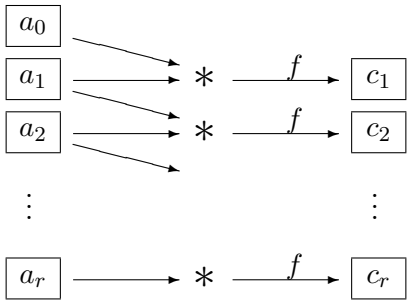
3.3 Varianten des CBC

Klartext-Autokey

Ersetzt man beim CBC das Geheimtext-Autokey-Verfahren durch Klartext-Autokey, so erhält man folgendes Schema:



welches man PBC = Plaintext Block Chaining nennen könnte.

Verschlüsselung: Die Verschlüsselung folgt nach Wahl eines Startwertes a_0 der Formel:

$$c_i := f(a_i * a_{i-1}) \quad \text{für } i = 1, \ldots, r.$$

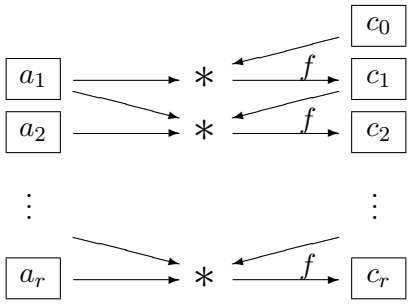
Entschlüsselung: Die Formel für die Entschlüsselung heißt:

$$a_i = f^{-1}(c_i) * a_{i-1}^{-1} \quad \text{für } i = 1, \ldots, r.$$

Dieses Verfahren ist allerdings völlig unüblich, und über seine Sicherheit ist anscheinend nichts bekannt.

PCBC = error-Propagating CBC

Dieses Verfahren ist ein Mix aus CBC und PBC und folgt dem Schema



Verschlüsselung: Die Verschlüsselung folgt (mit dem Startwert $a_0 =$ neutrales Element der Gruppe) der Formel:

$$c_i := f(a_i * a_{i-1} * c_{i-1}) \quad \text{für } i = 1, \ldots, r.$$

Für die Bitblock-Chiffrierung wird a_0 also als Nullblock gewählt.

Entschlüsselung: Die Formel für die Entschlüsselung heißt:

$$a_i = f^{-1}(c_i) * c_{i-1}^{-1} * a_{i-1}^{-1} \quad \text{für } i = 1, \ldots, r.$$

Dieses Verfahren wurde bei älteren Versionen von Kerberos verwendet, wegen gewisser Schwächen inzwischen jedoch aufgegeben.

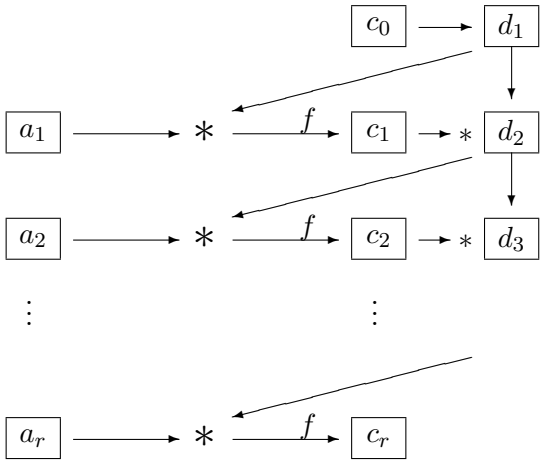
Verallgemeinerung nach MEYER/MATYAS

$$c_i := f(a_i * h(a_{i-1}, c_{i-1})) \quad \text{für } i = 1, \ldots, r,$$

wobei im Falle $\Sigma = \mathbb{F}_2^n$ z. B. für h die Addition modulo 2^n vorgeschlagen wird.

BCM = Block Chaining Mode

Diese Betriebsart folgt dem Schema:



Formel für die Verschlüsselung:

$$\begin{aligned} d_i &:= c_0 * \ldots * c_{i-1}, \\ c_i &:= f(a_i * d_i) \quad \text{für } i = 1, \ldots, r. \end{aligned}$$

Eine Anwendung des CBC

Der CBC-MAC (= „Message Authentication Code“) ist eine schlüsselabhängige „Hash-Funktion“, die zur Integritätsprüfung von Nachrichten verwendet wird. Sie ist in ISO/IEC 9797 normiert und mit dem DES-Verfahren im Bankenbereich verbreitet.

Sender und Empfänger einer Nachricht – die auch identisch sein können, wenn es sich um Nachrichtenspeicherung handelt – haben den Schlüssel k gemeinsam und verwenden die Verschlüsselungsfunktion $f = f_k$.

Der MAC eines Textes $a = (a_1, \ldots, a_r)$ ist der letzte Geheimtextblock, wenn a nach dem CBC verschlüsselt wird, also

$$\mathrm{MAC}(a) = c_r = f(a_r * f(a_{r-1} * \cdots f(a_1 * c_0) \ldots)).$$

Wird $\mathrm{MAC}(a)$ zusammen mit a verschickt, kann der Empfänger die Echtheit von Absender und Inhalt prüfen, denn nur wer den Schlüssel hat, kann diesen Wert richtig berechnen.

Der Nachteil des geteilten Geheimnisses k ist allerdings, dass in einem Rechtsstreit zwischen den beiden Parteien jeder dem anderen eine Fälschung unterstellen kann.