





Алиса знает:

- Открытый ключ Алисы
- Закрытый ключ Алисы
- Открытый ключ Боба

Алиса может вычислить:

- Общий секретный ключ

Серер знает:

- Открытый ключ Алисы
- Открытый ключ Боба

Сервер может вычислить:

Боб знает:

- Открытый ключ Боба
- Закрытый ключ Боба
- Открытый ключ Алисы

Боб может вычислить:

- Общий секретный ключ

