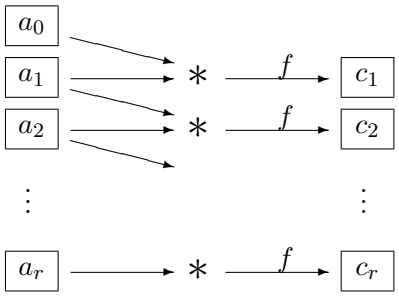
3.3 Variants of CBC

Plaintext Autokey

Replacing the ciphertext autokey encryption for CBC mode by plaintext autokey yields the following scheme:



that sometimes is called PBC = Plaintext Block Chaining.

Encryption: After choosing an initialization vector a_0 the formula for encryption is:

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

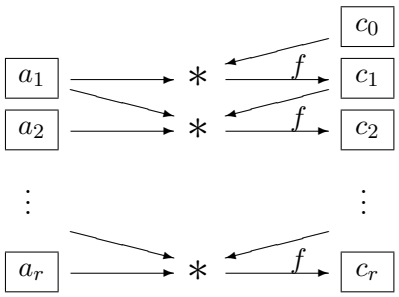
Decription: The formula is:

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

However this method seems not to be in widely accepted use, and there seem to be no relevant results on its security.

PCBC = error-Propagating CBC

This procedure mixes CBC and PBC. It follows the scheme:



Encryption: After choosing the initialization vector $a_0 = e$ (neutral element of the group) encryption is by the formula

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

In the case of a bitblock cipher we choose $a_0 = 0$, the null block.

Decryption: The formula is

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

This mode was implemented in early versions of Kerberos but then abandoned.

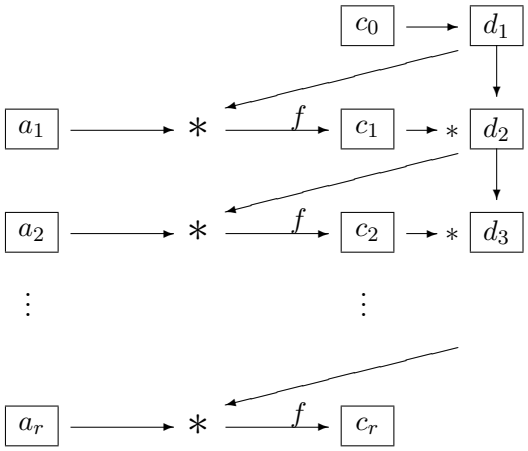
Generalization by Meyer/Matyas

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

where in the case $\Sigma = \mathbb{F}_2^n$ addition modulo 2^n is suggested for h.

BCM = Block Chaining Mode

This mode follows the scheme:



Formula for encryption:

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

An Application of CBC

CBC-MAC (= "Message Authentication Code") is a key-dependent "hash function" that serves for checking the integrity of messages. It is standardized in ISO/IEC 9797 and used in electronic banking.

Sender and receiver of the message—these could be the same person if the MAC used for securing the integrity of a stored file—share the key k and use the encryption function $f = f_k$.

The MAC of a text $a = (a_1, \ldots, a_r)$ is the last ciphertext block where a is encrypted in CBC mode. Hence

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

If $\mathrm{MAC}(a)$ is sent together with a, then the receiver may check the authenticity of the sender and the integrity of the content. Only someone who has the key can calculate this value correctly.

The disadvantage of this procedure is the need of sharing a secret k. In a legal dispute each of the two parties can contend a forgery by the other one.