CYCLIC CODES

- Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.
- For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword. In this case, if we call the bits in the first word *ao* to *a6'* and the bits in the second word *bo* to *b6*, we can shift the bits by using the following:

$$b_1 = a_0 \quad b_2 = a_1 \quad b_3 = a_2 \quad b_4 = a_3 \quad b_5 = a_4 \quad b_6 = a_5 \quad b_0 = a_6$$

Cyclic Redundancy Check

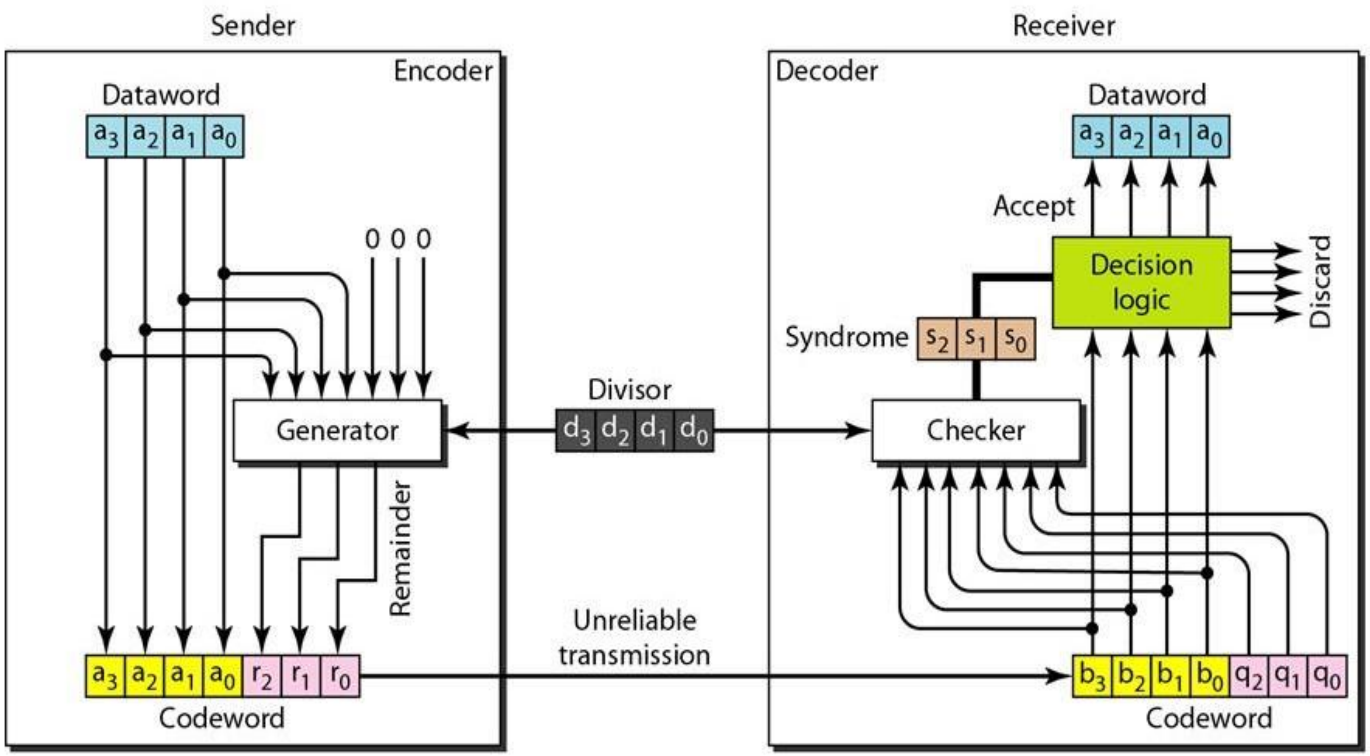
- A cyclic redundancy check (CRC) is an error-detecting code.
- used in networks such as LANs and WANs.

- Dataword is K bits(4 here)
- Codeword has **n** bits(7 here)
- Augumented bits n-k (7-4=3)
- Divisor size is n-k+1 (7-4+1=4)

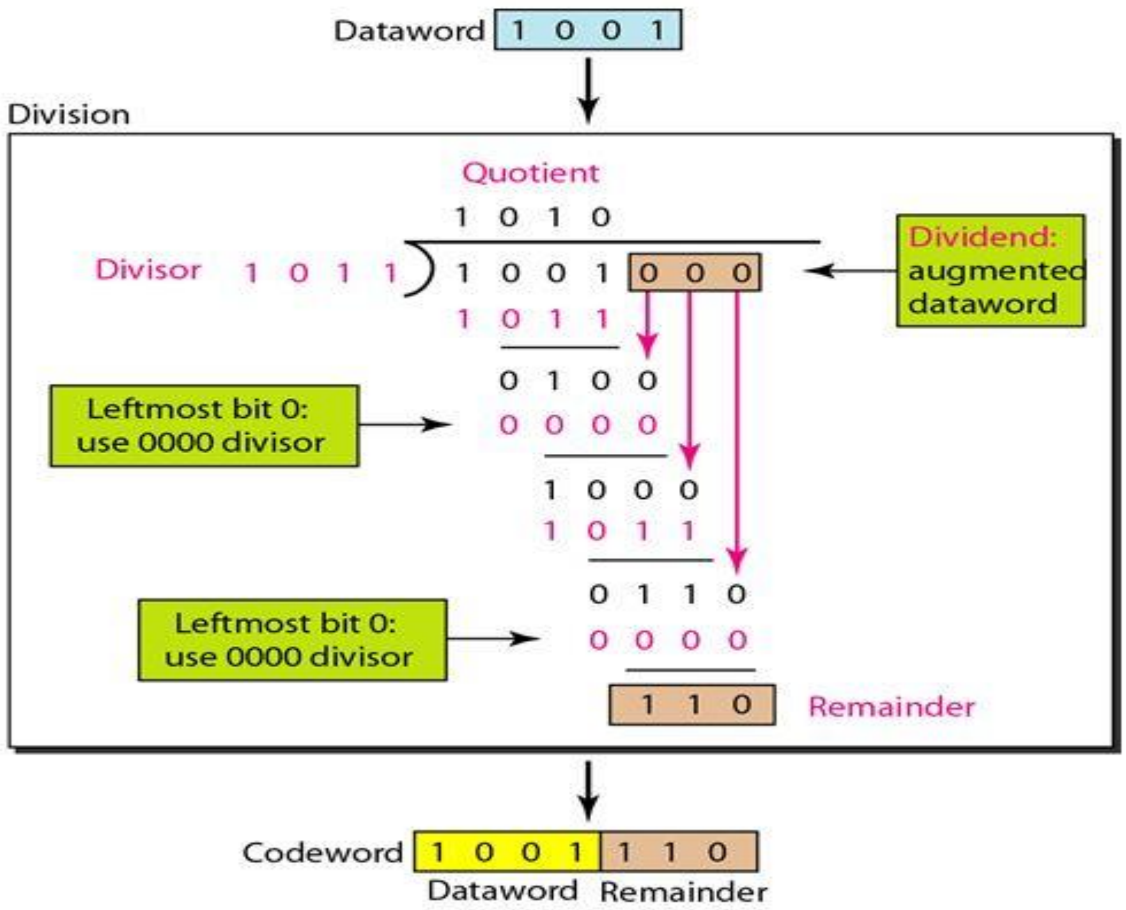
Table: A CRC code with C(7, 4)

Dataword	Codeword	Dataword	Codeword
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

Figure *CRC encoder and decoder*



Division in CRC encoder



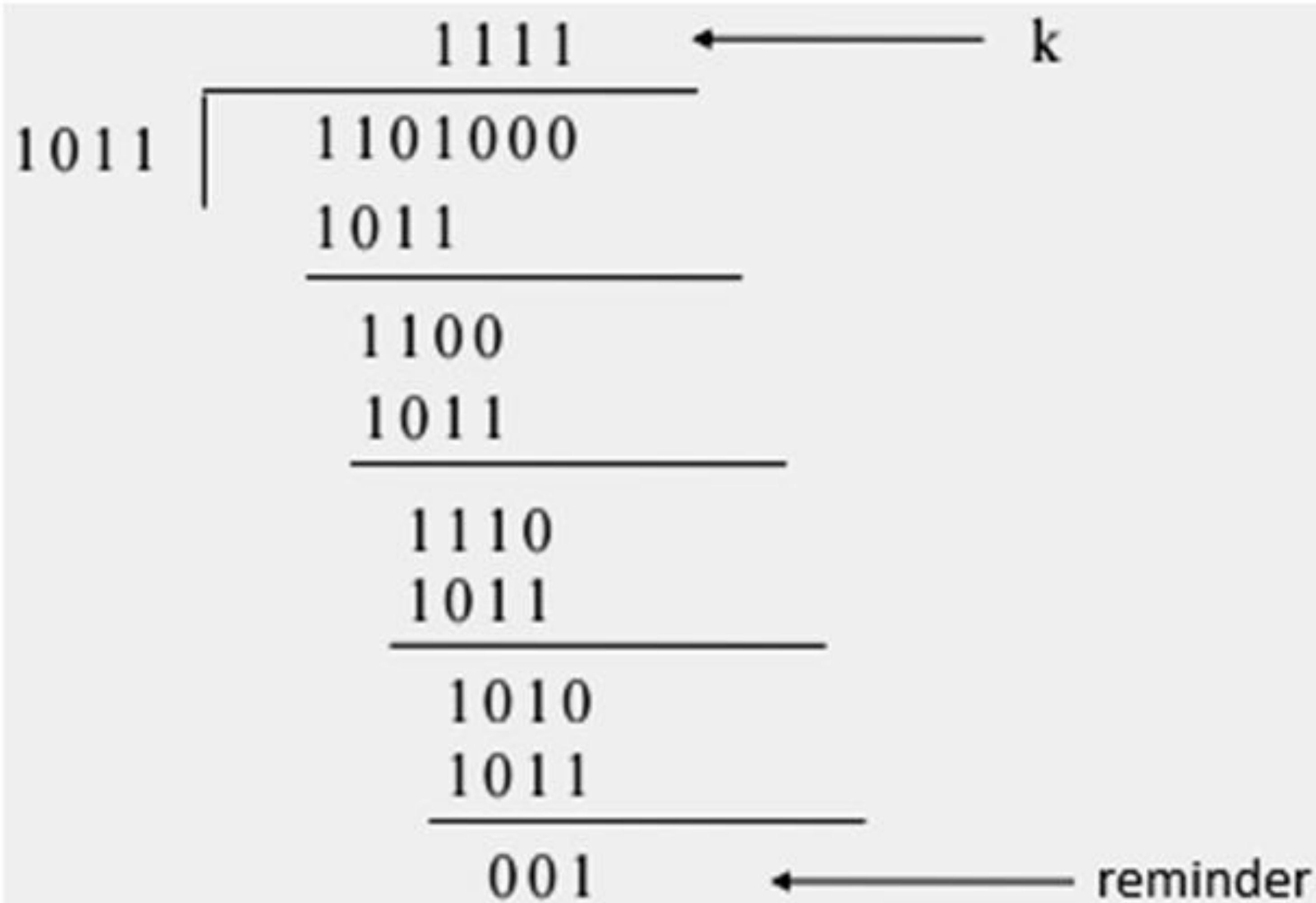
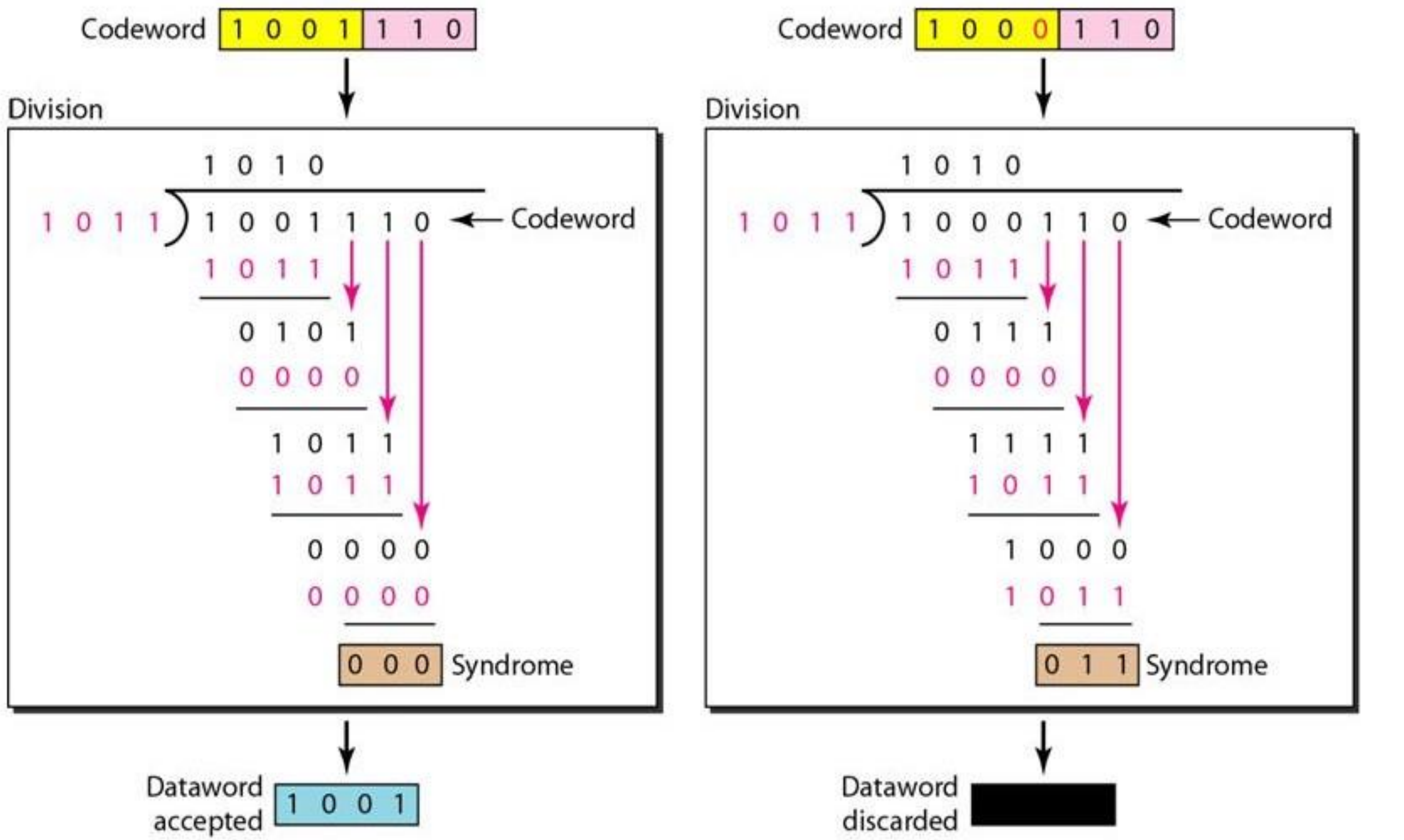

1111
k
1011
1101000
1011
1100
1011
1110
1011
1010
1011
001
reminder

Figure *Division in the CRC decoder for two cases*

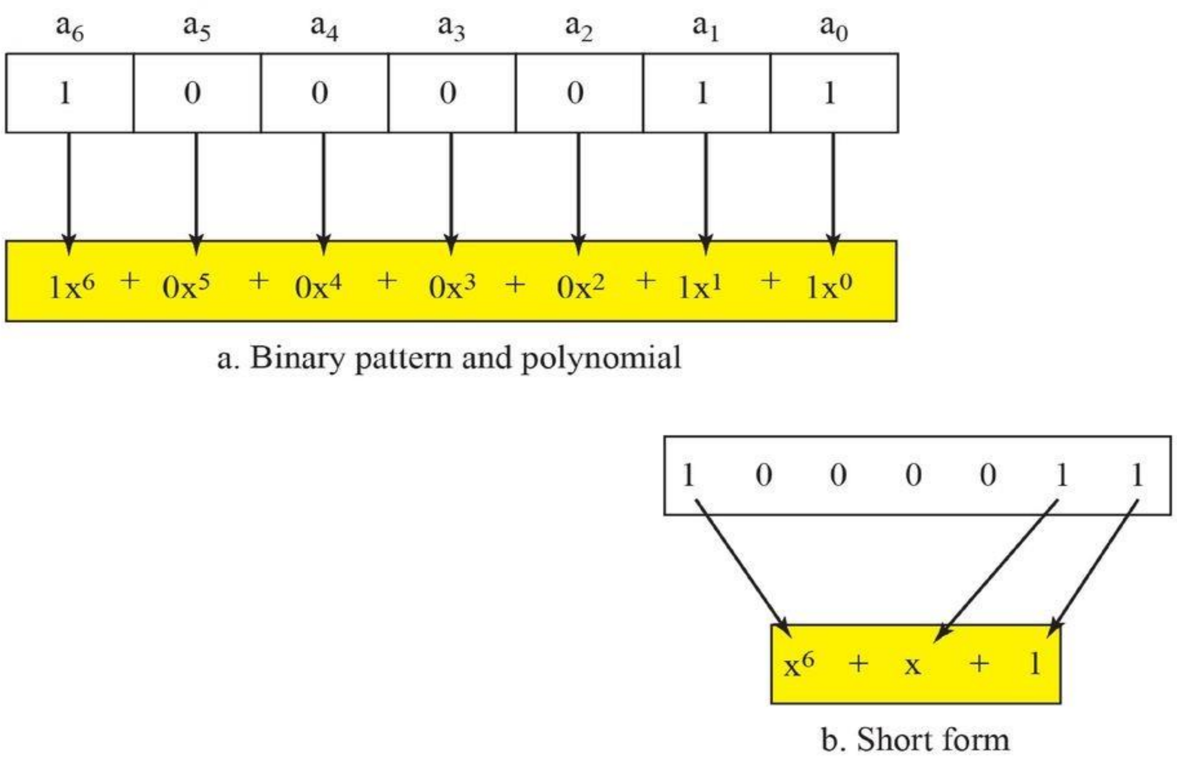


Polynomials

- A better way to understand cyclic codes and how they can be analyzed is to represent them as p.olynomials

FIGURE:

A polynomial to represent a binary word



Degree of a Polynomial

- The degree of a polynomial is the highest power in the polynomial. For example, the degree of the polynomial $x6 + x + 1$ is 6.

- Note that the degree of a polynomial is 1 less that the number of bits in the pattern. The bit pattern in this case has 7 bits.

Adding and Subtracting Polynomials

- First, addition and subtraction are the same. Second, adding or subtracting is done by combining terms and deleting pairs of identical terms.

- For example, adding $x^5 + x^4 + x^2$ and $x^6 + x^4 + x^2$ gives just $x^6 + x^5$. The terms x^4 and x^2 are deleted. However, note that if we add, for example, three polynomials and we get x^2 three times, we delete a pair of them and keep the third.

Multiplying or Dividing Terms

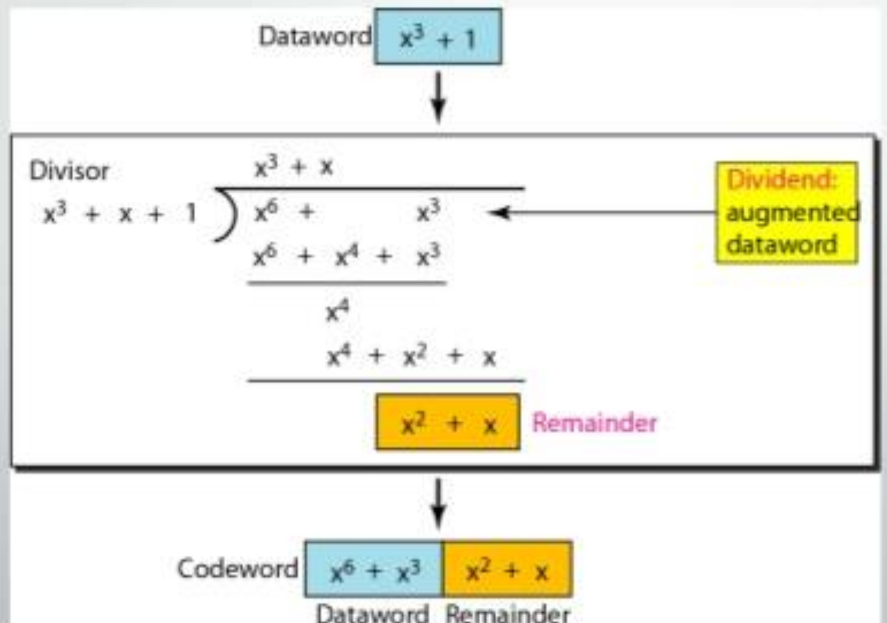
- In this arithmetic, multiplying a term by another term is very simple; we just add the powers. For example, x^3 x x^4 is x^7 .
- For dividing, we just subtract the power of the second term from the power of the first. For example, x^5 / x^2 is x^3.

Multiplying Two Polynomials

Multiplying a polynomial by another is done term by term. Each term of the first polyno- mial must be multiplied by all terms of the second. The result, ofcourse, is then simplified, and pairs of equal terms are deleted. The following is an example:

$$(x^5+x^3+x^2+x)(x^2+x+1)$$
$$=x^7+x^6+x^5+x^5+x^4+x^3+x^4+x^3+x^2+x^3+x^2+x$$
$$=x^7+x^6+x^3+x$$

CRC DIVISION USING POLYNOMIALS



EXAMPLE 2

Generator (divisor) polynomial: $g(x) = x^3 + x + 1$

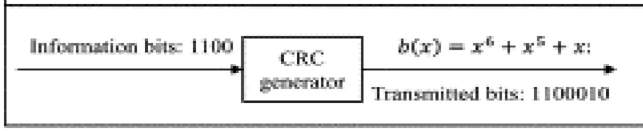
Information polynomial: $i(x) = x^3 + x^2$

Dividend polynomial: $p(x) = x^3 i(x) = x^6 + x^5$

$$
\begin{array}{r|l}
 & x^3 + x^2 + x \\
\hline
x^3 + x + 1 & x^6 + x^5 \\
 & x^6 + x^4 + x^3 \\
\hline
 & x^5 + x^4 + x^3 \\
 & x^5 + x^3 + x^2 \\
\hline
 & x^4 + x^2 \\
 & x^4 + x^2 + x \\
\hline
 & x
\end{array}
$$

Remainder polynomial: $r(x) = x$

Transmitted polynomial: $b(x) = p(x) + r(x) = x^6 + x^5 + x$



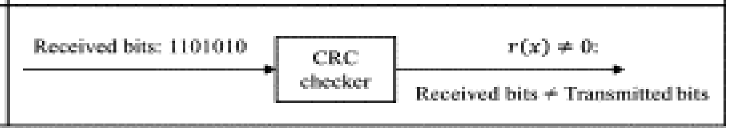
CRC generator at the transmitter

Generator (divisor) polynomial: $g(x) = x^3 + x + 1$

Received (dividend) polynomial: $b'(x) = x^6 + x^5 + x^3 + x$

$$
\begin{array}{r|l}
 & x^3 + x^2 + x + 1 \\
\hline
x^3 + x + 1 & x^6 + x^5 + x^3 + x \\
 & x^6 + x^4 + x^3 \\
\hline
 & x^5 + x^4 + x \\
 & x^5 + x^3 + x^2 \\
\hline
 & x^4 + x^3 + x^2 + x \\
 & x^4 + x^2 + x \\
\hline
 & x^3 \\
 & x^3 + x + 1 \\
\hline
 & x + 1
\end{array}
$$

Remainder polynomial: $r(x) = x + 1$



CRC checker at the receiver


Thank you