# CRC Algorithm

## Cyclic_redundancy check:

The CRC is a complex algorithm derived from the CHECKSUM error detection algorithm, using the MODULO algorithm as the basis of operation. It is based on the value of polynomial coefficients in binary format for performing the calculations. For Example: x2+x+1 (polynomial equation)

## Another definition:

CRC or Cyclic Redundancy Check is a method of detecting accidental changes/errors in the communication channel.
CRC uses **Generator Polynomial** which is available on both sender and receiver side. An example generator polynomial is of the form like $x^3 + x + 1$. This generator polynomial represents key 1011. Another example is $x^2 + 1$ that represents key 101.

```
n : Number of bits in data to be sent
    from sender side.
k : Number of bits in the key obtained
    from generator polynomial.
```

### Sender Side (Generation of Encoded Data from Data and Generator Polynomial (or Key)):

1. The binary data is first augmented by adding k-1 zeros in the end of the data
2. Use ***modulo-2 binary division*** to divide binary data by the key and store remainder of division.
3. Append the remainder at the end of the data to form the encoded data and send the same

**Receiver Side (Check if there are errors introduced in transmission)**
Perform modulo-2 division again and if the remainder is 0, then there are no errors.
In this article we will focus only on finding the remainder i.e. check word and the code word.

#### What is CRC 32 algorithm used for?

CRC32 is a popular checksum algorithm used to detect data corruption. Multiple variants of the algorithm exist which have similar mathematical properties.

## Modulo 2 Division:

The process of modulo-2 binary division is the same as the familiar division process we use for decimal numbers. Just that instead of subtraction, we use XOR here.

- In each step, a copy of the divisor (or data) is XORed with the k bits of the dividend (or key).
- The result of the XOR operation (remainder) is (n-1) bits, which is used for the next step after 1 extra bit is pulled down to make it n bits long.
- When there are no bits left to pull down, we have a result. The (n-1)-bit remainder which is appended at the sender side.

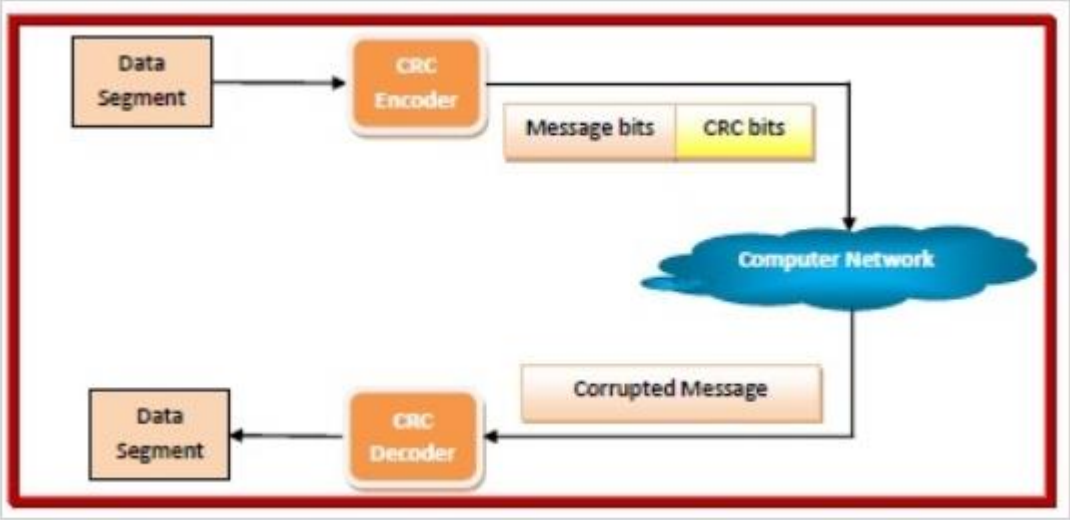
## Types of CRC:

The most commonly used polynomial lengths are 9 bits (CRC-8), 17 bits (CRC-16), 33 bits (CRC-32), and 65 bits (CRC-64). A CRC is called an n-bit CRC when its check value is n-bits.

### Computation of CRC:

When messages are encoded using CRC (polynomial code), a fixed polynomial called generator polynomial,*GG(x)* is used. The value of is mutually agreed upon by the sending and the receiving parties. A *k* – bit word is represented by a polynomial which ranges from $X^0$ to $x^{k-1}$. The order of this polynomial is the power of the highest coefficient, i.e.(K-1) The length of *G(x)* should be less than the length of the message it encodes. Also, both its MSB (most significant bit) and LSB (least significant bit) should be 1. In the process of encoding, CRC bits are appended to the message so that the resultant frame is divisible by *G(x)*.

- **algorithm for Encoding using CRC**
    - The communicating parties agrees upon the size of message,*M(x)* and the generator polynomial, *G(x)*.
    - If *r* is the order of *G(x)*,*r*, bits are appended to the low order end of *M(x)*. This makes the block size bits, the value of which is $x^rM(x)$.
    - The block $x^rM(x)$ is divided by *G(x)* using modulo 2 division.
    - The remainder after division is added to $x^rM(x)$ using modulo 2 addition. The result is the frame to be transmitted, *T(x)*. The encoding procedure makes exactly divisible by *G(x)*.




- **Algorithm for Decoding using CRC**
    - The receiver divides the incoming data frame T(x) unit by G(x) using modulo 2 division. Mathematically, if E(x) is the error, then modulo 2 division of [*M(x)* + *E(x)*] by *G(x)* is done.
    - If there is no remainder, then it implies that *E(x)*. The data frame is accepted.
    - A remainder indicates a non-zero value of E(x), or in other words presence of an error. So the data frame is rejected. The receiver may then send an erroneous acknowledgment back to the sender for retransmission.