CS4732/5732 **Cryptography** **Summer 2020**

Project #1 [50 points]

Due date is Thursday, July 4th

This is the math option for our project1. It involves theoretical concepts in classical ciphers and modular arithmetic.

1) [10 points] How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.
   Playfair uses a 5x5 matrix which is constructed by using a keyword. The matrix can be filled with the letters of the keyword, duplicated are not allowed.
   The letters of the keyword are filled in the matrix from the left to the right and from top to bottom. The reaming matric can be filled with the remaining alphabets in the alphabetic order.
   All the letters are treated separately except the letters I and J. Both I and J treated as a single letter.

   There are 25 characters in the matric. Consider that no key can generate identical result. The number of keys generated in Playfair matrix is 25!. This can be represented in the power of 2 so **2^84**

2) [15 points] Prove that:

a) a = b (mod n) implies b = a (mod n)

if n is a positive integer and a is an integer than a mod n is defined as the reminder when a is divided by n. here n is the modulus so the equation is a=qn+r were 0<=r<n; q=floor(a/n)

if (a mod n) = b mod n this means a === b(mod n)^2 then two integers a and b are said to be congruent modulo n.

To demonstrate a===n(mod n) implies b===a(mod n) let us consider if n|(a-b) then (a-b)=kn for some integer k. from this we can say that a=b+kn

Hence a(modn)=(remainder when n dived b+kn)=(reminder when k divides b) =b(modn)

Here we proved that n|(a-b) in the same way it is proved that n|(-1)(b-a)

Let us consider if n|(-1)(b-a) then (b-a)=kn for some integer k from this we can say that b=a+kn

Then b(mod n) =(remainder when n divides a+kn)=(remainder when k divides a) = a(mod n)

Hence it is proved that a===b(mod n) implies b ===a(mod n)

b) [(a mod n) – (b mod n)] mod n = (a – b) mod n

let us consider a mod n = c and b mod n = d

we can write a = c+kn and b = d + ln for some integers k and I. then

a-b(mod n) = (c+kn-d-ln)mod n

=(c-d+(k-l)n)mod n

(c-d)mod n

[(a mod n)-(b mod n)] mod n

Hence [(a mod n)-(b mod n)] mod n = a-b(mod n)

c) [(a mod n) × (b mod n)] mod n = (a × b) mod n

Let us consider a mod n =c and b mod n = d

We can write a=c+kn and b=d+ln for some integer k and i. then

A*b(mod n) = (cd + dkn+cln+knln)mod n

=(cd +(dk+cl+knl)n)mod n

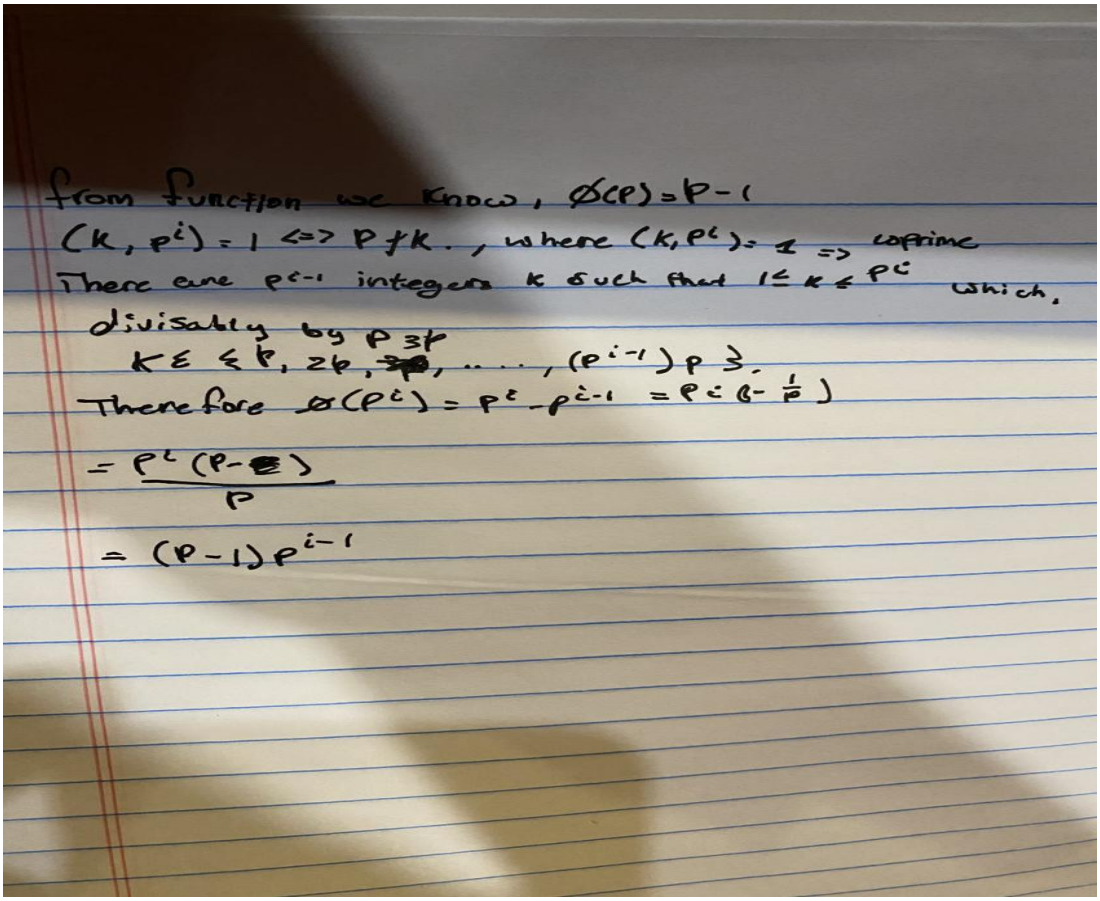
=(cd)mod n

= [(a mod n)*(b mod n)]mod n

Hence, [(a mod n) × (b mod n)] mod n = (a × b) mod n

3) [5 points] Assume a rotor could not map a connection on one side directly to the other (that is, A could not map to A in its initial location). How many unique rotors could be created?

4) [10 points] Prove that if p is prime, then the totient of $p^i = p^i - p^{i-1}$. Hint: What numbers have a factor in common with p^i?



5) [10 points] Prove or demonstrate that gcd(n, n+1) = 1 for any two consecutive numbers n and n+1.

Assume two positive consecutive numbers and both numbers cannot be divisible by 2. This condition is only positive number (1,2) and there gcd is equal to one.

Let n is a positive integer

Assume x is the grated common divisor of n and n+1

Then x should be dividing n and n+1 and find difference of both the integers

The common factor of two consecutive numbers is one. Therefor one is the GCD of n, n+1.

Therefore, gcd(n,n+1)=1

Example)

Consider an example n=8 n+1=9 then

8)9(1

8

1

If the consecutive numbers 8 and 9 remainder is 1 so the gcd is 1

OR

Factors of 8 = 1,2,4,8

Factors of 9 = 1,3,9

Common factor if (8,9) =1

So gcd of the two consecutive numbers is 1. For any sequence of consecutive numbers, the gcd is 1.

Submission:

Submit your solutions, either as a text document, pdf or scanned pdf. Do not submit a picture album of your text.