**CRC-32 specification to protect Encrypted Key Block in the OTAR procedure of the Extended Procedures**

# CRC-32 Encrypted Key Block Error Control Field Coding Procedures

## Conventions

The following convention is used to identify each bit in an *N*-bit field. The first bit in the field to be transmitted (i.e., the most left justified when drawing a figure) is defined to be ‘Bit 0’; the following bit is defined to be ‘Bit 1’ and so on up to ‘Bit *N*–1’. When the field is used to express a binary value (such as a counter), the Most Significant Bit (MSB) shall be the first transmitted bit of the field, i.e., ‘Bit 0’ (see figure 1‑1).



Figure 1‑1 : Bit Numbering Convention

## CRC-32 Encoding Procedure

For the encoding procedure, the (*n–*32)-bit Encrypted Key Block shall be the information message.

The encoding procedure shall accept an (*n–*32)-bit Encrypted Key Block and generate a systematic binary (*n*,*n*–32) block code by appending a 32-bit Cyclic Redundancy Check (CRC-32) as the final 32 bits of the Encrypted Key Block.

NOTES

1. The Bit Numbering Convention as specified in 1.1 is applicable below.

If M(*X*) is the (*n*–32)-bit information message to be encoded expressed as a polynomial with binary coefficients, with the first bit transferred being the most significant bit M0 taken as the coefficient of the highest power of *X,* then the equation for the 32-bit Cyclic Redundancy Check, expressed as a polynomial R(*X*) with binary coefficients, shall be:

R(*X*) = [*X*32 ∙ M(*X*)] modulo G(*X*)

where G(*X*) is the generating polynomial given by:

G(*X*) = *X*32 + *X*23 + *X*21 + *X*11 + *X*2 + 1

and where the first transferred bit of the Cyclic Redundancy Check is the most significant bit R0 taken as the coefficient of the highest power of *X*.

The *n*-bit CRC-32-encoded block, expressed as a polynomial C(*X*) with binary coefficients, shall be:

C(*X*) = *X*32 ∙ M(*X*) + R(*X*)

The (*n*–32) bitsof the message are input in the order *M*0,…, *Mn*−33, and the *n* bits of the codeword are output in the order *C*0,…, *Cn*−1 = *M*0,…, *Mn*−33, *R*0,…, *R*31.

NOTE – A possible implementation of an encoder is described in figure B‑3. For each frame, the shift register is preset to the ‘all zero’ state prior to encoding. This initialization differs from that performed for the 16-bit CRC described in other CCSDS books, for which the cells are initialized to all ‘ones’. The ganged switch is in position 1 while the information bits are being transferred and in position 2 for the 32 Cyclic Redundancy Check bits.



**Figure** **B‑3** **: A Possible Implementation of the CRC-32 Encoder**

**CRC-32 Decoding Procedure**

The decoding procedure shall accept an *n*-bit received codeword, including the 32-bit Cyclic Redundancy Check, and generate a 32-bit syndrome.

An error shall be detected if and only if at least one of the syndrome bits is non-‘zero’.

The received block C\*(*X*) shall equal the transmitted codeword C(*X*) plus (modulo two) the *n*-bit error block E(*X*), C\*(*X*) = C(*X*) + E(*X*), where both are expressed as polynomials of the same form, i.e., with the most significant bit C0 or E0 taken as the binary coefficient of the highest power of *X*.

With C\*(*X*) being the *n*-bit received codeword with the first transferred bit being the most significant bit C0\* taken as the coefficient of the highest power of *X*, then the equation for the 32-bit syndrome, expressed as a polynomial S(*X*) with binary coefficients, shall be:

S(*X*) = [*X*32 ∙ C\*(*X*)] modulo G(*X*)

The syndrome polynomial will be ‘zero’ if no error is detected, and non-‘zero’ if an error is detected, with the most significant bit S0 taken as the coefficient of the highest power of *X*.

NOTE – A possible implementation of the syndrome polynomial generator is described in figure B‑4. For each frame, the shift register cells are initialized to ‘zero’. This initialization differs from that performed for the 16-bit CRC described in other CCSDS books, for which the cells are initialized to ‘all ones’. The codeword includes *n* bits, i.e., (*n*–32) information message bits plus the 32 bits of the Cyclic Redundancy Check. All the *n* bits of the codeword are clocked into the input and then the storage stages are examined. For an error-free block, the contents of the shift register cells will be zero. A non-zero content indicates an erroneous block.

****

**Figure** **B‑4** **: A Possible Implementation of the CRC-32 Decoder**