CSCI361 Assignment 1

Asjad Athick
4970512
mama158

Part 2

1.
a)

1 <= a < 14
0 <= b < 14

gcd(a, m), where m = 14 = size of the alphabet must be 1. a and m need to be coprime

gcd(a,14) = 1

If the key is a multiple of the size of the alphabet, one to one mappings will not be possible

b)

The possible values of a are (6)
1, 3, 5, 9, 11, 13

The possible values of b are 0, 1 .. 13 (14 values)

14 * 6 = 84 distinct keys for the cipher

c)

a = “B” = 11
b = 3

Plaintext	4	9	7	0	5	1	2
a(X)	44	99	77	0	55	11	22
+ b	47	102	80	3	58	14	25
mod(14)	5	4	A	3	2	0	B
Ciphertext	**5**	**4**	**A**	**3**	**2**	**0**	**B**

2)

X (P)	x^2 + x +1	mod 15 == y
0	1	1
1	3	3
2	7	7
3	13	13
4	21	6
5	31	1
6	43	13
7	57	12
8	73	13
9	91	1
10	111	6
11	133	13
12	157	7
13	183	3
14	211	1

The mapping is not valid, as the function is not a one to one mapping. The duplicate values of y are highlighted in the same color.