Алгоритм Диффи-Хеллмана

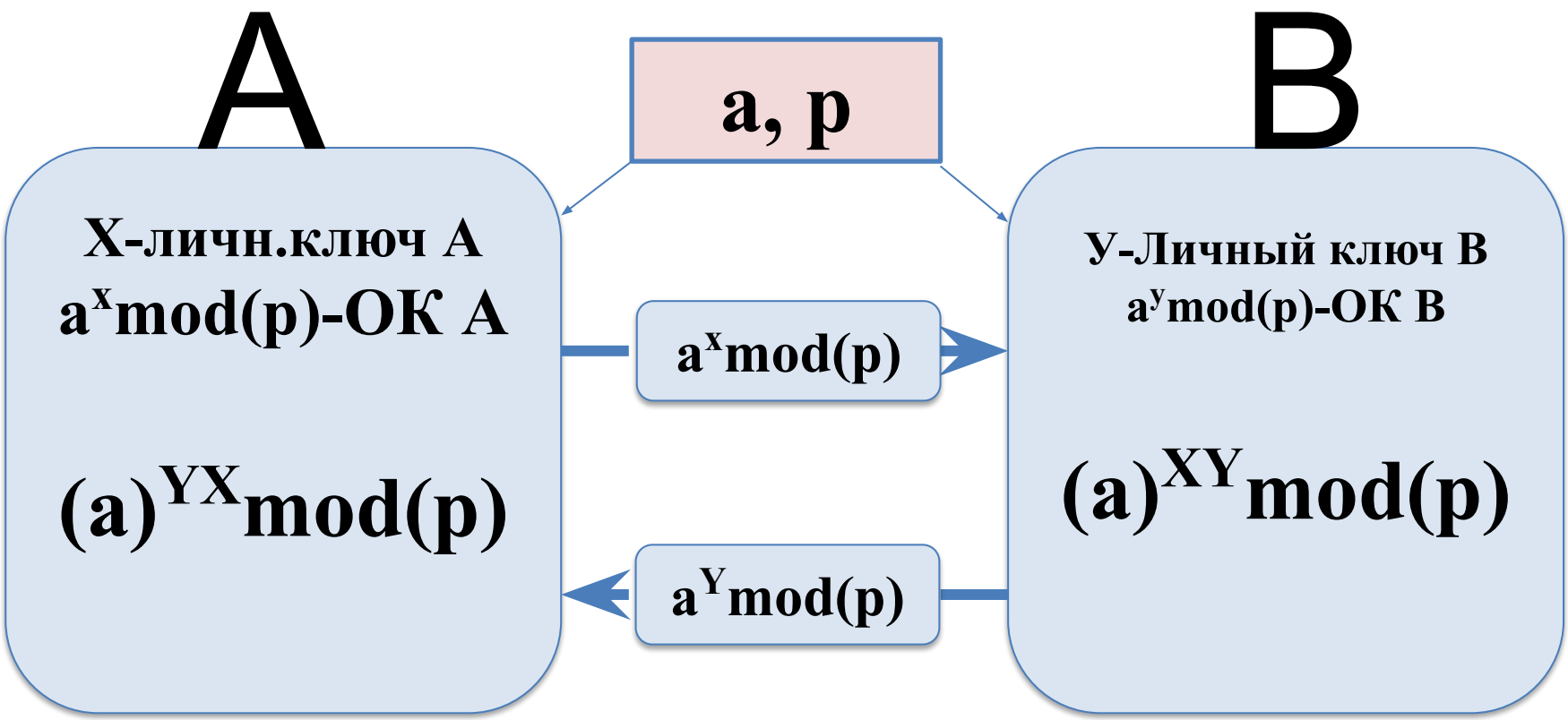
Алгоритм Диффи-Хеллмана

- позволяет двум удаленным пользователям выработать секретный ключ в результате переговоров по прослушиваемому каналу.

Алгоритм предполагает:

- независимое генерирование каждым из двух пользователей своего случайного числа;
- преобразование этого числа вследствие процедур;
- обмен преобразованными ключами по открытому каналу;
- вычисление общего секретного ключа.

Алгоритм Диффи — Хеллмана



a подбирается таким образом, чтобы $a^n mod(p)$, $0<n<p-1$ давало бы все целые числа в диапазоне от ***1*** до ***p***. При этом числа ***p*** и ***(p-1)/2*** – простые**.**

Вычисление общего секретного ключа по алгоритму Диффи-Хеллмана

Польз-ли договариваются по секр. каналам о пересекающихся значениях **a** и **p** (это м.б. всем известные параметры)

пользователь А подбирает случайным образом число ***x***, пользователь В – число ***y*** (личные ключи) ;

пользователь А вычисляет $A=a^x mod(p)$, пользователь В вычисляет $B=a^y mod(p)$;

пользователи обмениваются полученными открытыми ключами;

пользователь А вычисляет $(B)^x mod(p)$, пользователь В вычисляет $(A)^y mod(p)$;

полученное число a^{xy} является общим секретным ключом;

Злоумышленник, перехвативший значения **A, B,** a^x ***и*** a^y не сможет сформировать секретное значение a^{xy} **.**