Assignment 1: Implement Cyclic Redundancy Check (CRC)

Submission due: 4th week of January 2018

CRC is a technique for detecting errors in digital data, but not for making corrections when errors are detected. It is used primarily in data transmission. In the CRC method, a certain number of check bits, often called a checksum, are appended to the message being transmitted. The receiver can determine whether or not the check bits agree with the data. The CRC is based on polynomial arithmetic, in particular, on computing the remainder of dividing one polynomial by another.

Since every file or message can be thought of as a single pattern of bits it can be treated as a single large binary number. The CRC technique makes use of a polynomial divisor of length n+1 to divide the source number – discarding the quotient and using the remainder as the checksum for that message. The result of the CRC algorithm is a check value that can be used to determine whether or not the file or message being examined is the same file or message that was used to create the check value.

There are many polynomial divisors of different lengths used to calculate CRCs as shown in the table below.

In this assignment, you have to implement a CRC scheme of your choice from the table below. You can write the program in any language. The checksum program should accept the name of a test file (contains a sequence of frames) from the command line and then print your signature block and the correct checksum on console standard output. Next, test the same program to produce a PASS/FAIL result.

Please note that your selection of CRC scheme can help you to make your assignment different from your classmates. Write the code by yourself and protect your code. The assignment is simple, but we encourage you to do improvisation with this.

Polynomial Name	Polynomial	Use
CRC-1	$x + 1$	Parity
CRC-4-ITU	$x^4 + x + 1$	ITU G.704
CRC-5-ITU	$x^5 + x^4 + x^2 +1$	ITU G.704
CRC-5-USB	$x^5 + x^2 + 1$	USB
CRC-6-ITU	$x^6 + x + 1$	ITU G.704
CRC-7	$x^7 + x^3 + 1$	Telecom systems, MMC
CRC-8-ATM	$x^8 + x^2 + x + 1$	ATM HEC
CRC-8-CCITT	$x^8 + x^7 + x^3 + x^2 + 1$	1-Wire bus
CRC-8-Maxim	$x^8 + x^5 + x^4 + 1$	1-Wire bus
CRC-8	$x^8 + x^7 + x^6 + x^4 + x^2 + 1$	General
CRC-8-SAE	$x^8 + x^4 + x^3 + x^2 + 1$	SAE J1850
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x + 1$	General
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$	Telecom systems
CRC-15-CAN	$x^{15} + x^{14} + x^{10} + x^8 + x^7 + x^4 + x^3 + 1$	CAN
CRC-16-CCITT	$x^{16} + x^{12} + x^5 + 1$	XMODEM,X.25, V.41, Bluetooth, PPP, IrDA, CRC-CCITT
CRC-16	$x^{16} + x^{15} + x^2 + 1$	USB
CRC-24-Radix64	$x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$	General
CRC-32-IEEE802.3	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	Ethernet, MPEG2
CRC-32C	$x^{32} + x^{28} + x^{27} + x^{26} + x^{25} + x^{23} + x^{22} + x^{20} + x^{19} + x^{18} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^6 + 1$	General
CRC-32K	$x^{32} + x^{30} + x^{29} + x^{28} + x^{26} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{11} + x^{10} + x^7 + x^6 + x^4 + x^2 + x + 1$	General
CRC-64-ISO	$x^{64} + x^4 + x^3 + x + 1$	ISO 3309
CRC-64-ECMA	$x^{64} + x^{62} + x^{57} + x^{55} + x^{54} + x^{53} + x^{52} + x^{47} + x^{46} + x^{45} + x^{40} + x^{39} + x^{38} + x^{37} + x^{35} + x^{33} + x^{32} + x^{31} + x^{29} + x^{27} + x^{24} + x^{23} + x^{22} + x^{21} + x^{19} + x^{17} + x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^4 + x +1$	ECMA-182