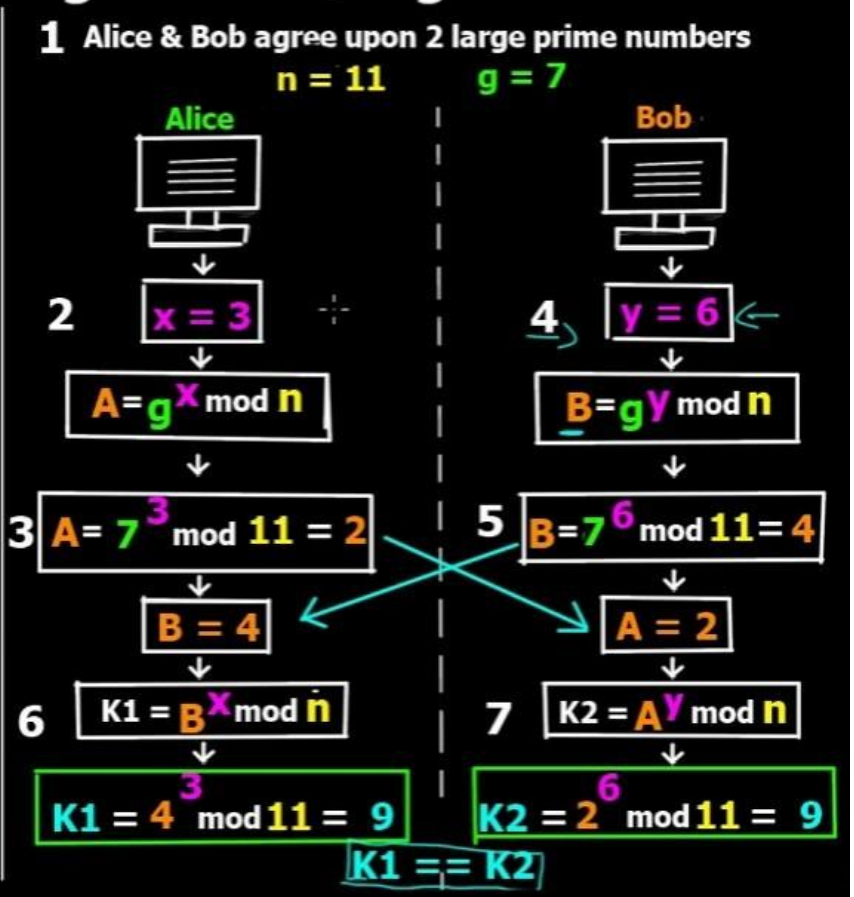
# Diffie-Hellman Key Exchange Agreement/Algorithm

## Diffie-Hellman Key Exchange/Agreement Algorithm

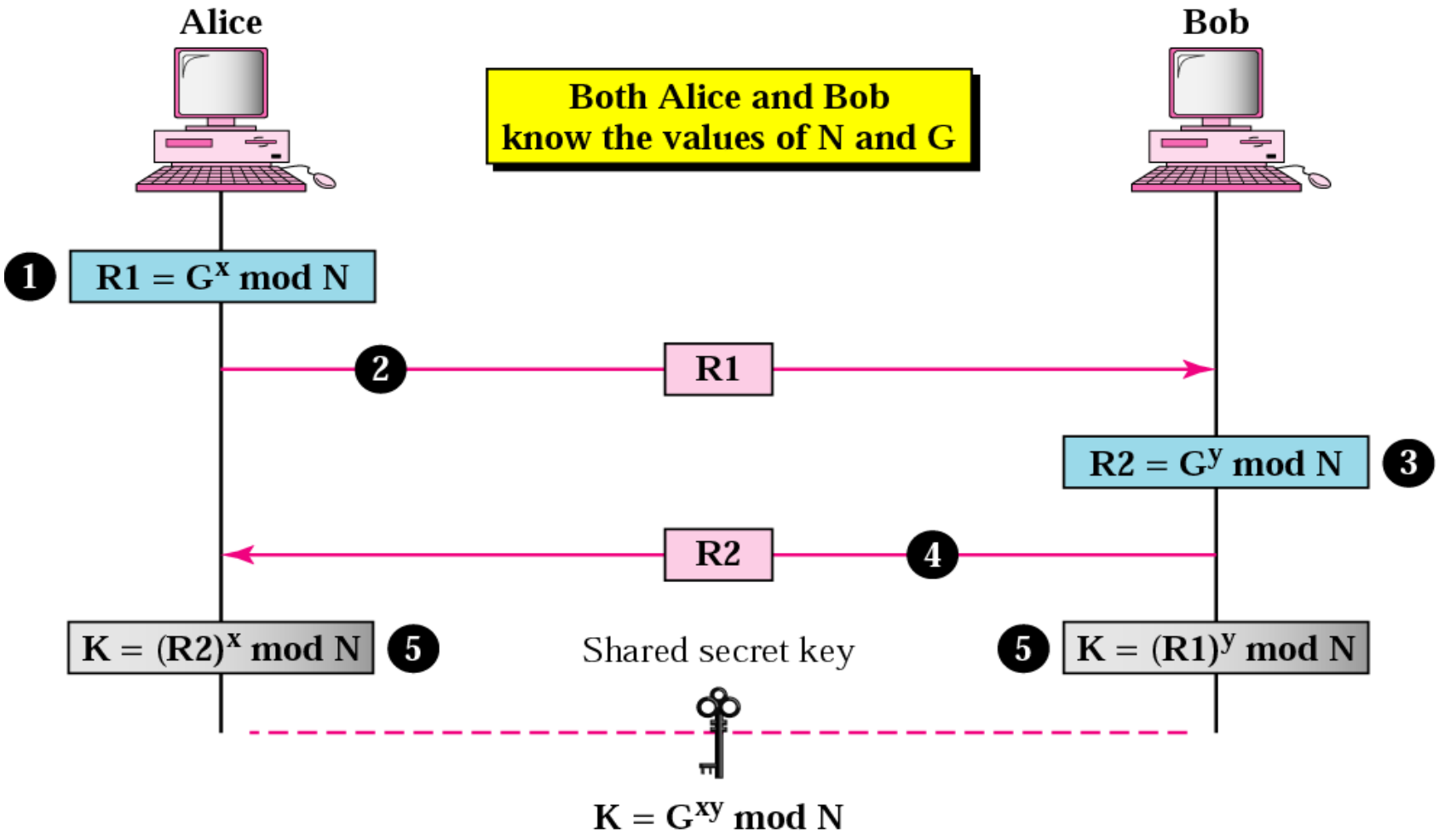
>> Two parties, can agree on a symmetric key using this technique.
>> This can then be used for encryption/ decryption.
>> This algorithm can be used only for key agreement, but not for encryption or decryption.
>> It is based on mathematical principles.

## 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 method



*The symmetric (shared) key in the Diffie-Hellman protocol is*

$$K = G^{xy} \bmod N.$$

Agree upon two numbers:

P Prime Number 13

G Generator of P 6

Private = 5

Randomly generate a Private Key

Private = 4

$(6^{5})$ MOD 13

(7776) MOD 13

Public = 2

Calculate Public Key:

$(G^{Private})$ MOD P

$(6^{4})$ MOD 13

(1296) MOD 13

Public = 9

Exchange Public Keys

$(9^{5})$ MOD 13

(59049) MOD 13

Shared Secret = 3

Calculate the Shared Secret

$(Shared\ Public^{Private})$ MOD P

$(2^{4})$ MOD 13

(16) MOD 13

Shared Secret = 3

PRACTICAL NETWORKING .NET

# *Example*

Assume G = 7 and N = 23. The steps are as follows:

1. Alice chooses x = 3 and calculates R1 = $7^3$ mod 23 = 21.
2. Alice sends the number 21 to Bob.
3. Bob chooses y = 6 and calculates R2 = $7^6$ mod 23 = 4.
4. Bob sends the number 4 to Alice.
5. Alice calculates the symmetric key K = $4^3$ mod 23 = 18.
6. Bob calculates the symmetric key K = $21^6$ mod 23 = 18.

The value of K is the same for both Alice and Bob;
$G^{xy}$ mod N = $7^{18}$ mod 23 = 18.

www.irongeek.com/diffie-hellman.php

**Dirty Diffie-Hellman**
**(Like dirty Santa, but geekier)**

Crappy PHP script for a simple Diffie-Hellman key exchange calculator. I guess I could have used Javascript instead of PHP, but I had rounding errors.

Set these two for everyone

g: 10 p: 541

| | Alice | Bob |
|---|---|---|
| a: | 3 | |
| b: | | 6 |

Submit

a = 3

$A = g^a \bmod p = 10^3 \bmod 541 = 459$

b = 6

$B = g^b \bmod p = 10^6 \bmod 541 = 232$

Alice and Bob exchange A and B in view of Carl

$key_a = B^a \bmod p = 232^3 \bmod 541 = 347$

$key_b = A^B \bmod p = 459^6 \bmod 541 = 347$