**Протокол Хьюза**

Вариация алгоритма Диффи-Хелмана.

Общие параметры: – большое простое число, – первообразный корень .

Частные параметры: – большое число, удовлетворяющая условию (для стойкости желательно также условие: , где – простое число.

Шаги протокола:

Шаг 1. Алиса: ,

Шаг 2. Боб:

Шаг 3.

Шаг 4. :

Шаг 5. Б: ,

На выходе