Fall 2017 CIS 3362 Final Exam

Last Name: _____ First Name: _____

1) (10 pts) Decrypt the following ciphertext that was encrypted using the shift cipher:

```
mubsecujejxuvydqbunqc
```

---

2) (10 pts) Consider an affine cipher on an alphabet of size n = 57 with the encryption function

$$f(x) = (34x + 12) \bmod 57$$

What is the corresponding decryption function, $f^{-1}(x) = cx + d$, where $0 < c, d < 57$?

3) (10 pts) Consider the two following sets of letter frequencies:

Frequency	A	B	C	D	E	F
Set 1	6	19	23	10	15	27
Set 2	26	8	16	26	4	20

(a) (4 pts) Find the mutual index of coincidence between the two sets.

(b) (6 pts) Let Set 1 represent the frequency of the language of the plaintext of a given language and Set 2 represent the frequency of one bin of letters (all shifted with the same shift) of ciphertext encrypted via Vigenere cipher. By eyeballing Set 2, determine the shift (an integer in between 0 and 5, inclusive) necessary to encrypt this bin of letters. To support your answer, take the mutual index of coincidence of Set 1 and the set created by shifting Set 2 "back" by the appropriate shift and show that this MIC is well above the value of 1/6, which would be roughly what would be expected of an incorrect shift.

4) (17 pts) The following function correctly performs encryption for the Hill Cipher. Answer the questions that follow the code about the code:

```
char* encrypt(char* plain, int key[][SIZE]) {
    int n = strlen(plain), i, j;
    char* cipher = malloc((n+1)*sizeof(char));
    cipher[n] = '\0';

    for (i=0; i<n; i++) {
        int ch = 0;
        for (j=0; j<SIZE; j++)
            ch = (ch + key[i%SIZE][j]*(plain[SIZE*(i/SIZE)+j]-'a'))%26;
        cipher[i] = (char)(ch+'a');
    }

    return cipher;
}
```

(a) (2 pts) What does SIZE likely represent?

(b) (3 pts) In order for this code to work, what pre-condition must be true about the length of the string represented by plain?

(c) (2 pts) In order for this code to work, what pre-condition must be true about each character in the string represented by plain?

(d) (4 pts) Explain why the indexes to the matrix key (in the one line the matrix is accessed) are i%SIZE and j, respectively.

(e) (4 pts) Explain why the index to the plain matrix (in the one line the matrix is accessed) is SIZE*(i/SIZE)+j.

(f) (2 pts) Explain the role of the - 'a'

5) (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 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 4, you will earn a maximum of 5 points out of 15.)***

$$\begin{pmatrix} 7A & 93 & A2 & 12 \\ 23 & FE & 36 & 4F \\ 97 & 58 & 20 & 62 \\ B2 & B7 & A7 & D3 \end{pmatrix}$$

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

6) (10 pts) Here is the description of the Miller-Rabin primality test from Wikipedia:

```
write n − 1 as 2^r·d with d odd by factoring powers of 2 from n − 1
WitnessLoop: repeat k times:
   pick a random integer a in the range [2, n − 2]
   x ← a^d mod n
   if x = 1 or x = n − 1 then
      continue WitnessLoop
   repeat r − 1 times:
      x ← x^2 mod n
      if x = 1 then
         return composite
      if x = n − 1 then
         continue WitnessLoop
   return composite
return probably prime
```

Trace through the execution of the algorithm for k = 1, n = 81, a = 6. Fill in the chart below showing each relevant value. Please use your calculator for making the appropriate calculations. Only the values filled in will be graded. Note that there may be more than the necessary number of rows supplied in the chart. ONLY FILL in the ones based on what the algorithm calculates. Credit will be taken away if too many rows of the chart (or too few) are filled in.

Value of r = _____ Value of d = _____

First value of x	
Second value of x	
Third value of x	
Fourth value of x	
Fifth value of x	
Sixth value of x	

Return value: _____

7) (12 pts) Let the input to the Expansion matrix E in DES be 49E48C31 in hex. Express the output of the E matrix in hex.

_____

8) (6 pts) Consider a Diffie-Hellman key exchange with p = 83 and g = 13. Let Alice's secret key be 12 and Bob's secret key be 15. What is the shared secret key that they exchange, in between 0 and 82, inclusive? (Please write what calculations you made on your calculator.)

_____

9) (8 pts) Consider the Elliptic Curve $E_{37}(5,9)$. Let the point P on this curve be (19, 9) and the point Q be (5, 23). What is P + Q?

_____

10) (2 pts) By what abbreviation do we typically refer to Secure Hash Algorithms? _____

Scratch Page - Please carefully mark anything you would like graded on this page.