CIS 3362 Final Exam

Date: 12/9/2015

Name: _____

1) (7 pts) Consider an adjusted shift cipher on an alphabet with 36 characters, the letters 'A' through 'Z', followed by the digits '0' through '9', where the numerical value of the digits range from 26 to 35, inclusive. (Thus, the digits follow the letters in the ordering of the 36 symbols and the numeric value of 'A' is set to 0.) Use this cipher to encrypt "CIS3362" with a shift of 12.

_____

2) (12 pts) The Playfair cipher with the secret keyword "DECEMBER" produced the ciphertext "EASJGWGFPIBPJPTNADMCXCXC". What is the corresponding plaintext? Remove padding characters as necessary.

_____

3) (14 pts) The encryption key for a Hill cipher is $\begin{pmatrix} 6 & 5 \\ 7 & 11 \end{pmatrix}$. A message created with this key is "MEQJ". What is the corresponding plaintext?

4) (12 pts) Let the input to the E matrix in the DES round function be 8FE67B92, in hexadecimal. Express the output in hexadecimal as well.

_____

5) (8 pts) One year on Venus is 225 days. What is the probability that of a random sample of 10 Venetians, all of them have different birthdays? Please write down the answer in product notation and then use your calculator to get an approximation for the value.

Product Notation: _____

Approximate Value of Desired Probability: _____

6) (15 pts) If the state matrix is the following right before the Mix Columns step of AES, what is the entry in row 4, column 1, 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 1, column 4, you will earn a maximum of 5 points out of 15.)***

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

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

7) (12 pts) Consider an RSA system with p = 13, q = 23 and e = 95, what is d?

_____

8) (15 pts) Consider the Elliptic Curve $E_{37}(14, 3)$. Let P be the point (10, 12) and Q be the point (22, 9). Calculate both P + Q and 2P.

P + Q = _____ 2P = _____

9) (18 pts) You have received a digital signature signed with the Digital Signature Algorithm. The value of r you have received is 15 and the value of s you have received is 5. The public components of the system are: p = 83, q = 41 and g = 2. The public key for the user from which you've received the message is y = 5. The hash value of the message you've received is 19. Show the following steps of verifying the signature:

a) Calculate w.
b) Calculate u_1.
c) Calculate u_2.
d) Calculate v, showing the values of g, u_1, y and u_2 being plugged into the appropriate equation.
e) Show the necessary comparison to be made and determine if the signature is valid or not.

Show work here:

w = _____ u_1 = _____ u_2 = _____ v = _____

10) (10 pts) Alice and Bob want to exchange 1024 bits for a set of secret keys via Quantum Cryptography. Alice plans on sending bits to Bob, randomly picking the orientation of her reader, with Bob not knowing, so that they can detect any intruder. They would like a probability of 2^{-100} that an intruder could successfully read all the bits sent without being detected. Recall that after sending the bits, Alice and Bob "sample" some of the bits and check which readers they used, verifying that the exchange was secure if all of the bits for which they used the same reader in their sample were correctly interpreted by Bob. Roughly how many bits must Alice send originally, to give Alice and Bob at least a 50% chance of having exchanged 1024 bits while making the chance that an intruder intercepted the bits roughly 2^{-100}? (Note: A range of answers will be accepted for this question, but an answer that is artificially high will lose credit. Full credit will only be given for work that justifies the answer.)

_____

11) (2 pts) The next installment of Star Wars, The Force Awakens, comes out in theaters on December 18th. Harrison Ford, who plays Han Solo in the movie, shares his last name with which popular American car company?

_____

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