EE4215 Cybersecurity Technology

Assignment 4 (Solution)

1.

a)

The public key should be

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

We compute it using the square-and-multiply method as follows:

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

b)

The secret key is $k = {y_A}^b (\text{mod } p) = 147^{94} (\text{mod } 157)$.

We compute it using the square-and-multiply method as follows:

$$147^2 (\text{mod } 157) = 100$$
$$147^4 (\text{mod} 157) = 109$$
$$147^8 (\text{mod } 157) = 106$$
$$147^{16} (\text{mod } 157) = 89$$
$$147^{32} (\text{mod } 157) = 71$$
$$147^{64} (\text{mod } 157) = 17$$
$$147^{94} (\text{mod } 157) = 147^{64} 147^{16} 147^8 147^4 147^2 \ (\text{mod } 157) = 89$$

2.

a) Since $N = 37 \times 47$, which implies $\phi(N) = (p-1)(q-1) = 36 \times 46 = 1656$, and $25d \equiv 1 \ (\text{mod } 1656)$.

1656	25		
1	0	1656	a
0	1	25	b
1	-66	6	$c = a - 66b$
-4	265	1	$d = b - 4c$

Hence, $d \equiv 265 \ (\text{mod } 1656)$.

b) The ciphertext is given by $c = 314^{25} \ (\text{mod } N) = 314^{25} \ (\text{mod} 1739)$.

$$314^2 \text{ mod } 1739 = 1212 \ mod \ 1739$$
$$314^4 \text{ mod } 1739 = 1228 \text{ mod } 1739$$
$$314^8 \text{ mod } 1739 = 271 \text{ mod } 1739$$
$$314^{16} \text{ mod } 1739 = 403 \text{ mod } 1739$$
$$314^{25} \ (\text{mod} 1739) = 314^{16+8+1} \text{ mod } 899 = 403 \times 271 \times 314 \text{ mod } 1739$$
$$= 1541 \ mod \ 1739$$

Hence, $c = 1541$.