CS 4732/57322 Homework #2

Due electronically by midnight 6/29/2020. **No homework will be accepted after that time.**

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.

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.

The One-time pad uses a random key throughout the message so the key need not be repeated. A key must be discarded after using for encryption and decrypting a message.

1) Large Random Keys – It is difficult to make a lot of random keys. If there are small messages it is not difficult to make keys. But a heavily used system may need millions of characters to prepare keys. Supplying this type of keys is a very significant task.
2) Daunting – Key distribution and protection is more difficult. For each and every message to be sent a key of message length must be needed by sender and receiver. It is difficult to secure the keys whiles distributing them to the receiver.

2. (8 points) Aliens have came 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.

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

Modular	Ordinary
It will operate on a finite set of integers	It will operate on infinite set of all integers
In this ab=0 is possible, no need to become a=0 or b=0	In this ab=0 is only when a=0 or b=0
It depends on the polynomial	It will not depend on the polynomial
Simultaneous equations may have a number of solutions	It will have only one solution or have no solution
Every non zero number has an inverse	No integer has an inverse
Modulus and base or used	Modulus and base are not used

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

a) $5x \equiv 4 \ (mod\ 3)$

5 = 6-1

(6-1)x=4mod3

6x-x=3+1mod3

-x=1mod3

X=-1mod3

X=3m-1 where m is any integer

Setting m=0,1,2 we get three solutions

X=-1,2,5

b) $7x \equiv 6\ (mod\ 5)$

7x-6=7*1-6=1

7x-6=7*2-6=8

7x-6=7*3-6=15

7x=6mod5

7x3=6(mod5)

21=6(mod5)

Therefore, the equation satisfies for x=3

c) $9x \equiv 8\ (mod\ 7)$

9x-8=9*1-8=1

9x-8=9*2-8=10

9x-8=9*3-8=19

9x-8=9*4-8=28 which is divisable by 7

Hence the equation satisfies for x=4

36===8(mod7)

Therefore, the equation satisfies for x=4

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

1071 ÷ 816 = 1 R 255 *(1071 = 1 × 816 + 255)*

816 ÷ 255 = 3 R 51 *(816 = 3 × 255 + 51)*

255 ÷ 51 = 5 R 0 *(255 = 5 × 51 + 0)*

When remainder R = 0, the GCF is the divisor, b, in the last equation. GCF = 51

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

Since $6 \equiv -1 \pmod 7$, the class $[6]_7$ is its own inverse. Furthermore, $2 \cdot 4 = 8 \equiv 1 \pmod 7$, and $3 \cdot 5 = 15 \equiv 1 \pmod 7$, so $[2]_7$ and $[4]_7$ are inverses of each other, and $[3]_7$ and $[5]_7$ are inverses of each other.

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.

Prime factorization is : 3,7

Totient function is equal to 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.

You can do it via the formula as you do, but you can also simply use the definition that $\varphi(n)\varphi(n)$ is the number of numbers kk, with $1 \le k \le n1 \le k \le n$, such that $\gcd(n,k)=1\gcd(n,k)=1$.
Clearly, if $\gcd(k,n)=1\gcd(k,n)=1$, then $\gcd(n-k,n)=1\gcd(n-k,n)=1$ as well, so (for $n>2n>2$) all the numbers relatively prime to nn can be matched up into pairs $\{k,n-k\}\{k,n-k\}$. So $\varphi(n)\varphi(n)$ is even.