Homework Number: 4
Name: Dylan Huynh
ECN login: huynh38
Due Date: 2/14/2023

1. a) $(9x^5 +4x^4 +8x^3 +2x^2 +3x+4)+(6x^5 +2x^4 +9x^3 +7x^2 +5x+7)$
$= (15x^5 + 6x^4 + 17x^3 + 9x^2 + 8x + 11) \bmod 11$
$= \mathbf{(4x^5 + 6x^4 + 6x^3 + 9x^2 + 8x)}$

b) $(8x^3 +6x^2 +8x+1)\times(3x^3 +9x^2 +7x+5)$
$= (24x^6 +18x^5 +24x^4+3x^3) + (72x^5 +54x^4 +72x^3+9x^2) + (56x^4 +42x^3 +56x^2+7x) + (40x^3 +30x^2 +40x+5)$
$= (2x^6 +7x^5 +2x^4+3x^3) + (6x^5 +10x^4 +6x^3+9x^2) + (x^4 +9x^3 +x^2+7x) + (7x^3 +8x^2 +7x+5)$
$= (2x^6 +13x^5 +13x^4+3x^3 +8x^2 +7x+5)$
$\mathbf{= (2x^6 +2x^5 +2x^4+3x^3 +8x^2 +7x+5)}$

c) $(3x^3 -5x^2 +10x-3) / 3x + 1$
First line x^2 so first line of subtraction is $(3x^3 - 5x^2) - (3x^3 + x^2) = -6x^2 \bmod 11 = 5x^2$
$5x^2 + 10x - 3 / 3x + 1$ next value is x so subtraction is $(5x^2 + 10x) - (3x^2 + x) = 2x^2 + 9x$
$(2x^2 + 9x - 3) / (3x + 1)$ $3x + 1$ goes into $9x -3$ three times so subtraction is $2x^2 + 9x-3 - 9x - 3 = -6 \bmod 11 = 2x^2 + 5$
Quotient = $\mathbf{(x^2 + x + 3) + (2x^2 + 5) / (3x + 1)}$

2. a) 111 x 110 = 11100 + 1110 = 10010 = $x^4 + x \bmod x^3 + x + 1$
$x^4 + x - x^4 - x^2 - x = \mathbf{x^2}$

b) 100 - 111 = 011 |
x + 1

c) 111 / 101 $x^2 + x + 1 / x^2 + 1 = 1$
$x^2 + x + 1 - x^2 - 1 = x$
$\mathbf{= 1 + x/(x^2 + 1)}$

In the code, I first encrypt or decrypt based on the input. Both functions initialize blocks of 128 bits depending on their input file type, the round keys are generated using the lecture code, which are made by XORing the previous word, with the calculated gee factored in, and the respective word from the last 4 word set. Gee is calculated by rotating the 4 byte word by a byte, using the byte substitution table (which I precalculated instead of calculating in the program), and then XORRing with the round constant. One adding of the round keys is done, and then for the 4 rounds, in encryption

the order is substitution of the bytes, shifting the rows, mixing the columns, and then adding the round key, whereas in decryption, it is inverse shifting the rows, inverse substitution of the bytes, adding the round keys in reverse order, and then inverse mixing of the columns. As mentioned previously, both substitution tables for the sub_bytes step was precalculated as the table is constant, so the function just finds the complement for the value by using the value as the index to the corresponding table. For row shifting, the rows are shifted by the row index to the left, (for example, row 2 is shifted by 2 to the left), and for the inverse the rows are shifted by the row index to the right. For column mixing, although the coefficients are different for the inverse and regular, they are both 4 modular multiplications and 3 XORs within a column, so I just but the corresponding 2, 3, 1, 1 coefficients to the correct values depending on which row they were in and for inverse I did the same using E, B, D, and 9. The last round does not include the mixing and inverse mixing steps, respectively. Then the algorithm just formats the output according to specifications and then writes out.

The encryption is
2bd280a572d58f866b407a63e2ac60a4a58e4f16d71808c75b85a3188aa78de70453883
720af225915d84feff6fc415edfd642d338f4d61f1d8b696e47a0e2f3769c340a5d249ebaa
e0fd1817f6db4166b2b9e32c7a9c93dcf801f52946997ba0f0584ee0b118e3335a5efabf95
9e799736ec47b6df311c0f05ede6c2ae6a130d33722616b931f1982d9039f7609f77d734d
54b495016d43c5e22e7f9d4b7f9d3fbf031faf35f93de2178d6b7b1281db88be2c3708441
843af5ab489dabde7ddefd3407c4b895fa18bb803259e4c292536017682376f140070dec
722414b5c971b144be144ccbd55169ca58c8785393ab6023ca02c62e3184dacc3598ed9
027a9ef4debd3dbf04b953eabee5ee753046c695ff58206fabcc29e59d4917ceddc0f791d
d3790be6a55dad78c25fb35924c9e3ab50e50fd268ab9c20338a4098aacfb3053534ac97
37828be7a615b609196ec23cf880fa1ae2407ba15a4c4c305f612181320100e5b87649e4
eb9565c83e1d0898312461e38d63c8452e38abe8099c4cb17964a0d4dd3bbde0ec018d
37c2aaa9fe33e1f69a9d886a7c3fa0f03554965f572d90506bb3c07fc8d8af0d0f10ce1b6e
ef25f64e4c0a0d8ece2958b860a3c14e84993511caad9e5f5611f7516d82d89e5680cb8a
248b5c3a686d26164c98dc9dd4f8336390afda6503b79dce3e9e561b0f006bf32a7071e1
6fd7e7da6a72a884afce43f42a61c85926a17056f54084f6355fbe34d6d05eb6cedef0864
b8

The decrypted message is As a constructor in Formula One, Ferari has a record 16 Constructors' Championships. Their most recent Constructors' Championships was won in 2008. The Team also holds the record for the most Drivers' Championships with 15, won by nine different drivers: Alberto Ascari, Juan Manuel Fangio, Mike Hawthorn, Phil Hill, John Surtees, Niki Lauda, Jody Scheckter, Michael Sschumacher and Kimi Raikkonen. Raikkonen's title in 2007 is the most recent for the team. The 2020 Tuscan Grand Prix marked Ferrari's 1000th Grand Prix in Formula One.

(There is extra whitespace due to padding).