Section 5 Lecture 33 –Diffie-Hellman Key Exchange

Exercises

Q1)

Perform the full Diffie-Hellman key exchange to establish a secret key in the following:

(i) $p = 13$, $g = 6$, Alice has private key $a = 4$ and Bob has private key $b = 7$

(ii) $p = 5$, $g = 2$, Alice has private key $a = 2$ and Bob has private key $b = 4$

(iii) $p = 23$, $g = 5$, Alice has private key $a = 13$ and Bob has private key $b = 8$

Q2)

The following steps set up a secret key between Alice, Bob and Carol:

- Alice sends $A_1 = g^a \pmod p$ to Bob
- Bob calculates $B_1 = (A_1)^b \pmod p$ and sends it Carol
- Carol calculates $(B_1)^c \pmod p$ which establishes her secret key
- Bob calculates $B_2 = g^b \pmod p$ and sends it Carol
- Carol calculates $C_1 = (B_2)^c \pmod p$ and sends it Alice
- Alice calculates $(C_1)^a \pmod p$ which establishes her secret key
- Carol calculates $C_2 = g^c \pmod p$ and sends it Alice
- Alice calculates $A_2 = (C_2)^a \pmod p$ and sends it Bob
- Bob calculates $(A_2)^b \pmod p$ which establishes his secret key
- The three established secret keys should all match and can be used for communication

Illustrate this procedure with $p = 17$ and $g = 3$, Alice chooses secret key $a = 7$, Bob chooses secret key $b = 4$ and Carol chooses secret key $c = 10$.