CIS 3362 Exam #2
October 28, 2015

Last Name: _____ , First Name: _____

1) (16 pts) If the input to the S-boxes is 69E4 CF08 3B52, in hex, what is the output?

_____

2) (8 pts) Imagine a DES-like cipher with a block size of 16 with the following IP matrix:

$$\begin{pmatrix} 6 & 13 & 7 & 5 \\ 11 & 15 & 9 & 16 \\ 2 & 14 & 3 & 12 \\ 8 & 1 & 4 & 10 \end{pmatrix}$$

What is the corresponding IP^{-1} matrix?

3) (18 pts) If the state matrix is the following right before the Mix Columns step of AES, what is the entry in row 3, column 2, right after the Mix Columns step? ***(Note: Please be very, very, very careful that you work out the correct entry. If you find the entry of row 2, column 3, you will earn a maximum of 5 points out of 15.)***

$$\begin{pmatrix} 3A & 95 & A2 & 12 \\ 2C & 7E & 36 & 4F \\ 97 & F9 & 20 & 62 \\ B2 & C8 & A7 & D3 \end{pmatrix}$$

Note that the fixed matrix multiplier for the Mix Columns step in AES is $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$.

4) (13 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[36] = 3A 74 E5 8D (in hex)
w[39] = 8F 17 60 C2 (in hex)

Calculate w[40], showing each of the following intermediate results: RotWord(temp), SubWord(RotWord(temp)), Rcon[i/4], and the result of the XOR with Rcon[i/4].

RotWord	SubWord	Rcon[i/4]	XOR	FinalResult

5) (8 pts) Calculate 78^{216} mod 117.

6) (9 pts) Given that a is a primitive root (generator) of p = 29, list the other primitive roots of 23, in terms of a. (Hint: your answers will all be of the form a^x mod p, where x is an integer in between 1 and 22, inclusive.)

____ , ____ , ____ , ____ , ____ , ____ , ____ , ____ , ____ , ____ , ____ , ____ , ____ , ____ , ____
(Note: all slots may not be used.)

7) (12 pts) The Miller-Rabin Primality Test is shown below.

```
Input: n > 2, an odd integer to be tested for primality;
       k, a parameter that determines the accuracy of the test
Output: composite if n is composite, otherwise probably prime
write n − 1 as 2^s·d with d odd by factoring powers of 2 from n − 1
LOOP: repeat k times:
   pick a randomly in the range [2, n − 1]
   x ← a^d mod n
   if x = 1 or x = n − 1 then do next LOOP
   for r = 1 .. s − 1
      x ← x^2 mod n
      if x = 1 then return composite
      if x = n − 1 then do next LOOP
   return composite
return probably prime
```

Consider running the test for n = 49, k = 1 and a = 2. Show each value of x calculated while the algorithm executes and the return value of the algorithm.

8) (15 pts) Consider an RSA system with n = 91 and e = 25. Calculate d.

9) (1 pt) Which company makes Mars candy bars? _____

Scratch Page - Please clearly mark any work on this page you would like grade.