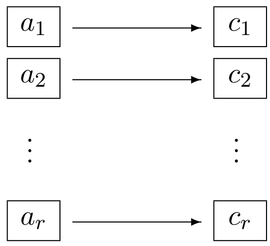
3.1 ECB = Electronic Code Book

Description

Let r be the number of blocks of the plaintext $(a_1, \ldots, a_r)$.

Encryption: In ECB mode each block is encrypted independently of the other blocks:

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



Decryption: $a_i = f^{-1}(c_i)$.

Properties

ECB mode simply is a monoalphabetic substitution on Σ. For sufficiently large $\#\Sigma$ this is secure from a ciphertext-only attack. But there are several disadvantages:

- ECB encryption leaks information on identical blocks. Even if the plaintext is not random, the rule of thumb from the Birthday Paradox applies in the interpretation (for $\Sigma = \mathbb{F}_2^n$): "After $2^{n/2}$ bits ECB encryption begins to leak information." Wikipedia has a nice illustration of this effect, see `http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation` The other modes significantly enlarge this bound.
- Building a "codebook" from known plaintext blocks is not unrealistic. For structured messages, say bank transactions, there occur many blocks of known plaintext.
- An active attack by exchanging or inserting single blocks of ciphertext (for example with known, "sympathic" plaintext) is possible. For example an attacker who knows which block contains the receiver of a money transfer could exchange this block with a corresponding block from another transfer for another receiver. He doesn't need to know the key.

- If the situation allows for an attack with *chosen* plaintext (as in a black box analysis), trial encryption and dictionary attacks can be mounted.

In view of these problems generating diffusion between the plaintext blocks seems a much better approach. In the following sections we look at modes of operation that achieve this effect.