Name: Leung Chun Wai SID: 56046680

Assignment 4

1.

$$p = 157$$
$$g = 5$$

A.

$$5(mod\ 157) = 5$$
$$5^2(mod\ 157) = 5^2(mod\ 157) = 25$$
$$5^4(mod\ 157) = 25^2(mod\ 157) = 154$$
$$5^8(mod\ 157) = 154^2(mod\ 157) = 9$$
$$5^{16}(mod\ 157) = 9^2(mod\ 157) = 81$$
$$5^{32}(mod\ 157) = 81^2(mod\ 157) = 124$$
$$5^{64}(mod\ 157) = 124^2(mod\ 157) = 147$$

$$a = 64$$
$$y_A = g^a(mod\ p)$$
$$= 5^{64}(mod\ 157)$$
$$= 147$$

B.

$$147(mod\ 157) = 147$$
$$147^2(mod\ 157) = 147^2(mod\ 157) = 100$$
$$147^4(mod\ 157) = 100^2(mod\ 157) = 109$$
$$147^8(mod\ 157) = 109^2(mod\ 157) = 106$$
$$147^{16}(mod\ 157) = 106^2(mod\ 157) = 89$$
$$147^{32}(mod\ 157) = 89^2(mod\ 157) = 71$$
$$147^{64}(mod\ 157) = 71^2(mod\ 157) = 17$$

$$b = 94$$
$$k_{AB} = {y_A}^b(mod\ p)$$
$$= 147^{94}(mod\ 157)$$
$$= 147^{1011110_b}(mod\ 157)$$
$$= 100 \times 109 \times 106 \times 89 \times 17(mod\ 157)$$
$$= 89$$

2.

$$N = 37 \times 47$$
$$= 1739$$
$$e = 25$$

A.

$$\phi(N) = (37 - 1)(47 - 1)$$
$$= 1656$$
$$ed \equiv 1\big(mod\ \phi(N)\big)$$
$$25d \equiv 1(mod\ 1656)$$

1656	**25**		
1	0	1656	A
0	1	25	B
1	-66	6	$C = A - 66B$
-4	**265**	1	$D = B - 4C$

$$d = 265$$

B.

$$314(mod\ 1739) = 314$$
$$314^2(mod\ 1739) = 314^2(mod\ 1739) = 1212$$
$$314^4(mod\ 1739) = 1212^2(mod\ 1739) = 1228$$
$$314^8(mod\ 1739) = 1228^2(mod\ 1739) = 271$$
$$314^{16}(mod\ 1739) = 271^2(mod\ 1739) = 403$$

$$m = 314$$
$$c = m^e(mod\ N)$$
$$= 314^{25}(mod\ 1739)$$
$$= 314^{11001_b}(mod\ 1739)$$
$$= 314 \times 271 \times 403(mod\ 1739)$$
$$= 1541$$