$3^3 \equiv 6 \pmod 7$,

$3^4 \equiv 4 \pmod 7$,

$3^5 \equiv 5 \pmod 7$,

$3^6 \equiv 1 \pmod 7$.

Лекция 20.09.23

1. Сколько проходов в протоколе Диффи и Хеллмана с тремя участниками?

В данном протоколе с тремя участниками будет ~~3 прохода~~ 2 цикла из 3 проходов => будет 6 проходов.

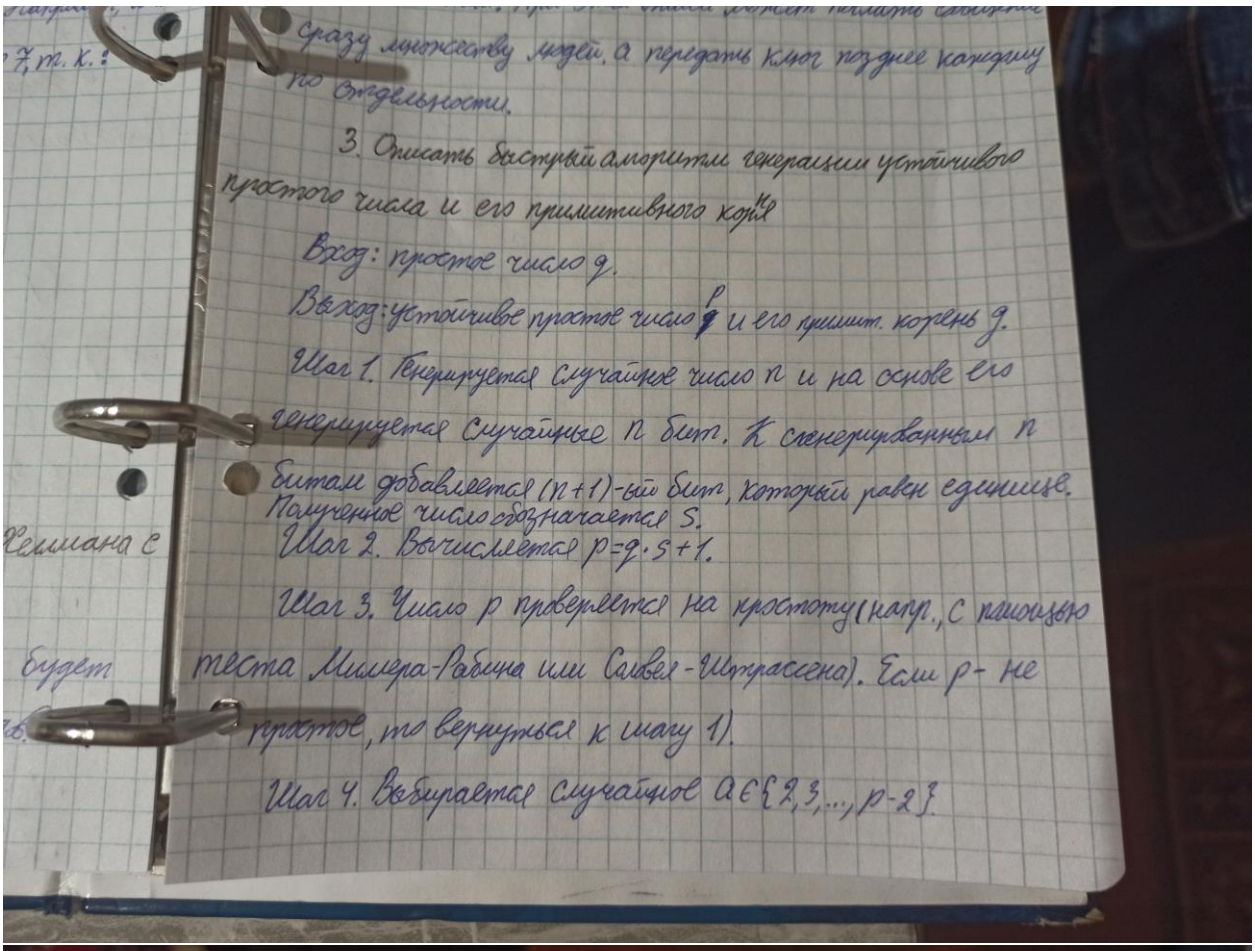
2. 1

2

2. Каким преимуществом отличается протокол Хьюза от протокола Диффи и Хеллмана?

Преимущество состоит в том, что ключ K можно вычислить заранее, до какого-либо взаимодействия, и Алиса может зашифровать сообщение с ключом K задолго до установления соединения с Бобом. При этом Алиса может послать сообщение сразу множеству людей, а передать ключ позднее каждому по отдельности.

3. Описать быстрый алгоритм генерации устойчивого простого числа и его примитивного корня



сразу множеству людей, а передать ключ позднее каждому по отдельности.

3. Описать быстрый алгоритм генерации устойчивого простого числа и его примитивного корня

Вход: простое число q.

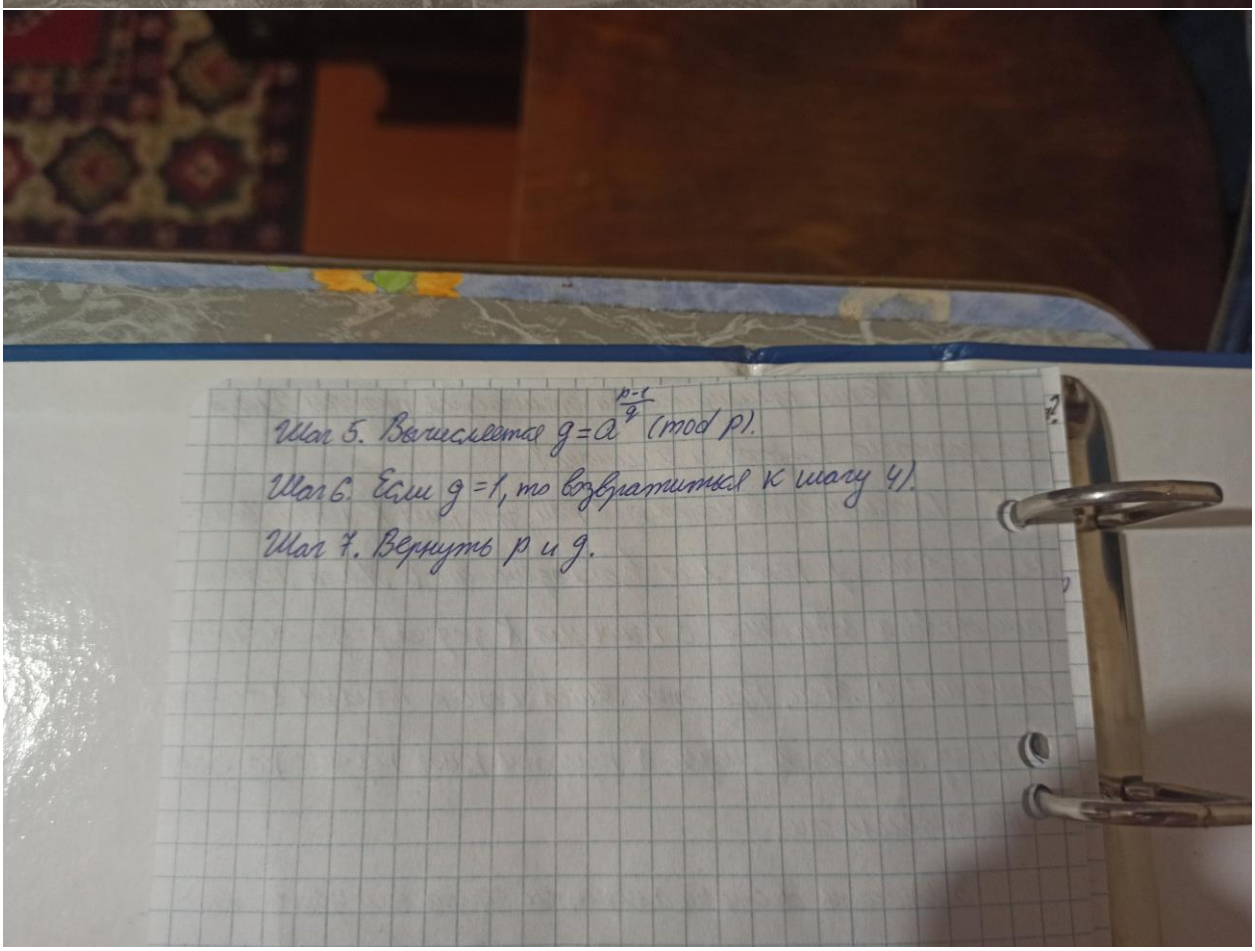
Выход: устойчивое простое число p и его примит. корень g.

Шаг 1. Генерируется случайное число n и на основе его генерируется случайные n бит. К сгенерированным n битам добавляется $(n+1)$-ый бит, который равен единице. Полученное число обозначается S.

Шаг 2. Вычисляется $p = q \cdot S + 1$.

Шаг 3. Число p проверяется на простоту (напр., с помощью теста Миллера-Рабина или Соловея-Штрассена). Если p - не простое, то вернуться к шагу 1).

Шаг 4. Выбирается случайное $a \in \{2, 3, \dots, p-2\}$.



Шаг 5. Вычисляется $g = a^{\frac{p-1}{q}} \pmod p$.

Шаг 6. Если $g = 1$, то возвратиться к шагу 4).

Шаг 7. Вернуть p и g.