My code first checks if it wants to encrypt or decrypt the input file. It then uses the key from the input file and runs the encryption or decryption algorithm based on the input. For both it follows the logic from the lectures.

For encryption, it reads from the file 128 bits at a time and reads it into a bitvector. For each 128 bits we do the round key logic. So we have already generated the round keys using the given function, we iterate through all 15 of them. For each round we normally do subbytes, shiftrows, mixcolumns, and add round keys. For the first round we add the round key and skip the rest of the steps, and for the last round we skip the mix columns steps. After the 15 rounds we append the output to an output bit vector and read the next 128 bits. We then output this to the last argument given in the command line as a hex string.

For decryption the steps are similar. The main difference is that the order of operations is different. Also since the output is in a text format, we have to first read the file, and then input that file as a hex string into the bitvector. Because of this we index differently in code but same in principle. We read 128 bits at a time but we iterate based on the size of the bitvector. The ordering change is that we do inverse shift rows, inverse sub bytes, add round keys, and then inverse mix columns. Each of the inverse functions are similar in order but different in operation which is described in the comments in the code. We also iterate backwards across the round keys and the same logic for the first and last round are the same as encryption. We still increment this to an output bitvector. We then output this to the last argument given to the command line as a text file.

Encrypted :
2bd280a572d58f866b407a63e2ac60a4a58e4f16d71808c75b85a3188aa78de70453883720af22
5915d84feff6fc415edfd642d338f4d61f1d8b696e47a0e2f3769c340a5d249ebaae0fd1817f6db41
66b2b9e32c7a9c93dcf801f52946997ba0f0584ee0b118e3335a5efabf959e799736ec47b6df311c
0f05ede6c2ae6a130d33722616b931f1982d9039f7609f77d734d54b495016d43c5e22e7f9d4b7f
9d3fbf031faf35f93de2178d6b7b1281db88be2c3708441843af5ab489dabde7ddefd3407c4b895f
a18bb803259e4c292536017682376f140070dec722414b5c971b144be144ccbd55169ca58c878
5393ab6023ca02c62e3184dacc3598ed9027a9ef4debd3dbf04b953eabee5ee753046c695ff5820
6fabcc29e59d4917ceddc0f791dd3790be6a55dad78c25fb35924c9e3ab50e50fd268ab9c20338a
4098aacfb3053534ac9737828be7a615b609196ec23cf880fa1ae2407ba15a4c4c305f612181320
100e5b87649e4eb9565c83e1d0898312461e38d63c8452e38abe8099c4cb17964a0d4dd3bbde
0ec018d37c2aaa9fe33e1f69a9d886a7c3fa0f03554965f572d90506bb3c07fc8d8af0d0f10ce1b6e
ef25f64e4c0a0d8ece2958b860a3c14e84993511caad9e5f5611f7516d82d89e5680cb8a248b5c3
a686d26164c98dc9dd4f8336390afda6503b79dce3e9e561b0f006bf32a7071e16fd7e7da6a72a8
84afce43f42a61c85926a17056f54084f6355fbe34d6d05eb6cedef0864b8

Decrypted :
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 are some null bytes here but they will not show on google docs)

Workout Problems

Thursday, February 9, 2023 2:08 PM

Theory Problems

1. Determine the following in GF(11), please show your work:
   (a) $(9x^5 + 4x^4 + 8x^3 + 2x^2 + 3x + 4) + (6x^5 + 2x^4 + 9x^3 + 7x^2 + 5x + 7)$
   (b) $(8x^3 + 6x^2 + 8x + 1) \times (3x^3 + 9x^2 + 7x + 5)$
   (c) $\frac{3x^3-5x^2+10x-3}{3x+1}$
2. For the finite field $GF(2^3)$, calculate the following for the modulus polynomial $x^3 + x + 1$, please show your work:
   (a) $(x^2 + x + 1) \times (x^2 + x)$
   (b) $(x^2) - (x^2 + x + 1)$
   (c) $\frac{x^2+x+1}{x^2+1}$

1a) $9x^5+4x^4+8x^3+2x^2+3x+4$

$+\ 6x^5+2x^4+9x^3+7x^2+5x+7$

$15x^5+6x^4+17x^3+9x^2+8x+11$

$\boxed{4x^5+6x^4+6x^3+9x^2+8x}$

1b) $(8x^3+6x^2+8x+1)\cdot(3x^3+9x^2+7x+5)$

$24x^6+18x^5+24x^4+3x^3$

$72x^5+54x^4+72x^3+9x^2$

$56x^4+42x^3+56x^2+7x$

$+40x^3+30x^2+40x+5$

$24x^6+90x^5+134x^4+157x^3+95x^2+47x+5$

$\boxed{2x^6+2x^5+2x^4+3x^3+7x^2+3x+5}$

56
54
10
24
134

72
42
40
3
157

1c) $\frac{3x^3-5x^2+10x-3}{3x+1}$

$\frac{8}{4}=2$ $4\overline{)8}$ $\frac{2}{}$

$3x^3-5x^2+10x-3$

$3\cdot x \bmod 11 = 5 \bmod 11$

$x = 5\cdot mi(3) \bmod 11$

$3x^3 - 5x^2 + 10x - 3$

$= 3x^3 + 6x^2 + 10x + 8$

$3 \cdot x \equiv 5 \cdot mi(3) \pmod{11}$

$x \equiv 5 \cdot mi(3) \pmod{11}$

$$3x+1 \overline{)\,3x^3+6x^2+10x+8}$$

$x^2 + 9x + 4$ R 4

$3x^3 + x^2$

$5x^2 + 10x + 8$

$27x^2 + 9x$

$x + 8$

$12x + 4$

4

$\frac{5x^2}{3x} = 5 \cdot mi(3)$

$= 5 \cdot 4$

$= 20$

$= 9x$

$\frac{1}{3} = mi(3) = 4$

$gcd(11,3) =$

$gcd(3,2)$ $2 = 1x11 - 3x3$

$gcd(2,1)$ $1 = 1x3 - 1x2$

$= 1x3 - 1x11 + 3x3$

$= 4x3 - 1x11$

4

$$= x^2 + 9x + 4 + \frac{4}{3x+1}$$

2. For the finite field $GF(2^3)$, calculate the following for the modulus polynomial $x^3 + x + 1$, please show your work:

   (a) $(x^2 + x + 1) \times (x^2 + x)$

   (b) $(x^2) - (x^2 + x + 1)$

   (c) $\frac{x^2+x+1}{x^2+1}$

2a) $(x^2 + x + 1) \cdot (x^2 + x)$

$x^4 + x^3 + x^2 + x^3 + x^2 + x$

$x^4 + x \pmod{x^3 + x + 1} = x^2$

$$x^3 + x + 1 \overline{)\,x^4 + x}$$

x R x^2

$x^4 + x^2 + x$

$$\frac{x^4+x^2+x}{x^2}$$

2b) $(x^2)-x^2-x-1$

$x+1$

2c) $\frac{x^2+x+1}{x^2+1}$

$$x^2+1 \overline{)\,x^2+x+1}\quad R\ x$$

$$x^2+1$$

$$x$$

$$= 1+\frac{x}{x^2+1}$$