**Методы защиты информации.**

**Лабораторная работа №4**

|  |
| --- |
| **Компьютерная реализация алгоритма шифрования Эль-Гамаля.** |

Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи алгоритма Эль-Гамаля.

**ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

**Алгоритм Эль-Гамаля**

Схема Эль-Гамаля (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

**Генерация ключей:**

* Генерируется случайное простое число p.
* Выбирается целое число g — первообразный корень p.
* Выбирается случайное целое число x такое, что 1 < x < p - 1.
* Вычисляется y = g^x mod p.
* Открытым ключом является y, закрытым ключом — число x.

**Шифрование**

Сообщение M должно быть меньше числа p. Сообщение шифруется следующим образом:

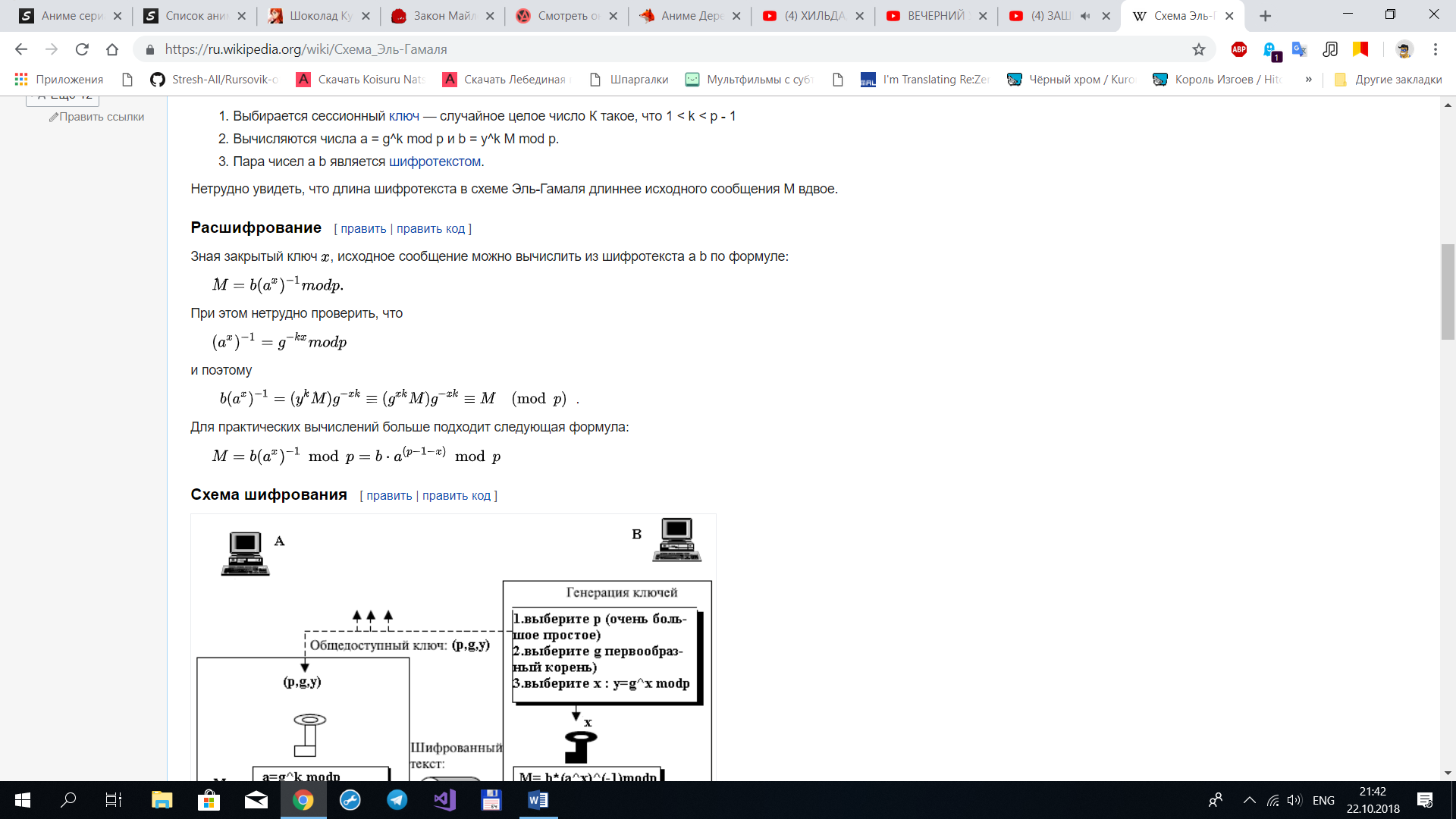
1. Выбирается сессионный ключ — случайное целое число К такое, что

1 < k < p - 1

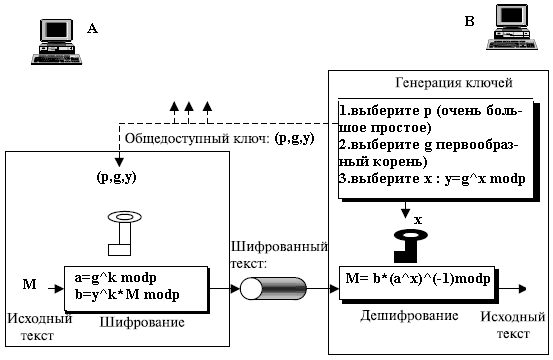
1. Вычисляются числа a = g^k mod p и b = y^k M mod p.
2. Пара чисел a b является шифротекстом.

Нетрудно увидеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

**Расшифрование**



**Схема шифрования**



**ЗАДАНИЕ:**

1)                Изучить теоретические сведения.

2)                Создать программы, читающие данные из файла и шифрующие (дешифрующие) их помощью алгоритма Эль-Гамаля.

**По результатам каждой работы студентом должен быть представлен и защищен отчет.**

**Содержание отчета включает:**

1. Титульный лист

2. Постановку задачи и описание использованных алгоритмов.

3. Блок – схему алгоритма.

4. Распечатку скриншотов результатов ввода данных и исполнения программы.

5. Распечатку программного кода.

6. Вывод.