HW04: Advanced Encryption Standard

Homework Number: 04
Name: Jack Gardner
ECN Login: gardne97
Due Date: 2/14/23

Problem 1:

Summary: The code borrows parts of the lecture 8 code for the generation of the key schedule and the byte substitution table. The 256 bit key and plaintext are read from the file, and the key schedule is generated. In encryption, at the very beginning, the first 128 bit chunk of plaintext is xored with the first four words of the key schedule. Then each 128 bit section is substituted using the generated table, then the chunk is turned into a state array, the row shifting step is applied, the columns are mixed , the state array is decomposed, and the corresponding key words are xored with the 128 bit section. These steps are repeated another 13 times, with the exception that on the last time, the mix columns step is excluded. Then the bitvector is converted to a hex string and written to the output file.

In decryption, the overall process is similar, although the steps are slightly altered and performed in a different order. The ciphertext is read from the input file and once again the key schedule and inverse sub bytes table is generated. The initial adding to the key happens again, although this time the end of the key schedule is used. Firstly, the rows are shifted again, although this time to the right instead of the left. The inverse substitution table is used for the inverse substitution step that follows. Then, the key is adding, working backwards down the key schedule. Finally, the inverse mix columns step works up the columns instead of down the columns. This is once again skipped on the last iteration. These 4 steps are repeated another thirteen times and the output plaintext is written to the output file.

Recovered Text: 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.

Encrypted text:

2bd280a572d58f866b407a63e2ac60a4a58e4f16d71808c75b85a3188aa78de70453883720af225915d84f
eff6fc415edfd642d338f4d61f1d8b696e47a0e2f3769c340a5d249ebaae0fd1817f6db4166b2b9e32c7a9c9
3dcf801f52946997ba0f0584ee0b118e3335a5efabf959e799736ec47b6df311c0f05ede6c2ae6a130d3372
2616b931f1982d9039f7609f77d734d54b495016d43c5e22e7f9d4b7f9d3fbf031faf35f93de2178d6b7b12
81db88be2c3708441843af5ab489dabde7ddefd3407c4b895fa18bb803259e4c292536017682376f14007
0dec722414b5c971b144be144ccbd55169ca58c8785393ab6023ca02c62e3184dacc3598ed9027a9ef4de
bd3dbf04b953eabee5ee753046c695ff58206fabcc29e59d4917ceddc0f791dd3790be6a55dad78c25fb359
24c9e3ab50e50fd268ab9c20338a4098aacfb3053534ac9737828be7a615b609196ec23cf880fa1ae2407b
a15a4c4c305f612181320100e5b87649e4eb9565c83e1d0898312461e38d63c8452e38abe8099c4cb1796
4a0d4dd3bbde0ec018d37c2aaa9fe33e1f69a9d886a7c3fa0f03554965f572d90506bb3c07fc8d8af0d0f10c
e1b6eef25f64e4c0a0d8ece2958b860a3c14e84993511caad9e5f5611f7516d82d89e5680cb8a248b5c3a6

86d26164c98dc9dd4f8336390afda6503b79dce3e9e561b0f006bf32a7071e16fd7e7da6a72a884afce43f4
2a61c85926a17056f54084f6355fbe34d6d05eb6cedef0864b8

HW04

1a. $\boxed{4x^5 + 6x^4 + 6x^3 + 9x^2 + 8x}$

1b.

	$8x^3$	$6x^2$	$8x$	1
$3x^3$	$2x^6$	$7x^5$	$2x^4$	$3x^3$
$9x^2$	$6x^5$	$16x^4$	$6x^3$	$9x^2$
$7x$	x^4	$9x^3$	x^2	$7x$
5	$7x^3$	$8x^2$	$7x$	5

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

1c.

	x^2	$9x$	4	R
$3x$	$3x^3$	$5x^2$	x	4
1	x^2	$9x$	4	

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

Box method for long division

2a. $(x^2+x+1)(x^2+x) = x^4+x^3+x^2+x^3+x^2+x = x^4+x$

$$x^3+x+1 \;\overline{)\; x^4 \quad\quad}\;\; x$$
$$-\,(x^4+x^2+x)$$
$$x^2+x+1$$

$x^4 = x^2+x$

$x^4+x = x^2$

$\boxed{x^2}$

b. $x^2-(x^2+x+1) = \boxed{x+1}$

c.

$$x^2+1 \;\overline{)\; x^2+x+1 \quad\quad}\;\; 1$$
$$-\,(x^2+1)$$
$$x$$

$1+\frac{x}{x^2+1} = 1 + x \cdot M.I.(x)$

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