2016 Fall CIS 3362 Final Exam 12/7/2016

Name: _____

1) (12 pts) You have intercepted a ciphertext encrypted using the Affine Cipher. You know that the letters R and E are among the three most frequenct letters in the corresponding plaintext, with there being more Rs than Es. Utilizing the frequencies of the ciphertext shown below, determine the possible mappings for R and E and then determine the corresponding plaintext.

ENUHUCWQNHCWLKMWRAWLMHOAZFLNUQOHZUH

2) (5 pts) Determine the index of coincidence of the following set of letters:

15 As, 35 Bs, 10 Cs, 25 Ds and 15 Es.

Please express your answer in a fraction in lowest terms.

_____

3) (8 pts) Use the ADFGVX cipher to encrypt the plaintext "CIS3362FINALEXAMON127". Use the keyword "CRYPTO" and the following ADFGVX square:

I	C	N	1 (one)	T	P
4	R	X	K	E	Z
8	Y	H	B	0(zero)	J
G	Q	7	2	V	6
9	L	A	F	S	D
5	W	O	U	M	3

4) (6 pts) Use the Hill cipher to encrypt the plaintext "RESTED" using the key $\begin{bmatrix} 13 & 11 & 3 \\ 4 & 22 & 17 \\ 19 & 16 & 5 \end{bmatrix}$.

_____

5) (6 pts) Let the plaintext input block to DES be P = 8DE439FA012B75C6. Calculate the first 24 bits (express your result as 6 hex characters) of IP(P).

_____

6) (10 pts) Consider performing the Mix Columns operation in AES. If the state matrix is equal to $\begin{bmatrix} 03 & DB & F6 & 5E \\ 81 & 9E & 6C & BB \\ 94 & 76 & EB & A9 \\ B3 & 26 & 95 & CD \end{bmatrix}$, what is the entry in row 4, column 3? Please express your answer as 2 hex characters. (Note: The fixed multiplication matrix for AES is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.

_____

7) (12 pts) Recall that a primitive root of a prime, p, is an integer a ($1 \leq a \leq p-1$) such that *the smallest* positive integer e such that $a^e \equiv 1 \pmod{p}$ is p-1. In particular, this result also means that the values $a^1, a^2, a^3, ..., a^{p-1} \bmod p$ are all distinct and form the set {1, 2, 3, ..., p-1}. Given that 13 is a primitive root mod 19, determine all of the other primitive roots mod 19. (Note: The intention here is NOT for you to try all of the other values by exponentiating them. There is a much faster way to do this and you're being graded on discovering that way. Since you have a calculator at your disposal, please do simplify your answers to be in between 1 and 18, inclusive. Also, more blanks than necessary are provided below so as to not give away the number of answers.)

_____ , _____ , _____ , _____ , _____ , _____ , _____ , _____ , _____ , _____ , _____ , _____

8) (10 pts) You have received a ciphertext in the RSA cryptosystem. The public keys are n = 187 and e = 87 and the ciphertext is 7. Determine the decryption exponent, d, and the corresponding plaintext.

Plaintext = _____

9) (8 pts) In Elliptic Curve Arithmetic what is the sum of the points (22, 17) and (8, 28) on the curve $E_{37}(15, 4)$?

(_____ , _____)

10) (5 pts) For the purposes of this question, assume that the probability that a person has a birthday in any particular month is precisely $\frac{1}{12}$. What is the probability that 6 randomly chosen people all have birthdays in different months?

_____

11) (8 pts) Consider verifying a signature via the El Gamal Digital Signature Scheme where the public elements are $q = 19$, $\alpha = 13$ and $Y_A = 10$. You have received the signature $S_1 = 14$, $S_2 = 16$ and have computed the hash value of the message to be $m = 16$. Show the process of verifying the signature.

12) (8 pts) Consider a DSA system with p = 159 and q = 79. Calculate a digital signature, (r, s), for this system where you choose k = 48, the public generator g = 2, the private key x = 3, and H(M) = 35. Show all of your work.

r = _____ , s = _____

13) (2 pts) On what day of the week does the movie Friday take place? _____

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