1.3 Kryptoanalyse von Zweifach-Chiffren

Der Treffpunkt-Angriff

Diese Attacke auf Zweifach-Chiffren wurde 1981 von Merkle und Hellman unter dem Namen „Meet in the Middle“ vorgestellt; sie ist nicht mit einem „Man in the Middle“-Angriff auf kryptographische Protokolle zu verwechseln, sondern ist eine Formalisierung eines Angriffs auf Mehrfach-Chiffren, der schon bei der Analyse von Rotormaschinen üblich war, siehe I.5.8.

Betrachtet wird die Komposition von zweimal der gleichen Chiffre mit verschiedenen Schlüsseln:

$$\begin{array}{ccccc} \Sigma^* & \xrightarrow{f_k} & \Sigma^* & \xrightarrow{f_h} & \Sigma^* \\ a & \mapsto & b & \mapsto & c. \end{array}$$

Sei ein bekanntes Klartext-Geheimtextpaar (a, c) gegeben. Dann bildet der Angreifer zwei Tabellen:

- alle $f_k(a)$, $k \in K$,
- alle $f_h^{-1}(c)$, $h \in K$,

und vergleicht diese. Jede Übereinstimmung ergibt ein mögliches Schlüsselpaar $(h, k) \in K^2$, das weiter getestet werden kann, etwa an einem weiteren bekannten Klartext.

Aufwand

Benötigt werden für diesen Angriff

- $2 \cdot \#K$ Verschlüsselungsoperationen (*nicht etwa* $(\#K)^2$!),
- $2 \cdot \#K$ Speicherplätze,

wobei die Zahl der nötigen Speicherplätze durch die Bemerkung halbiert wird, dass man nur eine der beiden Tabellen abspeichern muss.

Speichergrößen werden bekanntlich so bezeichnet:

2^{10}	2^{20}	2^{30}	2^{40}	2^{50}
Kilo	Mega	Giga	Tera	Peta

Dabei ist der Speicherbedarf – üblicherweise in Byte = Oktetten angegeben – noch mit der Größe eines Blocks des Verschlüsselungsverfahrens, etwa 64 Bit = 8 Byte, zu multiplizieren.

Man sieht, dass man schon mit 50-Bit-Schlüsseln in Größenbereiche kommt, die mit heutigen Speichertechniken nicht realisierbar sind. Da es bei der Kryptoanalyse allerdings mehr auf den Zeit- als auf den Speicherbedarf ankommt, ist die allgemeine Aussage gerechtfertigt:

Eine Zweifach-Chiffre ist nicht wesentlich sicherer als die zugrundeliegende Einfach-Chiffre. Insbesondere ist die Bitlänge für die exhaustive Schlüsselsuche bei weitem nicht verdoppelt sondern im wesentlichen nur um 1 Bit erhöht.

Fehlalarme

Eine Frage ist bei der Analyse offen geblieben: Wieviele der beim Tabellenabgleich gefundenen Übereinstimmungen führen zu einem falschen Schlüsselpaar? D. h., wie groß ist die Wahrscheinlichkeit eines Fehlalarms?

Dazu eine heuristische Überlegung: Gehen wir von einer Blockverschlüsselung von n-Bit-Blöcken mit l-Bit-Schlüsseln aus. Dann haben die Tabellen die Länge 2^l, es gibt also 2^{2l} Vergleiche. Da es 2^n verschiedene mögliche Werte gibt, kann man etwa $N_1 = 2^{2l-n}$ Übereinstimmungen erwarten. (Annahmen über die Zufälligkeit der Werte implizit. Die erste Übereinstimmung ist wegen des Geburtstagsphänomens nach etwa $2^{n/2}$ Versuchen zu erwarten, aber das nützt hier kaum.)

Probiert man die gefundenen Schlüsselpaare mit einem weiteren bekannten Klartext, so bleiben etwa $N_2 = N_1/2^n = 2^{2l-2n}$ Kandidaten übrig. Nach der Prüfung von insgesamt t bekannten Klartextblöcken kann man noch $N_t = 2^{2l-tn}$ Kandidaten erwarten – aber natürlich mindestens einen, nämlich den richtigen.

Eine eindeutige Lösung wird also im allgemeinen erreicht, wenn

$$t \geq \frac{2l}{n}.$$

Beispiele

1. DES, $n = 64$, $l = 56$: $N_1 = 2^{48}$, $N_2 = 2^{-16}$. *Es werden ungefähr* 2 *bekannte Klartextblöcke benötigt.*

2. IDEA, $n = 64$, $l = 128$: $N_1 = 2^{192}$, $N_2 = 2^{128}$, $N_3 = 2^{64}$, $N_4 = 1$. *Es werden ungefähr* 4 *bekannte Klartextblöcke benötigt.*

3. AES, $n = 128$, $l = 128$: $N_1 = 2^{128}$, $N_2 = 1$. *Es werden ungefähr* 2 *bekannte Klartextblöcke benötigt.* Allerdings ist wegen $\#K = 2^{128}$ die Zahl der benötigten Speicherplätze hier sehr weit außerhalb der Möglichkeiten (wie auch bei Beispiel 2).

Time-Memory-Tradeoff

Eine allgemeinere Überlegung führt zu einer Ausbalancierung von Zeit und Speicherplatz („Time-Memory-Tradeoff“): Man kann bei dem Treffpunkt-Angriff Speicherplätze auf Kosten von Rechenzeit sparen, wenn man nur Teiltabellen anlegt:

Hält man in einem Durchgang jeweils s Bits von h und k fest, so benötigt man jeweils 2^{l-s} Speicherplätze für die Tabellen der $f_k(a)$ bzw. $f_h^{-1}(c)$. Zur Kompensation muss man 2^{2s} solche Durchgänge mit je einem Tabellenpaar-Abgleich machen. Der Aufwand beträgt:

$2 \cdot 2^{l-s}$	Verschlüsselungsoperationen für ein Tafelpaar,
2^{2s}	Tafelpaar-Abgleiche, also insgesamt
$2 \cdot 2^{l+s}$	Verschlüsselungsoperationen,
$2 \cdot 2^{l-s}$	Speicherplätze.

Das Produkt aus der Anzahl der Verschlüsselungsoperation und der benötigten Speicherplätze ist $4 \cdot 2^{2l}$, unabhängig von s. *Der Angreifer kann also seine Ressourcen flexibel einsetzen.*

Beispiel DES: Hat der Angreifer 128 Terabyte Speicher zur Verfügung, so kann er 2 Tabellen von je 2^{40} Blöcken anlegen, also $s = 56 - 40 = 16$ wählen. Er benötigt dann insgesamt $2 \cdot 2^{72}$ Verschlüsselungsoperationen. Das liegt für den größten Geheimdienst der Welt zweifellos im Bereich des Machbaren.

Fazit: *Zweifach-Chiffren tragen zur Erhöhung der Sicherheit nicht lohnenswert bei.*