## Отчёт по лабораторной работе "Протокол Диффи — Хеллмана".

## Реализация протокола.

Были реализованы следующие алгоритмы: алгоритм генерации общего секрета, алгоритм получения параметров (g,p,q), алгоритм проверки числа на простоту, алгоритм проверки открытого ключа.

Краткое описание работы реализации:

- 1. Для начала Алиса вычисляет параметры цифровой подписи на основе RSA: публичный (n,e) и приватный ключ(n,d).
- 2. После (n,e) передаются Бобу, он проверяет формат пакета и отправляет "ОК" в случае успеха.
- 3. Если Алиса получила "OK", то она вычисляет параметры протокола (g,p,q), свой приватный (private Alice) и открытый ключ (public Alice).
- 4. Далее создается и отправляется Бобу сообщение вида: msg:signature, где msg public|g|p; signature подпись хэша от msg.
- 5. После получения Боб проверяет вычисляет хэш от msg и цифровую подпись уже имеющимся у него публичным ключом (n,e).
- 6. Если подпись действительна, то Боб генерирует свой публичный (public Bob) и приватный ключ (private Bob).
- 7. Затем Боб отправляет свой публичный ключ Алисе
- 8. Затем Боб и Алиса находят общий секретный ключ:

```
key = public Alice^{private Bob} mod p = public Bob^{private Alice} mod p
```

Были использованы следующие алгоритмы при реализации:

- 1. алгоритм получения параметров (g,p,q), а также алгоритм проверки открытого ключа <a href="https://www.protokols.ru/WP/rfc2631/">https://www.protokols.ru/WP/rfc2631/</a>
- для проверки чисел на простоту использовался тест Миллера-Рабина https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub186.pdf (стр.14):

```
Step 1. Set i = 1 and n \ge 50.
```

Step 2. Set w = the integer to be tested,  $w = 1 + 2^a m$ , where m is odd and  $2^a$  is the largest power of 2 dividing w - 1.

Step 3. Generate a random integer b in the range 1 < b < w.

Step 4. Set j = 0 and  $z = b^m \mod w$ .

Step 5. If j = 0 and z = 1, or if z = w - 1, go to step 9.

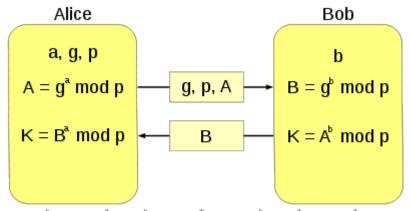
Step 6. If j > 0 and z = 1, go to step 8.

Step 7. j = j + 1. If j < a, set  $z = z^2 \mod w$  and go to step 5.

Step 8. w is not prime. Stop.

Step 9. If i < n, set i = i + 1 and go to step 3. Otherwise, w is probably prime.

3. алгоритм генерации общего секрета:



 $K = A^b \mod p = (g^a \mod p)^b \mod p = g^{ab} \mod p = (g^b \mod p)^a \mod p = B^a \mod p$