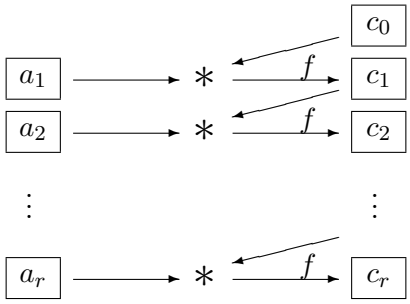
3.2 CBC = Cipher Block Chaining

Beschreibung

Mit einem zufällig gewähltem Startwert c_0 (auch IV = „Initialisierungsvektor“ genannt) sieht das Verfahren so aus:



Verschlüsselung: Beim CBC-Modus wird nach folgender Formel verschlüsselt:

$$\begin{aligned} c_i &:= f(a_i * c_{i-1}) \quad \text{für } i = 1, \ldots, r \\ &= f(a_i * f(a_{i-1} * \cdots f(a_1 * c_0) \ldots)). \end{aligned}$$

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

Eigenschaften

- Jeder Geheimtextblock hängt von *allen vorhergehenden* Klartextblöcken ab (Diffusion).
- Ein Angreifer kann Textblöcke nicht unbemerkt ersetzen oder einfügen.
- Gleiche Klartextblöcke werden im allgemeinen verschieden chiffriert.
- Ein Angriff mit bekanntem Klartext ist hingegen, im Vergleich zum ECB, nicht erschwert.
- Jeder Klartextblock hängt von zwei Geheimtextblöcken ab.
- D. h., bei fehlerhafter Übermittlung eines Geheimtextblocks werden (nur) zwei Klartextblöcke unleserlich (≫Selbstsynchronisation≪ des Verfahrens).

Frage: *Kann der Startwert c_0 bei Geheimhaltung als zusätzlicher Schlüssel dienen?* (Das wären im Beispiel DES aus 56 Bits des Schlüssels und 64 Bits des Startwerts insgesamt 120 Bits.)

Antwort: Nein!

Begründung: Nur a_1 hängt beim Entschlüsseln von c_0 ab, d. h., es wird lediglich bekannter Klartext am Anfang etwas besser verschleiert, wenn c_0 geheim bleibt. Ist der zweite oder ein späterer Klartextblock bekannt, kann der Angreifer wie bei EBC den Schlüssel bestimmen (durch vollständige Suche oder einen anderen Angriff mit bekanntem Klartext.

Bemerkungen

1. CBC ist die Komposition $f\circ$ (Geheimtext-Autokey). Ist also $f = \mathbf{1}_\Sigma$, so bleibt das (völlig untaugliche) Geheimtext-Autokey-Verfahren mit Schlüssellänge 1 übrig.

2. (John Kelsey in der Mail-Liste `cryptography@c2.net`, 24 Nov 1999) Falls eine „Kollision“ $c_i = c_j$ für $i \neq j$ auftritt, folgt $f(a_i * c_{i-1}) = f(a_j * c_{j-1})$, also $a_i * c_{i-1} = a_j * c_{j-1}$ und daraus $a_j^{-1} * a_i = c_{j-1} * c_{i-1}^{-1}$. Der Gegner gewinnt also etwas Information über den Klartext.

   Erwarten kann man diese Situation wegen des Geburtstagsphänomens nach ca. $\sqrt{\#\Sigma}$ Blöcken.

   Je länger der Text, desto mehr solcher Kollisionen sind zu erwarten. Auch dies bestätigt wieder die Faustregel über die Frequenz nötiger Schlüsselwechsel: rechtzeitig bevor $\sqrt{\#\Sigma}$ Blöcke erreicht sind.