1) GF (11)

a) $(9x^5 + 4x^4 + 8x^3 + 12x^2 + 3x + 4)$

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

$= 4x^5 + 6x^4 + 6x^3 + 9x^2 + 8x$

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

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

$= 2x^6 + 2x^5 + 2x^4 + 3x^3 + 7x^2 + 3x + 5$

c) $\dfrac{3x^3 - 5x^2 + 10x - 3}{3x + 1} = x^2 + 9x + 4 + \dfrac{4}{3x+1}$

$x^2 - 2x + 4$

$3x+1 \;\big|\; 3x^3 - 5x^2 + 10x - 3$

$3x^3 + x$

$-6x^2 + 10x - 3$

$-6x^2 - 2x$

$12x - 3$

$12x + 4$

-7

2) $GF(2^3)$ Modulus : $x^3 + x + 1$

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

$= (x^4 + x^3 + x^3 + x^2 + x^2 + x) \% (x^3 + x + 1)$

$= (x^4 + x) \% (x^3 + x + 1)$

$= x^2$

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

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

Homework Number: 04
Name: Samitha Ranasinghe
ECN Login: sranasi
Due Date: 02/14/2023

Problem 1

Plaintext message:

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.

Key: scuderiaferraritheprancinghorse!

Encrypted message:

2bd280a572d58f866b407a63e2ac60a4a58e4f16d71808c75b85a3188aa78de70453883720af
225915d84feff6fc415edfd642d338f4d61f1d8b696e47a0e2f3769c340a5d249ebaae0fd1817f
6db4166b2b9e32c7a9c93dcf801f52946997ba0f0584ee0b118e3335a5efabf959e799736ec4
7b6df311c0f05ede6c2ae6a130d33722616b931f1982d9039f7609f77d734d54b495016d43c5
e22e7f9d4b7f9d3fbf031faf35f93de2178d6b7b1281db88be2c3708441843af5ab489dabde7d
defd3407c4b895fa18bb803259e4c292536017682376f140070dec722414b5c971b144be144c
cbd55169ca58c8785393ab6023ca02c62e3184dacc3598ed9027a9ef4debd3dbf04b953eabee
5ee753046c695ff58206fabcc29e59d4917ceddc0f791dd3790be6a55dad78c25fb35924c9e3a
b50e50fd268ab9c20338a4098aacfb3053534ac9737828be7a615b609196ec23cf880fa1ae24
07ba15a4c4c305f612181320100e5b87649e4eb9565c83e1d0898312461e38d63c8452e38ab
e8099c4cb17964a0d4dd3bbde0ec018d37c2aaa9fe33e1f69a9d886a7c3fa0f03554965f572d9
0506bb3c07fc8d8af0d0f10ce1b6eef25f64e4c0a0d8ece2958b860a3c14e84993511caad9e5f
5611f7516d82d89e5680cb8a248b5c3a686d26164c98dc9dd4f8336390afda6503b79dce3e9e
561b0f006bf32a7071e16fd7e7da6a72a884afce43f42a61c85926a17056f54084f6355fbe34d
6d05eb6cedef0864b8

Decrypted message:

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.

Brief Explanation:

Contains code for encrypting and decrypting a message using AES with a specified key.

The main function first runs the genTables function which produces the S-Boxes for encryption and decryption. For the encryption lookup table, a for loop finds the multiplicative inverse for each integer in from 0 to 255 in GF(2^8) and XOR that with several circular rotated versions of it and a constant. We do the same thing for the decryption lookup array, except that we first do the XORing and then we compute the multiplicative inverse. For the decryption lookup table, the same thing is done except the XORing is done first.

The encrypt function first uses functions provided in lecture notes to obtain the set of round keys. The get_round_keys function is called which first obtains the key from the file and then calls code from lecture to produce 15 round keys from 60 key words. A bitvector file object is created with the file containing the message to be encrypted and then blocks are grabbed at 128-bit sizes to be encrypted. The block is padded with null bits if a block is less than 128 (usually needed for the last block) and the first-round key is XORed with the block. The 4 steps in AES are then executed using different functions. The byte substitution is done by obtaining 8 bits at a time and then grabbing the element from the S-Box which the index is the integer equivalent of the 8 bits. The padded element is then substituted with the 8 bits. The row shifting is done by first producing a 4x4 matrix of the 128-bit block with a byte in each element. The shifting is done manually by swapping the elements and then converting the matrix back to a Bitvector string. The column mixing is then done by again converting into a matrix and then using a matrix multiplying function tweaked to multiply in GF(2^8) and then the resulting matrix is converted back to a Bitvector string. At last, the round key for the respective round is then XORed and the steps are repeated in the next round. 14 rounds are executed with the same steps except in step 14 where the column mixing is omitted

The decrypt function is similar to encrypt function except the round keys are reversed, the order of the steps is different where first the inverse row shifting, then inverse byte substitution, then round key XORing and then inverse column mixing is done. The inverse column mixing is omitted in the last round. The inverse row shifting is different in that the cycle direction is opposite to the row shifting in encryption. The inverse byte substitution is different in using a different S-Box. The inverse column mixing is different in the ratios that each element is multiplied in each column.