Государственное образовательное учреждение

«Белорусский государственный технологический университет»

Отчет

*по лабораторной работе №6*

ТЕМА ЗАНЯТИЯ: КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ АЛГОРИТМОВ АСИММЕТРИЧНОГО ШИФРОВАНИЯ

|  |  |
| --- | --- |
|  | **Исполнитель:**  Студента (-ка) группы 2  Специальность\_\_\_\_ИСиТ\_\_\_  Гулевич Никита Максимович  (Ф.И.О.) |
|  | **Преподаватель**:  Ржеутская Н. В. |

Минск, 2025

Цель: овладеть основными криптографическими алгоритмами асимметричного шифрования.

АЛГОРИТМ RSA

1. Выберем 2 простых числа p и q
2. Вычислим n=p\*q
3. Вычислим функция эйлера ф(n)=(p-1)(q-1)
4. Ищем e, подойдет любое (ф,е)=1,очевидно,меньше ф
5. Ищем d, такое , что d\*e сравнимо с 1 по модулю ф

Зашифруем сообщение m

C=m^e mod n

Расшифруем

M=c^d mod n

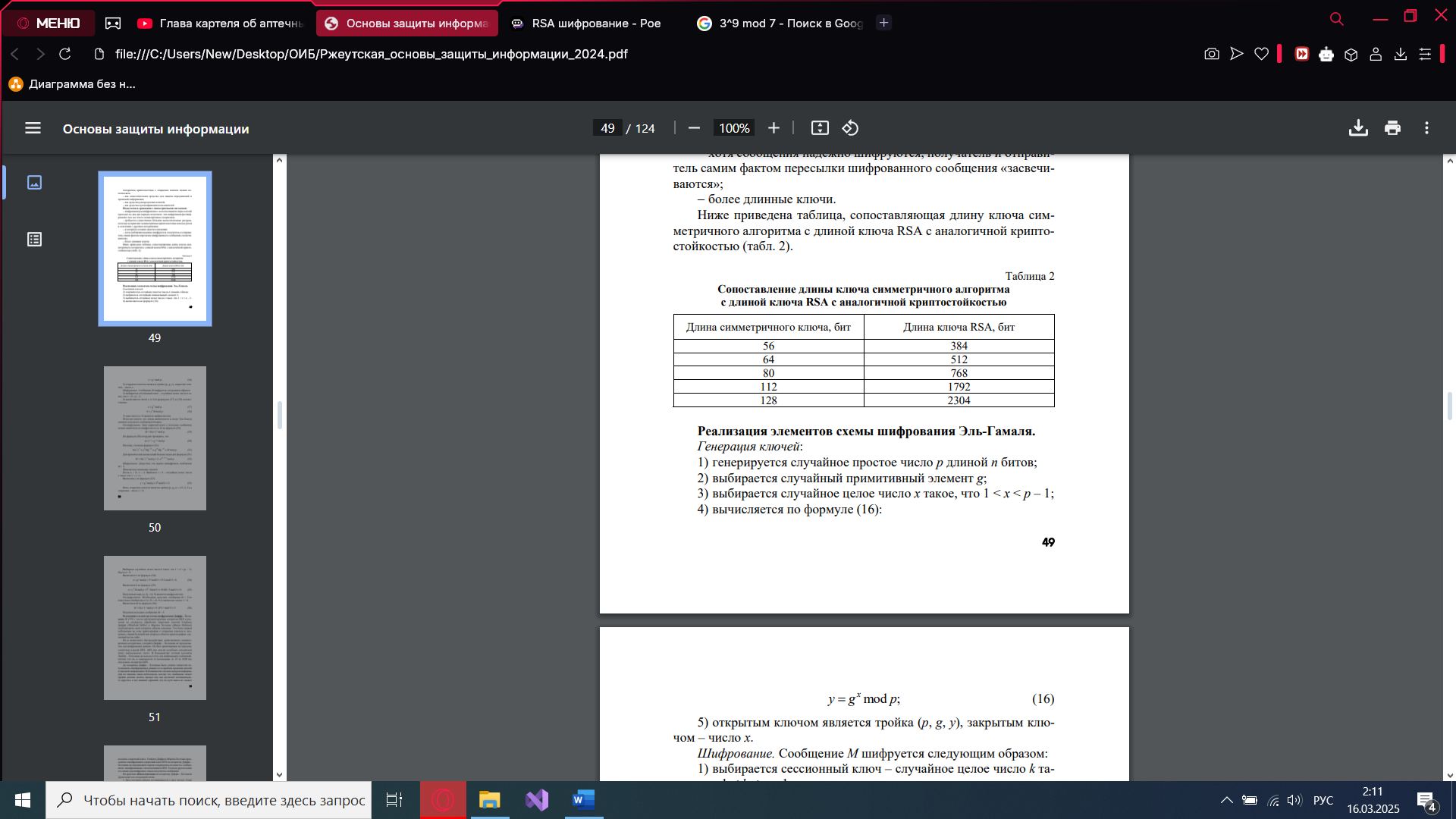
АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА

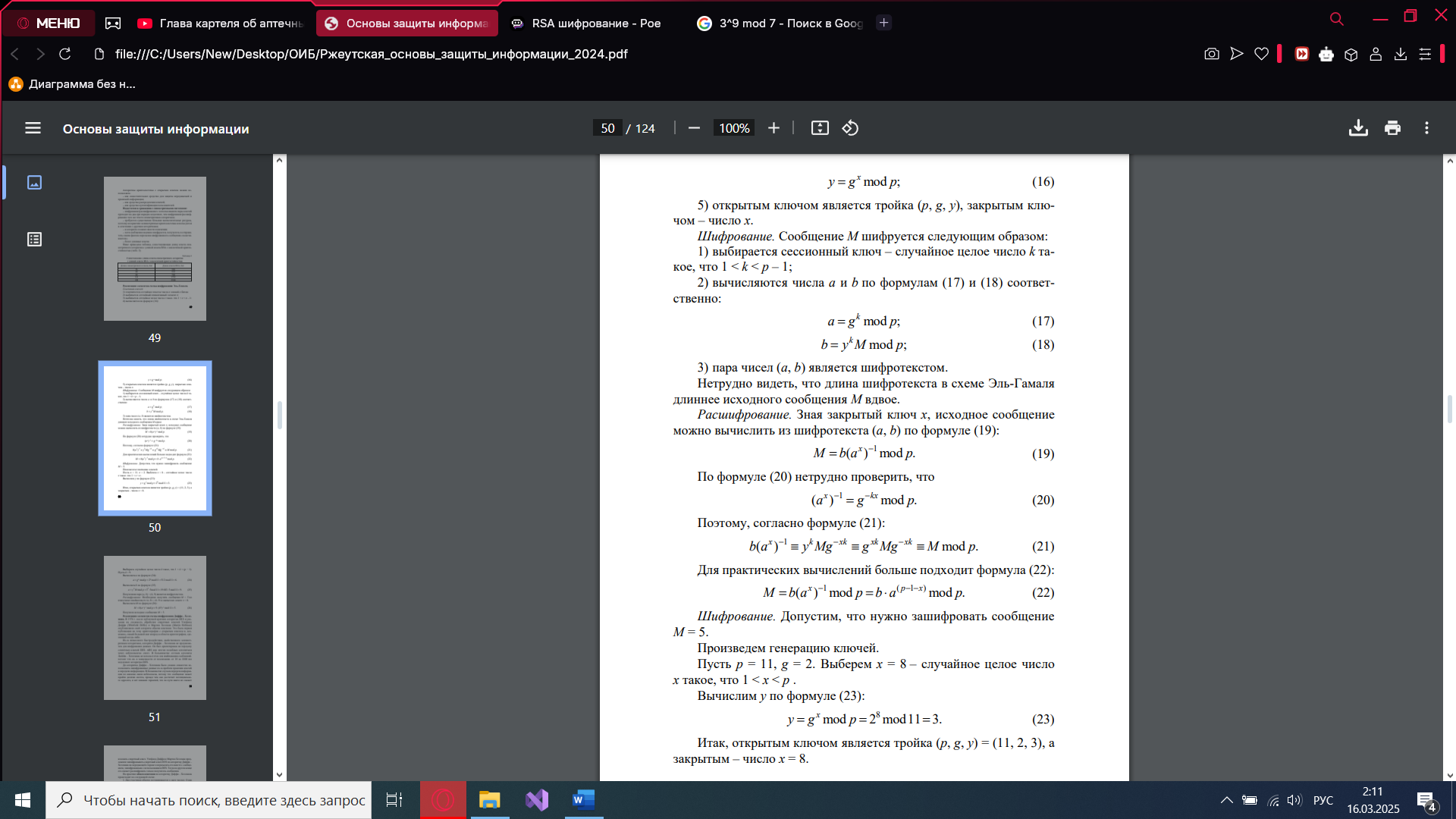
**Алгоритм Диффи-Хеллмана**

Алгоритм Диффи-Хеллмана используется для обмена ключами и позволяет двум сторонам создать общий секретный ключ по открытому каналу связи. Он состоит из следующих шагов:

1. **Выбор публичных параметров**:
   * Две стороны выбирают большое простое число p и основание g (примитивный корень по модулю p). Эти параметры могут быть известны всем.
2. **Генерация приватных ключей**:
   * Каждая сторона генерирует свой приватный ключ:
     + Пусть сторона A выбирает приватный ключ a (случайное число).
     + Сторона B выбирает приватный ключ b (случайное число).
3. **Генерация публичных ключей**:
   * Каждая сторона вычисляет свой публичный ключ:
     + Сторона A вычисляет A=g^a mod p.
     + Сторона B вычисляет B=g^b mod p.
4. **Обмен публичными ключами**:
   * Сторона A отправляет AAA стороне B, а сторона B отправляет BBB стороне A.
5. **Вычисление общего секретного ключа**:
   * Каждая сторона вычисляет общий секретный ключ:
     + Сторона A вычисляет K=B^a mod p
     + Сторона B вычисляет K=A^b mod p
   * Оба вычисления дадут одинаковый результат, и общий секретный ключ K будет известен обеим сторонам.

*Эль-Гамаля*





1. Объясните процесс работы алгоритма RSA.   
Факторизация больших чисел, довольно медленный.  
  
2. Объясните процесс работы алгоритма Диффи – Хеллмана.   
Не передает зашифрованные данные, а только промежуточные данные для получения ключа.  
  
3. Объясните процесс работы алгоритма Эль-Гамаля.  
Каждое шифрование происходит используя случайно сгенерированный ключ.

**Список использованных источников**

1. Н. В. Ржеутская, О. А. Нистюк, Н. И. Уласевич ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ Лабораторный практикум