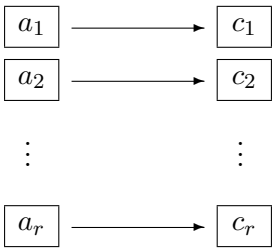
3.1 ECB = Electronic Code Book

Beschreibung

Sei r die Zahl der Blöcke, der Klartext also die Folge $(a_1, \ldots, a_r)$ von Blöcken.

Verschlüsselung: Beim ECB-Modus wird der Reihe nach einfach jeder Block für sich verschlüsselt:

$$a = (a_1, \ldots, a_r) \mapsto c = (c_1, \ldots, c_r) \in \Sigma^r \quad \text{mit } c_i = f(a_i).$$



Entschlüsselung: $a_i = f^{-1}(c_i)$.

Eigenschaften

Es handelt sich um eine monoalphabetische Substitution auf Σ. Falls $\#\Sigma$ sehr groß ist, ist das hinreichend sicher vor einem Geheimtextangriff. Nachteilig ist aber in jedem Fall:

- Information über identische Blöcke wird preisgegeben. Der Klartext ist zwar nicht zufällig, dennoch wird die Faustregel für das Geburtstagsphänomen hier oft interpretiert als: „Nach $2^{n/2}$ Bits beginnt beim ECB Information auszutreten.“ Durch die im folgenden behandelten Betriebsarten wird diese Grenze nach oben verschoben.

- Das Anlegen eines „Codebuchs“ aus bekannten Klartexten ist möglich. Bei strukturierten Nachrichten, z. B. Banktransaktionen, ist es ziemlich leicht, bekannte Klartextblöcke zu gewinnen.

- Ein aktiver Angriff durch Austausch oder Einschub einzelner Geheimtextblöcke (z. B. mit bekanntem, „sympathischen“ Klartext) ist möglich. Beispielsweise könnte ein Angreifer bei einer Banktransaktion, für die er weiß, in welchem Block der Empfänger definiert ist, diesen austauschen, um den Geldfluss umzuleiten. Was er dort hinschreiben muss, hat er aus einer früheren Transaktion als bekannten Klartextblock abgegriffen. Für diesen Angriff muss er den Schlüssel nicht kennen.

- Erlaubt die Situation einen Angriff mit gewähltem Klartext (Black-Box-Analyse), so ist Probeverschlüsselung bis hin zur Wörterbuch-Attacke möglich.

Besser ist es, eine Diffusion über die Klartextblöcke hinweg zu erzeugen. Das wird durch die im folgenden beschriebenen Betriebsarten erreicht.