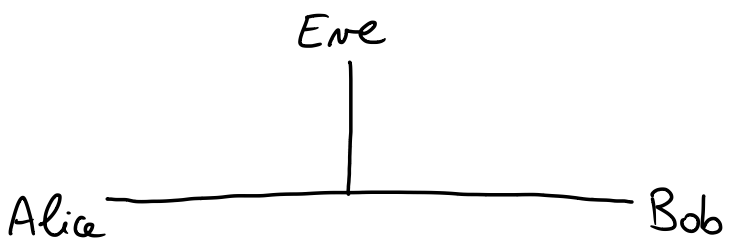
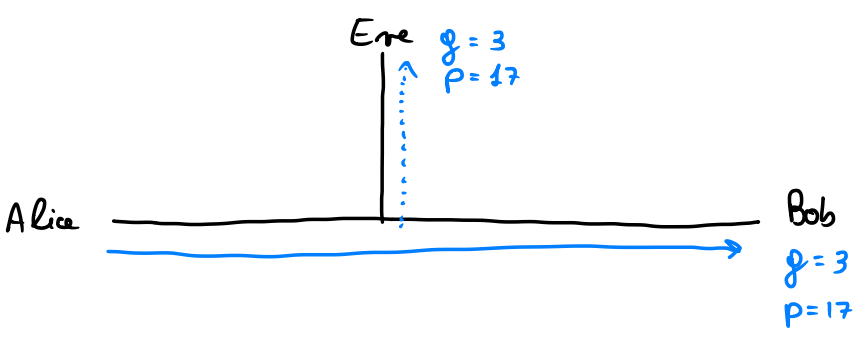
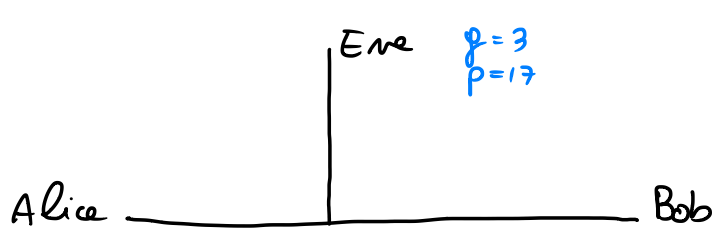
Diffie Hellman



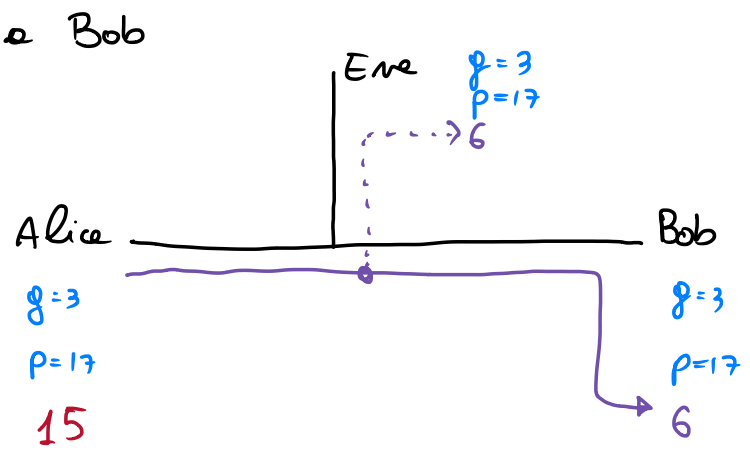
1. Alice e Bob si mettono d'accordo su un numero primo (17) e un generatore (3)



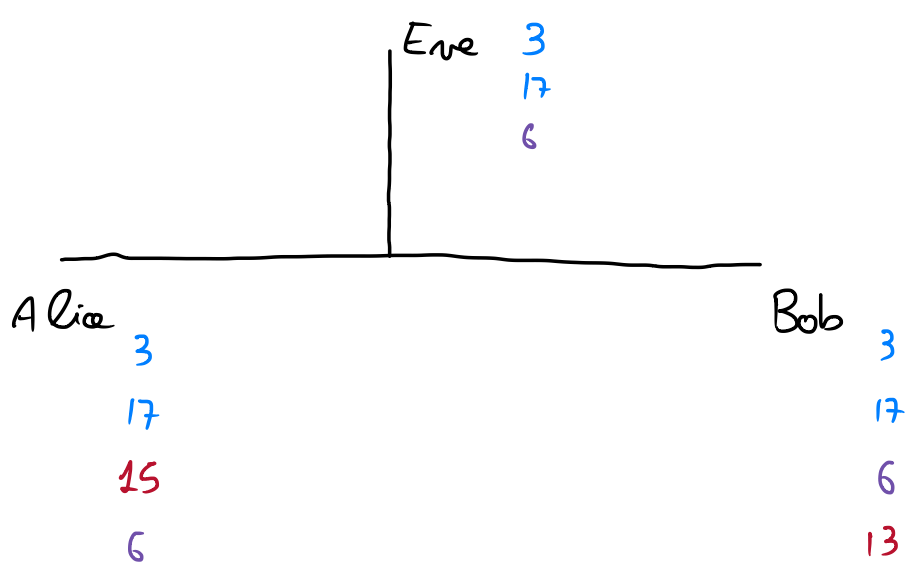
2. Alice genera un numero casuale (15) e lo tiene per se



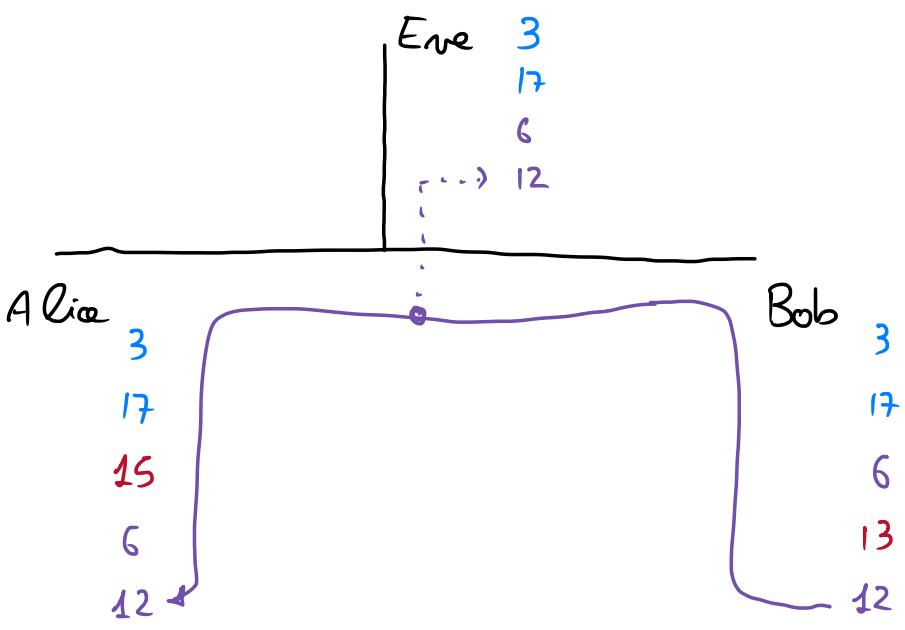
3. Alice calcola $3^{15} \% 17 = 6$ e lo manda a Bob



4. Bob sceglie il suo numero casuale (13)



5. Bob calcola $3^{13} \% 17 = 12$ e lo manda sul canale



6. Alice prende il risultato di Bob (12) e calcola

$12^{15} \% 17 = 10$ Segreto condiviso

7. Bob prende il risultato di Alice (6) e calcola

$6^{13} \% 17 = 10$ Segreto condiviso

PERCHÈ SUCCEDE

Alice calcola $12^{15} \% 17 = 10$

Bob $6^{13} \% 17 = 10$

$12^{15} \% 17 = 6^{13} \% 17$

Il 12 che ha usato Alice deriva da $3^{13} \% 17$

$12^{15} \% 17 =$

$= (3^{13} \% 17)^{15} \% 17 =$ ($3^{13} \% 17$ può essere eliminato)

$= (3^{13})^{15} \% 17 =$

$= (3^{15})^{13} \% 17$

Il 6 usato da Bob deriva da $3^{15} \% 17$

$6^{13} \% 17 =$

$= (3^{15} \% 17)^{13} \% 17 =$

$= (3^{15})^{13} \% 17$

Senza avere uno dei due numeri casuali privati Eve non è in grado di trovare la soluzione.
Con numeri abbastanza grandi è praticamente impossibile per Eve trovare la soluzione in una quantità di tempo accettabile.