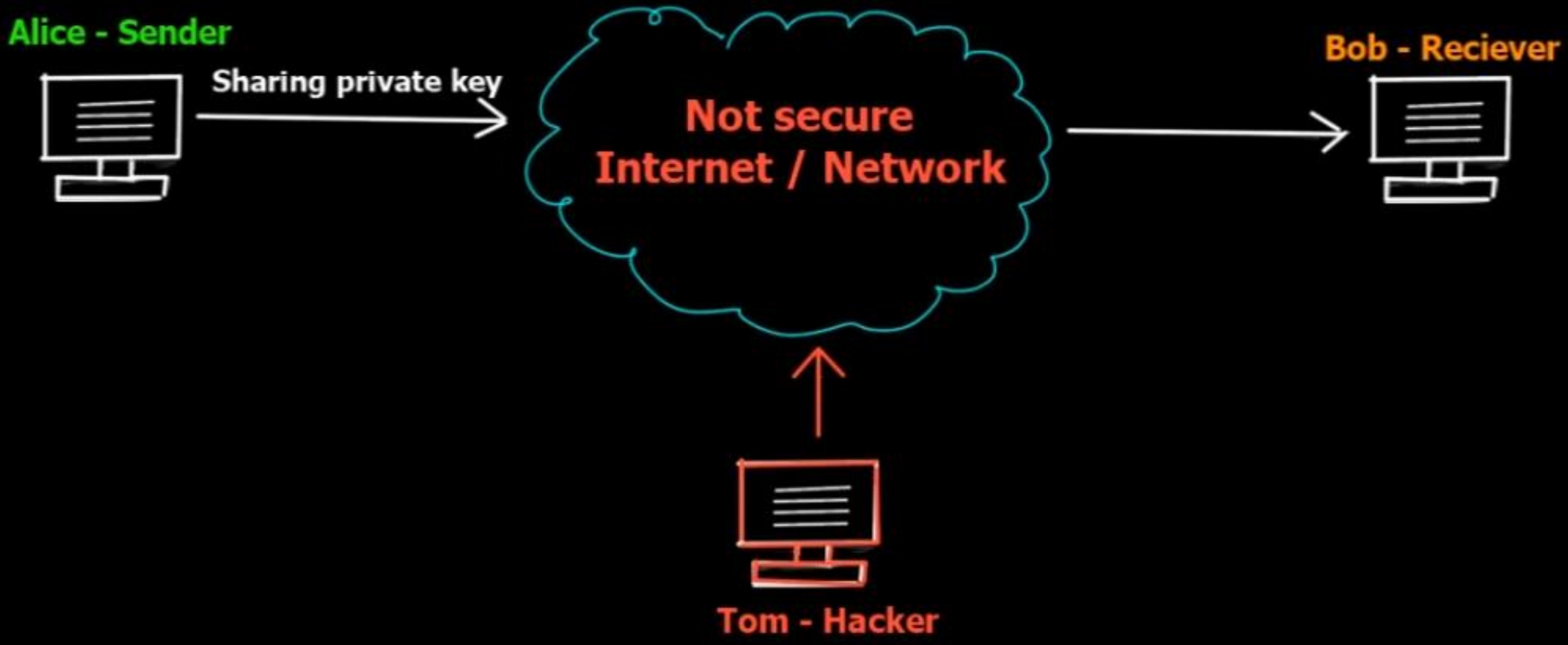
Diffie Hellman

Key Exchange

Diffie-Hellman Key Exchange Agreement/Algorithm

Symmetric Key Cryptography - The Problem of Key Distribution

>> Key exchange solution is not fool proof or is not practically possible.
>> This problem is called as key distribution or key exchange problem.
>> It is inherently linked with the symmetric key cryptography



Diffie-Hellman Key Exchange Agreement/Algorithm

Diffie-Hellman Key Exchange/Agreement Algorithm

>> Two parties, can agree on a symmetric key using this technique.

>> This can then be used for encryption/ decryption.

>> This algorithm can be used only for key agreement,
but not for encryption or decryption.

>> It is based on mathematical principles.

Algorithm -

1. Firstly Alice & Bob agree upon 2 large prime numbers - n & g
   These 2 numbers need not be secret & can be shared publicly.
2. Alice chooses another large random number x(private to her)
   & calcuates A such that : $A = g^x \bmod n$
3. Alice sends this to Bob.
4. Bob chooses another large random number y(private to him)
   & calcuates B such that : $B = g^y \bmod n$
5. Bob sends this to Alice.
6. Alice now computes her secret key K1 as follows:
   $K1 = B^x \bmod n$
7. Bob computes his secret key K2 as follows:
   $K2 = A^y \bmod n$
8. K1 = K2 (key exchange complete)

Diffie-Hellman Key Exchange Agreement/Algorithm

Diffie-Hellman Key Exchange/Agreement Algorithm

>> Two parties, can agree on a symmetric key using this technique.

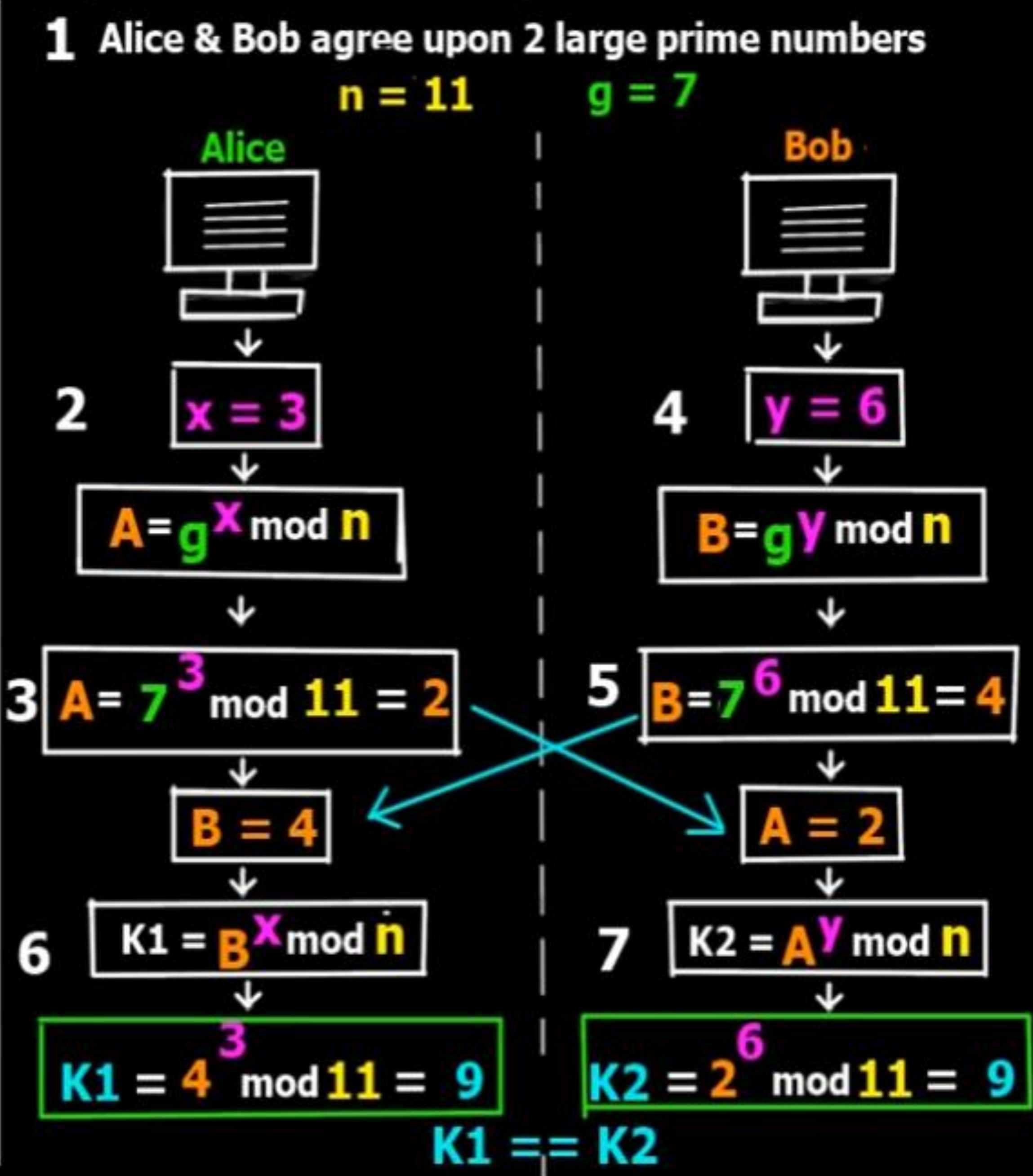
>> This can then be used for encryption/ decryption.

>> This algorithm can be used only for key agreement, but not for encryption or decryption.

>> It is based on mathematical principles.

Algorithm -

1. Firstly Alice & Bob agree upon 2 large prime numbers - n & g
   These 2 numbers need not be secret & can be shared publicly.
2. Alice chooses another large random number x (private to her) & calcuates A such that : $A = g^x \bmod n$
3. Alice sends this to Bob.
4. Bob chooses another large random number y (private to him) & calcuates B such that : $B = g^y \bmod n$
5. Bob sends this to Alice.
6. Alice now computes her secret key K1 as follows:
   $K1 = B^x \bmod n$
7. Bob computes his secret key K2 as follows:
   $K2 = A^y \bmod n$
8. K1 = K2 (key exchange complete)



Diffie-Hellman Key Exchange Agreement/Algorithm

Diffie-Hellman Key Exchange/Agreement Algorithm

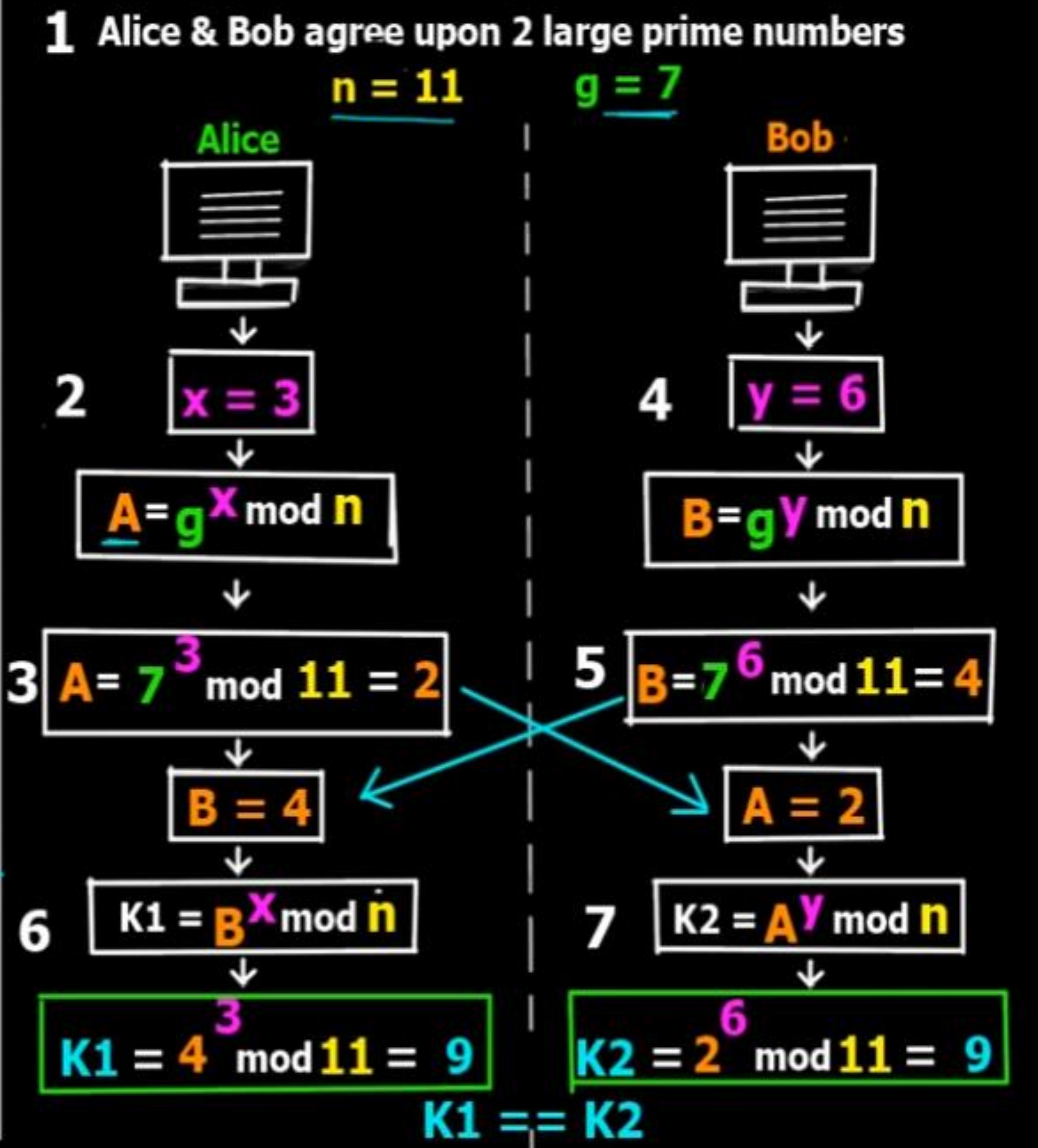
>> Two parties, can agree on a symmetric key using this technique.
>> This can then be used for encryption/ decryption.
>> This algorithm can be used only for key agreement, but not for encryption or decryption.
>> It is based on mathematical principles.

$7^3 = 343 \bmod 11$
$= 2$

Algorithm -

1. Firstly Alice & Bob agree upon 2 large prime numbers - n & g
   These 2 numbers need not be secret & can be shared publicly.
2. Alice chooses another large random number x(private to her) & calcuates A such that : $A = g^x \bmod n$
3. Alice sends this to Bob.
4. Bob chooses another large random number y(private to him) & calcuates B such that : $B = g^y \bmod n$
5. Bob sends this to Alice.
6. Alice now computes her secret key K1 as follows:
   $K1 = B^x \bmod n$
7. Bob computes his secret key K2 as follows:
   $K2 = A^y \bmod n$
8. K1 = K2 (key exchange complete)

31
11)343
33↓
13
-11
2



Diffie-Hellman Key Exchange Agreement/Algorithm

Mathematical Theory -

Firstly, take a look at what Alice does in step 6.

>> $K1 = B^{x} \bmod n$

What is B? From step 4, we have

>> $B = g^{y} \bmod n$

Therefore if we substitute this value of B in step 6.

>> $K1 = (g^{y})^{x} \bmod n = g^{yx} \bmod n$ ———— 1

Now, take a look at what Bob does in step 7.

>> $K2 = A^{y} \bmod n$

What is A? From step 2, we have

>> $A = g^{x} \bmod n$

Therefor if we substitute this value of A in step 7.

>> $K2 = (g^{x})^{y} \bmod n = g^{xy} \bmod n$ ———— 2

Now Basic Mathematics say that:

>> $K^{yx} = K^{xy}$

Therefore, in this case, we have

>> $K1 = K2 = K$