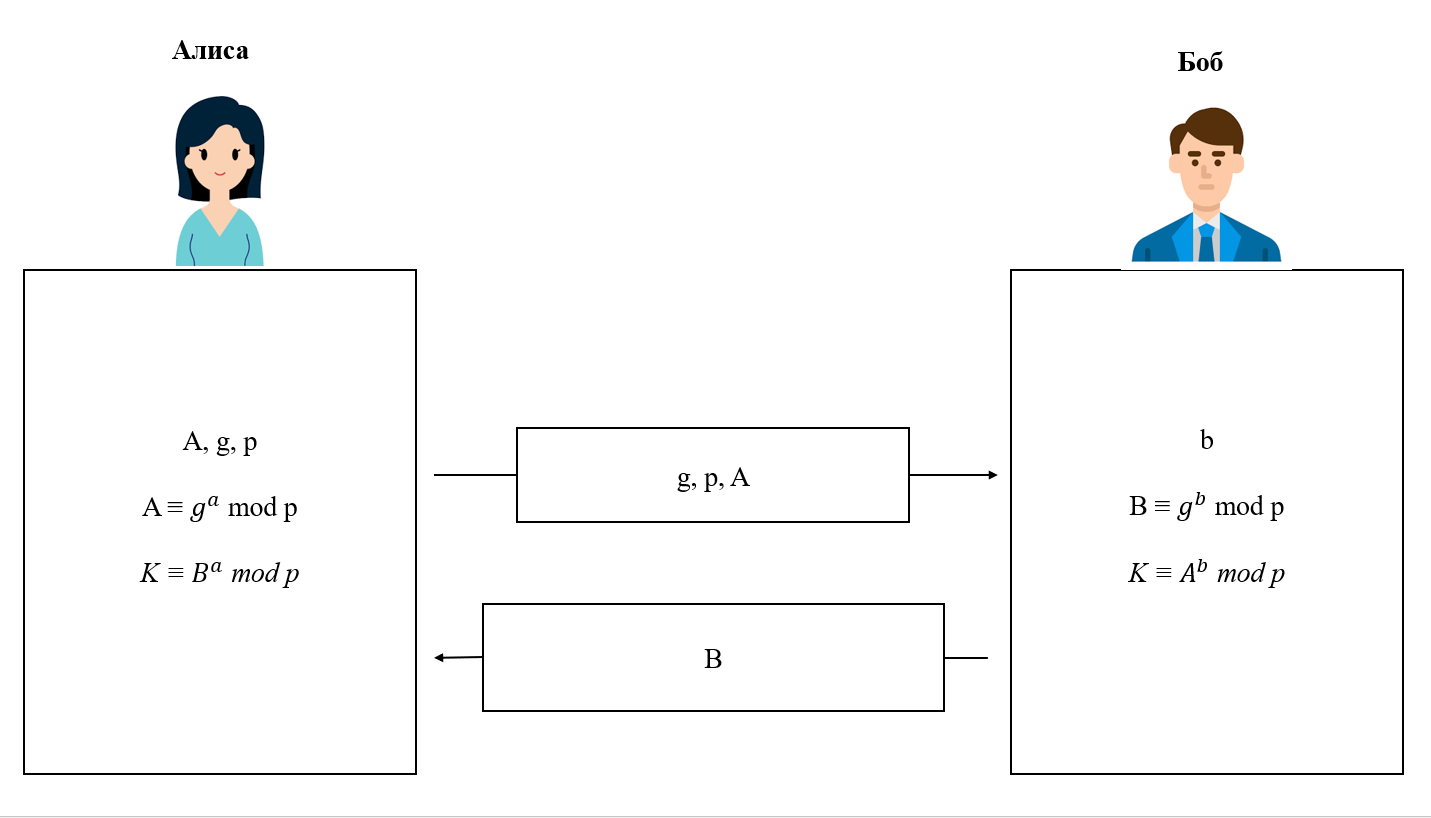
**ДИФФИ-ХЕЛМАН АЛГОРИТМІ**

Диффи-Хеллман алгоритмі ашық кілт алмасу әдісі болып табылады. Ол екі тараптың ортақ құпия кілтті ашық байланыс арқылы қауіпсіз түрде бөлісуіне мүмкіндік береді.



**Бұл алгоритм төмендегі қадамдардан тұрады:**

* p – үлкен жай сан және g – оның түбірі таңдалады.

**Алиса мен Боб өздеріне жабық кілттер (a және b) таңдайды.**

Жария кілттер есептеледі:

Алиса: A = ga mod p

Боб: B = gb mod p

**Алиса мен Боб ортақ құпия кілтті есептейді:**

K = Ba mod p = Ab mod p

**ПРАКТИКАЛЫҚ ТАПСЫРМА**

Алиса мен Боб келесі параметрлерді пайдаланады:

**• p=23**

**• g=5**

Алиса жабық кілт ретінде a=6, ал Боб b=15 таңдайды.

А,В,К мәндерін табыңыз.Осы мәндерді табатын Python-да бағдарлама құрыңыз.