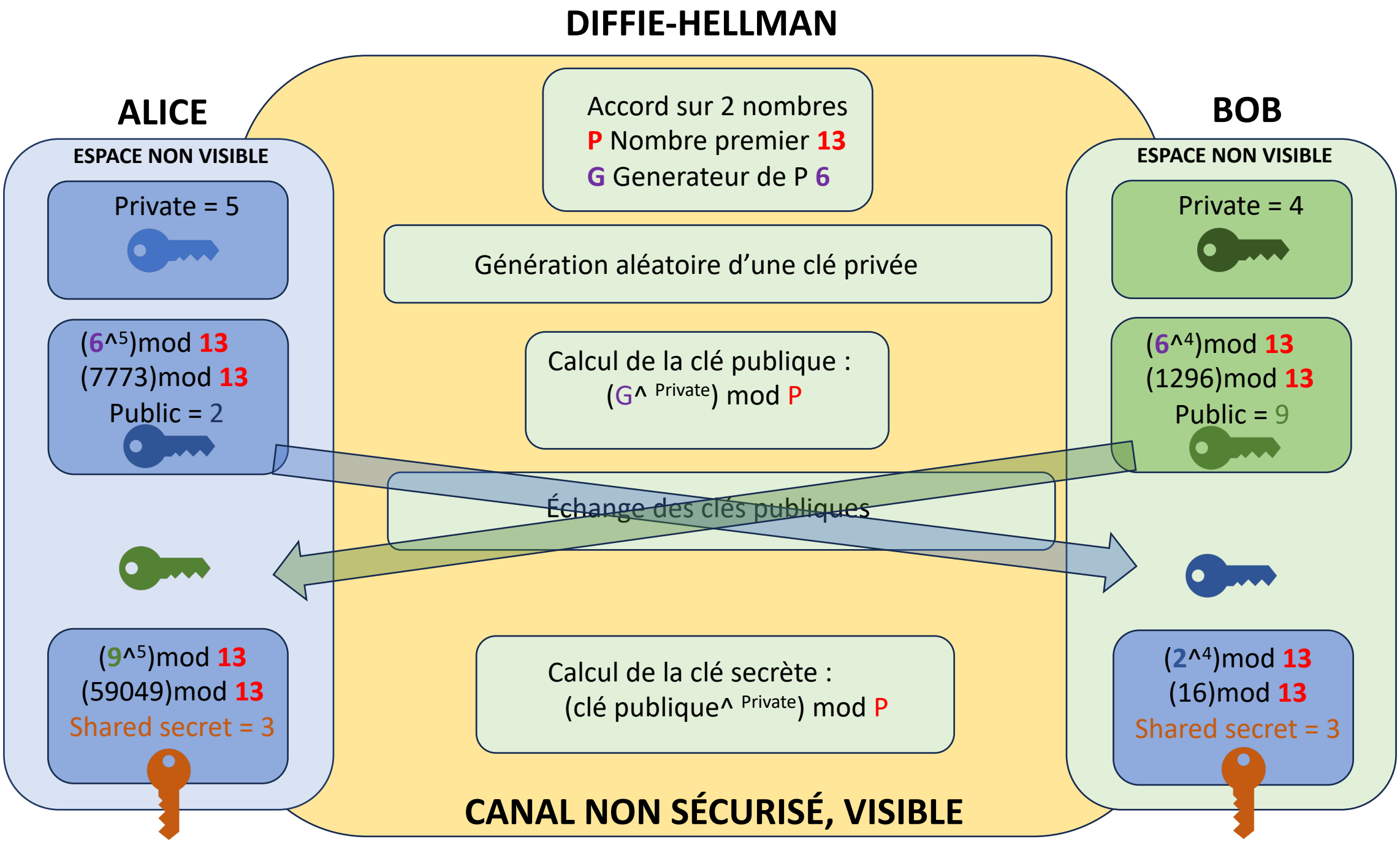
DIFFIE-HELLMAN
ALICE
ESPACE NON VISIBLE
Private = 5
(6^5)mod 13
(7773)mod 13
Public = 2
(9^5)mod 13
(59049)mod 13
Shared secret = 3
Accord sur 2 nombres
P Nombre premier 13
G Generateur de P 6
Génération aléatoire d'une clé privée
Calcul de la clé publique :
(G^ Private) mod P
Échange des clés publiques
Calcul de la clé secrète :
(clé publique^ Private) mod P
CANAL NON SÉCURISÉ, VISIBLE
BOB
ESPACE NON VISIBLE
Private = 4
(6^4)mod 13
(1296)mod 13
Public = 9
(2^4)mod 13
(16)mod 13
Shared secret = 3

# DIFFIE-HELLMAN

- Permet le partage de clé secrète sur un média non sécurisé
  Cette clé servira ensuite pour générer une clé symétrique

- La sécurité de DH est basée sur le problème du Logarithme Discret
  Exponentiation :
  G et X sont donnés, il est facile de trouver N

$G^{\wedge X} = N$

  Logarithme :
  G et N sont donnés, il est difficile de trouver X.

  Exponentiation discret :
  G,X et P sont donnés, il est facile de trouver N.

$G^{\wedge X} \text{ MOD } P = N$

  Logarithme discret :
  G,P et N sont donnés, il est impossible de trouver X mathématiquement.
  Seule la méthode qui consiste à essayer toutes les combinaisons possibles peut marcher (brute force).