

Mandatory

- Proprietary Entry Name : ACR {ISO standard 9979 acr (15)}
- Intended Range of Applications
 - Confidentiality : yes
 - Authentication : yes
 - Data Integrity : yes
 - Digital Signature : yes
 - Hash Function : yes
- Cryptographic Interface Parameters
 - Input Size : 64 bits
 - Output Size : 64 bits
 - Key Length : 128 bits
- Test Words :
 1. Let $\text{block}_0 = (01,02,03,04,05,06,07,08)$ denote a vector of 8 bytes.
 2. Let block_{i+1} be the result of the encipherment of block_i using the cryptographic algorithm ACR in Electronic Code Book mode under the key (0F,0E,0D,0C,0B,0A,09,08,07,06,05,04,03,02,01,00).
 3. Then $\text{block}_{1024} = (08,F8,47,E3,A5,C0,35,1D)$.
- Name of Sponsoring Authority : AFNOR
- Date of Registration : ~~April 1997~~ 8th May 1997
- Subject of a National Standard : no
- Patent Licence Restrictions : no

Optional

- Modes of Operation
 - Electronic Code Book : yes
 - Cipher Feedback : yes
 - Cipher Block Chaining : yes
 - Output Feedback : yes
 - Additive Stream Cipher : yes
 - Black Box : yes
- Other Information
 - Design Rules : block cipher
 - Specific Systems : in use by major French companies
 - Guidance on key selection : no restriction