Example 1

Let’s select:

G =4 N=7 [Link]

Bob and Alice generate random numbers (x and y):

X = 3

Y = 4

Bob calculates A:

A = G^x mod N = 4^3 mod 7 = 64 mod 7 = 1

Alice calculates B:

B = G^y mod N = 4^4 mod 7 = 256 mod 7 = 4

They swap values and they generate the key:

Key (Bob) = B^x mod N = 4^3 mod 7 = 256 mod 7 = 1

Key (Alice) = A^y mod N = 1^4 mod 7 = 256 mod 7 = 1

This is their shared key.

Example 2

In this example Bob and Alice have the same x and y value. Let’s select:

G =5 N=11 [Link]

Bob and Alice generate random numbers (x and y):

X = 7

Y = 7

Bob calculates A:

A = G^x mod N = 5^7 mod 11 = 78125 mod 11 = 3

Alice calculates B:

B = G^y mod N = 5^7 mod 11 = 78125 mod 11 = 3

They swap values and they generate the key:

Key (Bob) = B^x mod N = 3^7 mod 11 = 2187 mod 7 = 9

Key (Alice) = A^y mod N = 3^7 mod 11 = 2187 mod 7 = 9

This is their shared key.

Example 3

Let's select:

G =281 N=3049 [Link]

Bob and Alice generate random numbers (x and y):

X = 21

Y = 6

Bob calculates A:

$A = 281^{21} \bmod 3049 = 2856$

Alice calculates B:

$B = 281^{6} \bmod 3049 = 2545$

They swap values and they generate the key:

Key (Bob) = $2856^{21} \bmod 3049 = 452$

Key (Alice) = $2545^{6} \bmod 3049 = 452$

This is their shared key.

Tutorial

1 What is the shared key for G=5, N=23, x=6 and y=15? [Ans: 2][Link]

2 What is the shared key for G=7, N=11, x=7 and y=7? [Ans: 8][Link]

3 What is the shared key for G=8, N=13, x=7 and y=9? [Ans: 5][Link]

4 What is the shared key for G=10, N=541, x=5 and y=7? [Ans: 193][Link]

5 What is the shared key for G=3709, N=9157, x=17 and y=19? [Ans: 2795][Link]

6 What is the shared key for G=991, N=4397, x=13 and y=9? [Ans: 927][Link]

7 What is the shared key for G=877, N=1783, x=6 and y=15? [Ans: 1038][Link]

■ Prof Bill Buchanan, Feb 2015