Cryptography Assignment - 3
Pramod Aravind Byakod

1: Solve 122 x = 3 mod 343. Show step-by-step calculations.

343 = 2*122 + 99
122 = 1*99 + 23
99 = 4*23 + 7
23 = 3*7 + 2
7 = 3*2 + 1

Therefore GCD(343,122) = 1

1 = 7 - 3*2
1 = 7 – 3*(23 - 3*7)
1 = 10*7 – 3*23
1 = 10*(99 – 4*23) – 3*23
1 = 10*99 – 43*23
1 = 10*99 – 43(122 – 1*99)
1 = 10*99 – 43*122 + 43*99
1 = 53*99 – 43*122
1 = 53*(343 – 2*122) – 43*122
1 = 53*343 – 149*122

So $x \equiv -149*3 \bmod 343$
$\equiv -447 \bmod 343$
$\equiv 239 \bmod 343$

Hence x = 239

2: Is your ID number invertible modulo m = 2^{64}?
Let a be the least integer that is no less than your ID number and is invertible mod m. Use Sage xgcd to find the inverse of a modulo m. In a C++ program, assume that there is a variable x with type "unsigned long int" (64bits), and the product of a and x is 2018, what is x?
My ID is 113436879.
Let's consider a = 113436879
Using sage xcgd(113436879,2^64), we have the below results

```
SageMath version 8.1, Release Date: 2017-12-07
Type "notebook()" for the browser-based notebook interface.
Type "help()" for help.

sage: xgcd(113436879,2^64)
(1, 3429800212755979823, -21091301)
sage:
```

Therefore, from the above result, GCD(113436879,2^64)=1, x=3429800212755979823 and y=-21091301

Since GCD(113436879,2^64)=1, **113436879 is invertible modulo 2^64.**

Inverse of 113436879 mod 2^64 is 3429800212755979823

```
sage: 3429800212755979823*113436879 % 2^64
1
sage:
```

Given 113436879(x) = 2018 mod 2^64, we got to solve for x.
We have the old value of x, that is 3429800212755979823. Multiply this with 2018, we will get the new value of x.
x= 3429800212755979823*2018 = **6921336829341567282814**

```
sage: 3429800212755979823 * 2018
6921336829341567282814
sage: (6921336829341567282814 * 113436879) % 2^64
2018
sage:
```

3: Determine the unit group and the zero divisors of the ring Z/16Z.

a	b	GCD(a,b)
1	16	1
2	16	2
3	16	1
4	16	4
5	16	1
6	16	2
7	16	1
8	16	8
9	16	1
10	16	2
11	16	1
12	16	4
13	16	1
14	16	2
15	16	1

So, unit group of Z/16Z is (1,3,5,7,9,11,13,15)
And, Zero divisors of Z/16Z are (2,4,6,8,10,12,14)

4: Determine the unit group and the zero divisors of the ring Z/15Z.

a	b	GCD(a,b)
1	15	1
2	15	1
3	15	3
4	15	1
5	15	5
6	15	3
7	15	1
8	15	1
9	15	3
10	15	5
11	15	1
12	15	3
13	15	1
14	15	1

So, unit group of Z/15Z is (1,2,4,7,8,11,13,14)
And, Zero divisors of Z/15Z are (3,5,6,9,10,12)