CIS 3362 Final Exam

Date: 12/3/2014

Name: _____

1) (15 pts) Consider an RSA system where n = 323 and e = 137. What are p, q, φ(n) and d?

2) (10 pts) Let H(x) be an ideal hash function with a 16 bit output. If we randomly generate values $x_1, x_2, \ldots, x_{100}$, what is the probability that for some pair i and j, with $1 \leq i < j \leq 100$, we have $H(x_i) = H(x_j)$. Please express your answer in powers, factorials, product notation, etc.

3) (10 pts) Encrypt the plaintext "CRYPTO" using the Hill cipher with the encryption key $\begin{pmatrix} 3 & 4 & 7 \\ 1 & 2 & 12 \\ 11 & 9 & 5 \end{pmatrix}$. Express your result as six letters. Put a box around your final answer.

4) (10 pts) Two stories were told in class relating the history of the Queen Mary of Scots cipher and the Cracking of the Enigma. Choose one of these two stories and summarize it. Note: don't worry if you have forgotten the names of specific individuals; just describe the roles of each individual as it pertains to the story.

5) (5 pts) The input into S-box 8 in DES is 011011. What is the output, expressed in decimal (a single value in between 0 and 15, inclusive)?

_____

6) (10 pts) Let a DES key with parity bits expressed in HEX be BF 2C 57 92 DA 76 38 E5. Determine the first ten bits of the round 3 key.

_____

7) (15 pts) Let the input to the MixCols step of AES be $\begin{bmatrix} 95 & 90 & 49 & EE \\ C7 & 67 & 7C & F4 \\ 69 & B3 & D5 & 62 \\ DF & E7 & 86 & 96 \end{bmatrix}$. 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 4 column 1 of the result, expressing it in HEX. Put a box around your final answer **(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!!!)**

8) (15 pts) Consider the elliptic curve $y^2 = (x^3 + 10x + 7) \bmod 29$. Let the point P be (6, 14) and the point Q be (15, 20), on this curve. Determine the points 2P and P + Q.

9) (10 pts) Consider the DSA with $p = 29$, $q = 7$, $g = 3$ and $x = 4$. Let $k = 5$ and $H(M)$ be 2 for a particular message. Provide the corresponding signature (r, s). Since there are relatively few possible values for r and s, none of the points will be awarded for the correct answer. All the points will be awarded for showing the process of the computation.

10) (2 pts) Jeff Bezos named his website amazon.com after the largest river in the world, in terms of amount of water flow. After what river did he name his website?

_____

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