergibt, diesen Vorgang nenn man **Schlüsselaufbereitung**.

So benötigt man bei DES insgesamt 768BitsSchlüsselmaterial, da DES 16 Runden vorsieht und in jeder Runde ein 48Bit Schlüssel Eingang findet. Die Schlüssellänge eines DES Schlüssels ist jedoch nur 56Bit - es ist also ein Verfahren nötig, wie aus den 56bit des Schlüssels die benötigten 16 Subschlüssel der Länge 48Bit erzeugt werden können.