1.4 Dreifach-Chiffren

Die im vorigen Abschnitt gezeigte Schwäche der Zweifach-Chiffren führt dazu, dass man, wenn man eine Verstärkung braucht, zu Dreifach-Chiffren übergeht. Üblicherweise verwendet man das „EDE-Schema“ (Encryption, Decryption, Encryption)

$$f_g \circ f_h^{-1} \circ f_k \quad \text{für } g, h, k \in K.$$

Es hat den Vorteil, dass man mit der Schlüsselwahl $g = h = k$ die Kompatibilität mit der Einfach-Chiffre hat.

Der Treffpunkt-Angriff kann hier natürlich auch durchgeführt werden und ergibt, dass die Bitlänge für die vollständige Suche gegenüber der Einfach-Chiffre zwar nicht verdreifacht, aber doch immerhin (mehr als) verdoppelt ist.

Üblich ist auch ein vereinfachtes Schema: die Dreifach-Verschlüsselung mit zwei Schlüsseln:

$$f = f_k \circ f_h^{-1} \circ f_k \quad \text{für } h, k \in K.$$

Dieses Schema hat eine Schwäche bei einem Angriff mit gewähltem Klartext, die allerdings nur für Paranoiker bedenklich ist. Die Situation sei

$$\begin{array}{ccccccccc} \Sigma^* & \xrightarrow{f_k} & \Sigma^* & \xrightarrow{f_h^{-1}} & \Sigma^* & \xrightarrow{f_k} & \Sigma^*, \\ a & \mapsto & b & \mapsto & b' & \mapsto & c. \end{array}$$

Schritt 1: Mit $\#K$ Verschlüsselungsschritten und $\#K$ Speicherplätzen wird für jeden Zwischenwert b_0 die Tabelle

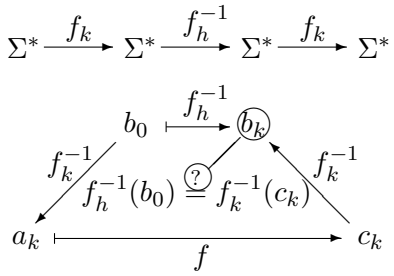
$$\{f_h^{-1}(b_0) \mid h \in K\}$$

vorausberechnet.

Schritt 2: Dann wird für alle Schlüssel $k \in K$ berechnet:

$$\begin{aligned} a_k &:= f_k^{-1}(b_0), \\ c_k &:= f(a_k), \\ b_k &:= f_k^{-1}(c_k); \end{aligned}$$

die zweite Zuweisung ist möglich, weil wir einen Angriff mit gewähltem Klartext durchführen, d. h., wir können f auf beliebige Klartexte anwenden. Das ganze benötigt $5 \cdot \#K$ einfache Verschlüsselungsschritte. Falls $b_k = f_k^{-1}(b_0)$, ist ein Kandidaten-Schlüsselpaar (h, k) gefunden, das weiter untersucht wird.



Der effizienteste bekannte Angriff wird beschrieben in:

- Van Oorschot/Wiener: A known plaintext attack on two-key triple encryption. Eurocrypt 90.