

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|------|-----------|-----------|-----------|---|---|---|---|-----------|---|---|---|---|---|----|---|---|
| 0x00 | * | Message 1 | | | | | | | | | | | | M2 | | |
| 0x10 | Message 2 | | | | | | | Message 3 | | | | | | | | |
| 0x20 | Message 3 | | | | | | | | | | | | | | | |
| 0x30 | M3 | | Message 4 | | | | | | | | | | | | | |
| ⋮ | | | | | | | | | | | | | | | | |

* Config Byte

Stores number
of messages

BlockCipherContext (128 bytes)

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | |
|------|------------------------|---|---|---|---------------|---|---|---|----------------------------|---|---------------|--|
| 0x00 | api (BlockCipherApi *) | | | | | | | | block_size | | | |
| 0x10 | key_len | | | | | | | | round_keys [96] (LEA) | | | |
| | | | | | | | | | round_keys [60] (AES/ARIA) | | | |
| 0x20 | | | | | | | | | | | | |
| 0x30 | | | | | | | | | | | | |
| 0x40 | | | | | | | | | | | | |
| 0x50 | | | | | nr (AES/ARIA) | | | | | | | |
| 0x60 | | | | | | | | | | | | |
| 0x70 | | | | | | | | | nr (LEA) | | padding (LEA) | |

BlockCipherApi (vtable, 40 bytes)

| BlockCipher API (vtable, 48 bytes) | | | | | | | | | | | | |
|------------------------------------|---------------|---|---|---|---|---|---------------|---|---|---|---|--|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | |
| 0x00 | name | | | | | | init | | | | | |
| 0x10 | encrypt_block | | | | | | decrypt_block | | | | | |
| 0x20 | dispose | | | | | | aes_dispose | | | | | |

Diagram illustrating the BlockCipher API (vtable, 48 bytes) structure and its mapping to functions:

- name** (0x00 - 0x06) points to **init**.
- init** (0x07 - 0x0C) points to **aes_init**.
- encrypt_block** (0x0D - 0x14) points to **aes_encrypt**.
- decrypt_block** (0x15 - 0x1C) points to **aes_decrypt**.
- dispose** (0x1D - 0x24) points to **aes_dispose**.

"AES"

aes_init

aes_decrypt

aes_encrypt

aes_decrypt

aes_dispose