**CS 4732/57322 Homework #2**

***Due electronically by midnight 6/30/2025***.

For submission, if done on paper please scan and submit as a pdf. If done in word, please submit the .docx or .doc format.

**IMPORTANT**: Clearly indicate outside resources utilized and sign below. Failure to cite use of outside resources will be reported for appropriate disciplinary actions. Note that discussions with other students are encouraged; copying – with or without modifications – is unacceptable and will also be reported.

I discussed one or more problems with the following people:

I hereby certify that any outside resources utilized, other than the textbook and class materials, are clearly cited. All other material I provide for this homework submission is my own original work.

Jamie Harris

*Printed name*

1. (6 points) The one-time pad is unbreakable, yet it isn’t used much at all. Name at least two problems with it.

One problem with one-time pad encryption is that every time you want to encrypt a new message, you need to generate a new cipher key. This compounds with another problem, the fact that the key for any given message must be at least as long as the message itself. Therefore, you can find yourself having to generate many large keys in rapid succession, which takes a lot of computing power and logistical overhead.

2. (8 points) Aliens have come down to earth and zapped all computers. Due to this, the US has decided to go back to rotor machines for their enciphering as they plan our counterattack. You have been tasked with administering this change. Name at least two things you would recommend to increase the security of our machines compared to the enigma machine.

I would recommend removing or modifying the mirror rotor so that a letter could potentially encode itself. This would make it harder to decrypt, because interceptors would have no way to know if a letter is encoding another letter or if it happens to be plaintext. I would also consider allowing the plugs to plug into neighboring letters, again to increase the amount of combinations and to potentially confuse cryptanalysts who would not expect it.

3. (7 points) What is the difference between modular arithmetic and ordinary arithmetic?

While ordinary arithmetic has an infinite amount of numbers to choose from, both as integers and as real numbers between any two integers, modular arithmetic is finite. When you reach the modulus base, the numbers cycle back over to 0 (eg, (6 + 1) (mod 7) = 0). Additionally, modular arithmetic only uses integers.

4. (9 points) Find an integer x that satisfies the equations below:

a)

4 = 1 (mod 3)

5(2)=10=1 (mod 3)

b)

6 = 1 (mod 5)

7(3) = 21 = 1 (mod 5)

c)

8 = 1 (mod 7)

9(4) = 36 = 1 (mod 7)

5. (10 points) Using Euclid’s algorithm to find the GCD, calculate GCD(816,1071). Show each step of the algorithm.

1071 = 816(1) + 255

816 = 255(3) + 51

255 = 51(5) + 0

GCD(816,1071)=51

6. (6 points) Find the multiplicative inverse of each nonzero element over the integers modulo 7.

2\*4=8=1 (mod 7) ->

3\*5=15=1 (mod 7) ->

1\*1=1 (mod 7) ->

6\*6=36=1 (mod 7) ->

7. (7 points) What is the value of the totient function of n=21. Give me the full list of numbers relatively prime to 21 that you used to calculate this value.

1

2

4

5

8

10

11

13

16

17

19

20

φ(21) = 12

8. (8 points) The totient function of n is even for n > 2. This is true for all n > 2. Give a concise argument for why this is so.

φ(n) is multiplicative, meaning φ(ab) = φ(a)φ(b). φ(p), where p is an odd prime > 2, is always equal to p-1, which means it will always be an even number. φ(2)=1. Therefore, when you break any n into its prime factors, you will get either φ(p1)φ(p2)...., with p>2, which will always be even, or φ(2)φ(p1)φ(p2)..., which will be 1 times an even number.