Section 5 Lecture 33 –Diffie-Hellman Key Exchange

Solutions

Q1)

(i)

Alice sends $A = g^a \pmod p = 6^4 \pmod{13} = 9$ to Bob
Bob sends $B = g^b \pmod p = 6^7 \pmod{13} = 7$ to Alice
Alice calculates $B^a \pmod p = 7^4 \pmod{13} = 9$
Bob calculates $A^b \pmod p = 9^7 \pmod{13} = 9$
The agreed secret key = 9

(ii)

Alice sends $A = g^a \pmod p = 2^2 \pmod 5 = 4$ to Bob
Bob sends $B = g^b \pmod p = 2^4 \pmod 5 = 1$ to Alice
Alice calculates $B^a \pmod p = 1^2 \pmod 5 = 1$
Bob calculates $A^b \pmod p = 1^4 \pmod 5 = 1$
The agreed secret key = 1

(iii)

Alice sends $A = g^a \pmod p = 5^{13} \pmod{23} = 21$ to Bob
Bob sends $B = g^b \pmod p = 5^8 \pmod{23} = 16$ to Alice
Alice calculates $B^a \pmod p = 16^{13} \pmod{23} = 3$
Bob calculates $A^b \pmod p = 21^8 \pmod{23} = 3$
The agreed secret key = 3

Q2)

- Alice sends $A_1 = g^a \pmod p = 3^7 \pmod{17} = 11$ to Bob
- Bob calculates $B_1 = (A_1)^b \pmod p = 11^4 \pmod{17} = 4$ and sends it Carol
- Carol calculates $(B_1)^c \pmod p = 4^{10} \pmod{17} = 16$ which is her secret key
- Bob calculates $B_2 = g^b \pmod p = 3^4 \pmod{17} = 13$ and sends it Carol
- Carol calculates $C_1 = (B_2)^c \pmod p = 13^{10} \pmod{17} = 16$ and sends it Alice
- Alice calculates $(C_1)^a \pmod p = 16^7 \pmod{17} = 16$ which is her secret key
- Carol calculates $C_2 = g^c \pmod p = 3^{10} \pmod{17} = 8$ and sends it Alice
- Alice calculates $A_2 = (C_2)^a \pmod p = 8^7 \pmod{17} = 15$ and sends it Bob
- Bob calculates $(A_2)^b \pmod p = 15^4 \pmod{17} = 16$ which is his secret key
- The three established secret keys 16 all match