CIS 3362 Test #2: Modern Symmetric Encryption Schemes (DES, AES) and Public Key Encryption (RSA, Diffie-Hellman)

Date: 10/24/2014

Name: ______________________________________

1) (6 pts) The input into S-box 6 in DES is 100110. What is the output, expressed in decimal (a single value in between 0 and 15, inclusive)?

____

2) (8 pts) In the middle of a round of DES, the input to the P array is 3D91AB75, in hexadecimal. What is the corresponding output from the P array, expressed in hexadecimal?

____

3) (6 pts) What is the prime factorization of 18271008?

____

4) (16 pts) Let the input to the MixCols step of AES be $\begin{bmatrix} 25 & 90 & 49 & EE \\ 9A & 67 & 7C & F4 \\ B5 & B3 & D5 & 62 \\ DF & E7 & 86 & 96 \end{bmatrix}$. Remember that the multiplication matrix used for encryption in AES is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$. Determine the entry in row 3 column 2 of the result. **(Note: Be very, very careful about the details here. If you get the wrong order of multiplication OR the wrong entry in the matrix, a *majority* of the points for this question will be automatically deducted. One of the things I am testing here is if you paid attention to these details!!!)**

5) (12 pts) Let the round 9 key for AES be the following in hexadecimal:

2984 E98B A275 BBCD F011 184E 73BC F329

Determine the first 4 bytes of the round 10 key. Please give your answer in hexadecimal.

____

6) (6 pts) What is φ(32632)?

____

7) (8 pts) What is the remainder when 761^{14282} is divided by 899?

____

8) (16 pts) Consider an RSA system where n = 247 and e = 175. What are p, q, φ(n) and d?

9) (12 pts) One of the primitive roots/generators of 19 is 2. Determine the other generators of 19 using this information. **(Note: Please do NOT do a brute force search for these generators. You will NOT get a *majority* of the credit for this question if you do this but get the correct answers. There's a quick way to determine these other generators and I am testing to see if you can figure out that quick way.)**

10) (8 pts) Use the Fermat Factoring method to factor 13231. **To get full credit, show each of your steps. If you just provide the factorization with no work, you will get 1 point total for this question.**

11) (2 pts) Rapper Pitbull shares his stage name with which breed of dog? ____________________

Scratch Page – Please clearly mark any work on this page you would like graded.