Разработка дидактических материалов для обучения языку Python

Гончаров Фёдор БПМИ202

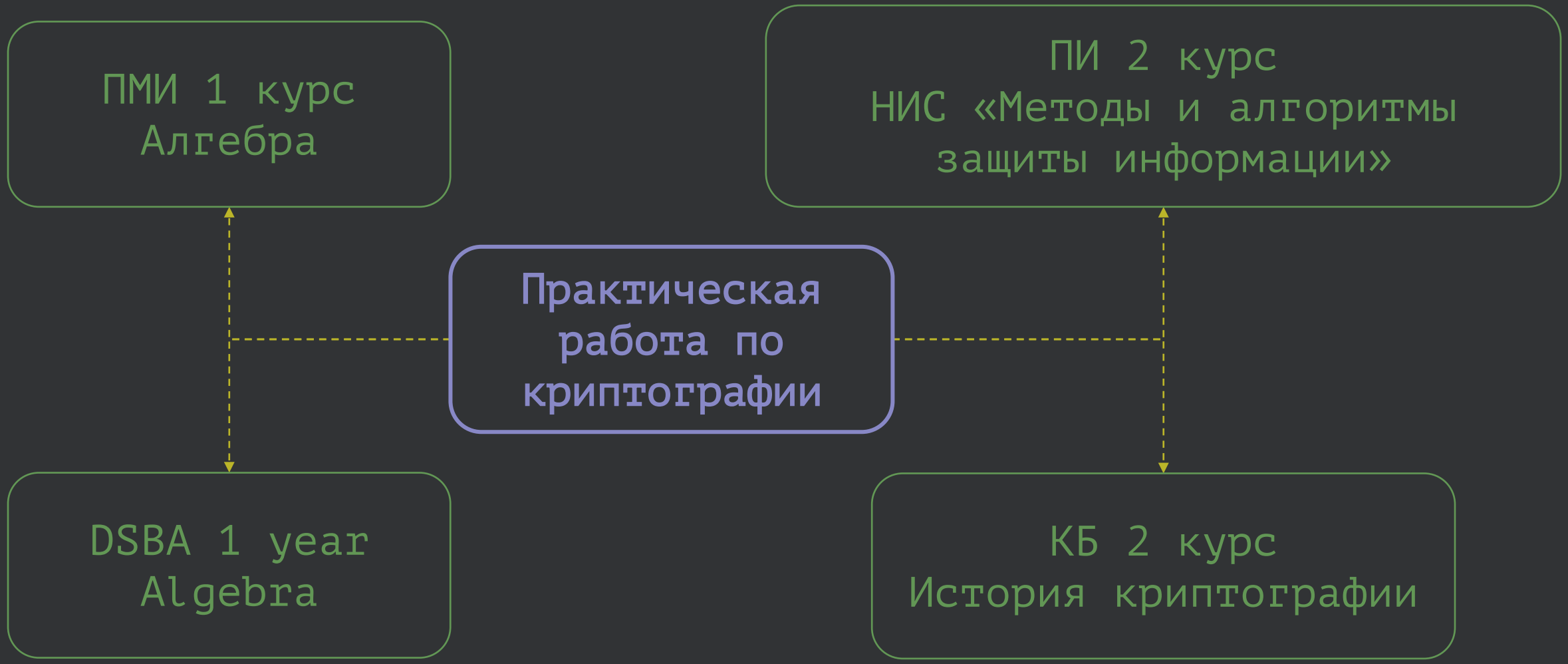
Введение

- Что объединяет все образовательные программы ФКН’а и специалитет Компьютерной безопасности в Вышке?

Введение

- Что объединяет все образовательные программы ФКН’а и специалитет Компьютерной безопасности в Вышке?
- Отсутствуют практические домашние задания по криптографии
- На занятиях недостаточно хороших визуализаций работы криптографических систем и алгоритмов

Решение


ПМИ 1 курс
Алгебра
ПИ 2 курс
НИС «Методы и алгоритмы защиты информации»
Практическая работа по криптографии
DSBA 1 year
Algebra
КБ 2 курс
История криптографии

Цель работы

Создание лабораторной работы по Алгебре и ее приложениям в Криптографии

Алгебра. Лабораторная работа 1, весна 2023

Сегодня информация и данные играют крайне важную роль как в жизни каждого человека и общества в целом, так и в экономике любой страны. Криптография (от греческого κρυπτός «скрытый» + γράφω "пишу"), оставаясь невидимой для большинства, обеспечивает безопасность обмена информацией не только между людьми, но и между цифро выми устройствами, гарантируя тем самым стабильность нашего мира. Криптография не просто интегрирована в современную жизнь, она способна изменять общество и оказывать влияние на исторические события.

В этой лабораторной работе вы познакомитесь со средой Jupyter Notebook и многими библиотеками

Структура работы

- Лабораторная работа выполнена в качестве .ipynb-файла на двух языках: русском и английском.
- К ней разработаны критерии и образцовое решение для оценивания работ.
- В каждом блоке присутствует
  - теория необходимая для решения
  - ссылки на полезные источники
  - задание для студентов

Критерии оценивания работы

- Три версии сложности работы
- Подробные критерии выставления баллов за задания
- 6 страниц

Преподавателю предлагается выделить для студентов три варианта выполнения данной практической работы (по сложности)

- Демонстрационная версия работы

Преподаватель предлагает студентам ознакомиться с работой алгоритмов, предложенных для реализации в данной лабораторной работе, объяснив их на занятии. (Для случаев, когда выполнение работы не соотносится с графиком студентов/преподавателей)

- Сложная версия работы

Преподаватель предлагает студентам выполнить каждый из 7-и блоков работы. Оценка всей работы складывается из качества выполнения каждого из блоков в соответствии со следующим соотношением: 0-3-3-2-2-1-2 (оценка за каждый блок соответственно)

- Легкая версия работы

Преподаватель предлагает студентам выполнить работу, не затрагивая блоки “Криптосистема RSA”, “Протокол с нулевым разглашением”, “Хэширование и поток шифрования”. Тогда максимальная оценка за соответствующие оставшиеся блоки меняется на:

0 - часть 0. (не оценивается)
4 - часть 1.
6 - часть 2.
1 - часть 5 (бонус).

Часть 2. Протокол Диффи-Хеллмана, криптосистема Месси-Омуры, схема Эль-Гамаля

- Оценка за данный блок формируется из выполнения трех подпунктов блока (реализации трех алгоритмов)

a. Схема Диффи-Хеллмана
100 баллов - правильно реализована схема обмена сообщениями
30 баллов - допущена ошибка при генерации ключей (выборка не из нужного диапазона), но в остальном схема верная
0 баллов - во всех остальных случаях

b. Схема Месси-Омуры
100 баллов - правильно реализована схема обмена сообщениями
30 баллов - допущена одна из ошибок: неправильно сгенерирован ключ или не проверено условие gcd(e, m-1) != 0, но в остальном верно
0 баллов - во всех остальных случаях

c. Схема Эль-Гамаля
100 баллов - правильно реализована схема обмена сообщениями
30 баллов - допущена ошибка в генерации ключей, но в остальном схема реализована верно
0 баллов - во всех остальных случаях

Баллы за подпункты суммируются и делятся на 100. То, что получается в итоге - оценка за блок. (Число от 0 до 3,00 с точностью до сотых долей)

(В случае выполнения легкой версии работы, оценка линейно переводится в шестибалльную, то есть полученная сумма умножается на 2 и делится на 100)

Часть 3. Криптосистема RSA

- Оценка за данный блок оценивается от 0 до 20 баллов, выставленных за одно практическое задание (передача сообщения с помощью протокола RSA)

2 балла - корректно сформированы ключи, передано сообщение от Алисы к Бобу с помощью протокола RSA
1 балла - не проверяется условие взаимной простоты ключа e и phi(n)
0,5 баллов - неправильно сформированы ключи, все остальное выполнено верно
0 баллов - во всех остальных случаях

Содержание работы

1. Введение, знакомство с необходимыми библиотеками
2. Алгоритм быстрого возведения в степень, постановка проблемы дискретного логарифмирования
3. Протокол Диффи-Хеллмана, криптосистема Месси-Омуры, схема Эль-Гамаля
4. Криптосистема RSA
5. Протоколы с нулевым разглашением
6. Диск Альберти, частотный анализ (Бонус)
7. Хэширование, потоковое шифрование (Бонус)

Введение, знакомство с необходимыми библиотеками

```
class Person:
  """
      A class used to represent people

      Attributes
      ----------
      name : string
          name of a person
      keys : list
          storage of persons private keys
      received : list
          storage of received values
      expected : int or string
          expected value after communication
  """
  def send_message(self, to, value, comment, log)

  def check_ans(self, ans)
```

Введение, знакомство с необходимыми библиотеками

```
class Message:
  """
      A class used to represent messages

      Attributes
      ----------
      fr : Person
          author of message
      to : Person
          addressee of message
      value : int or string
          value passed in massage
      comment : string
          add comments for log. use $...$ notaion to use LaTeX
  """
```

Введение, знакомство с необходимыми библиотеками

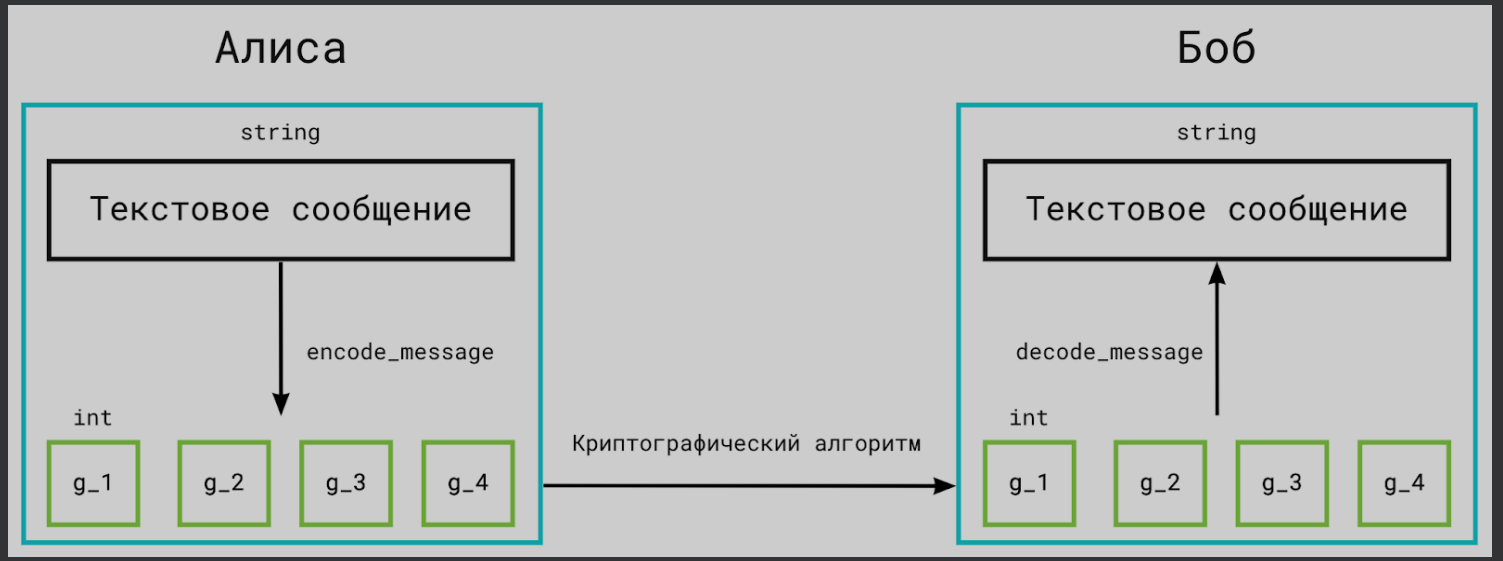
```
def encode_message(s):
    """
        Encode string s into a list of ints v
        Input
            s: string
        Output
            v: list of ints
    """
    return [ord(c) for c in s]
```

```
def decode_message(v):
    """
        Decode string s from a list of ints v
        Input
            v: list of ints
        Output
            s: string
    """
    return ''.join([chr(h) for h in v])
```

Введение, знакомство с необходимыми библиотеками

```
def visualize(log):
    """
        Draws communication process from log

        Input
            log: list of Messages
    """
```

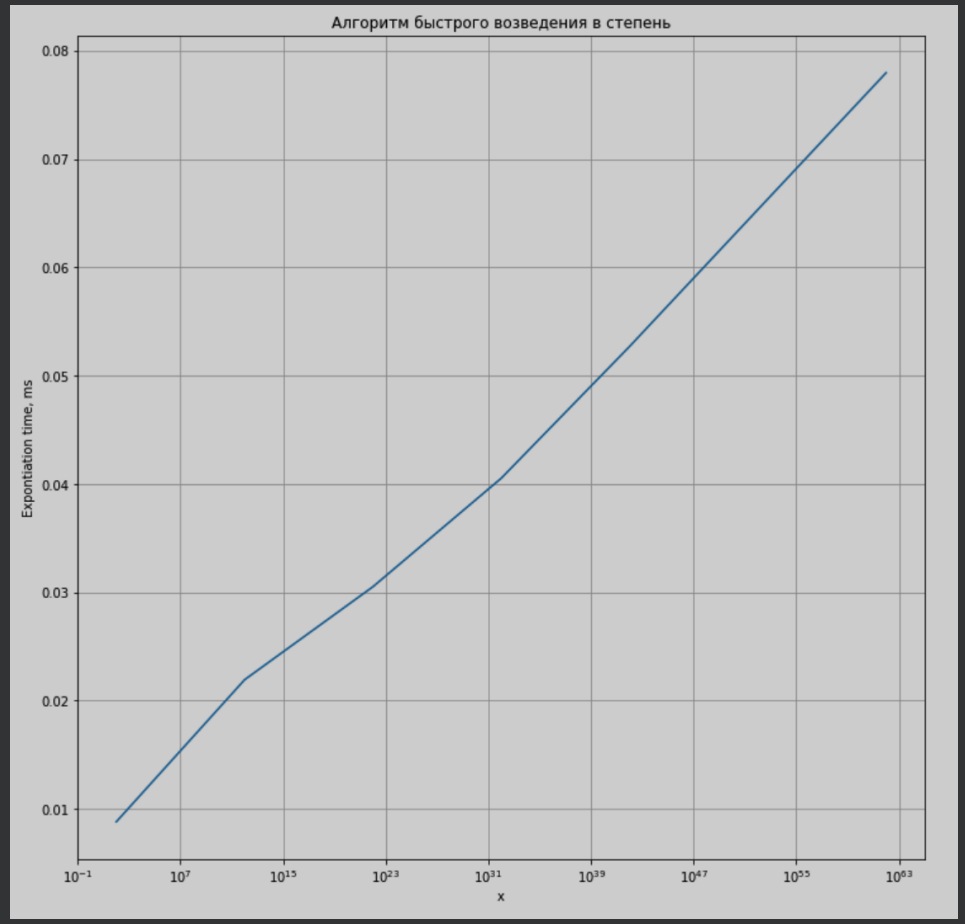


Возведение в степень, дискретный логарифм и факторизация

Каждая тема состоит из 3 задач:

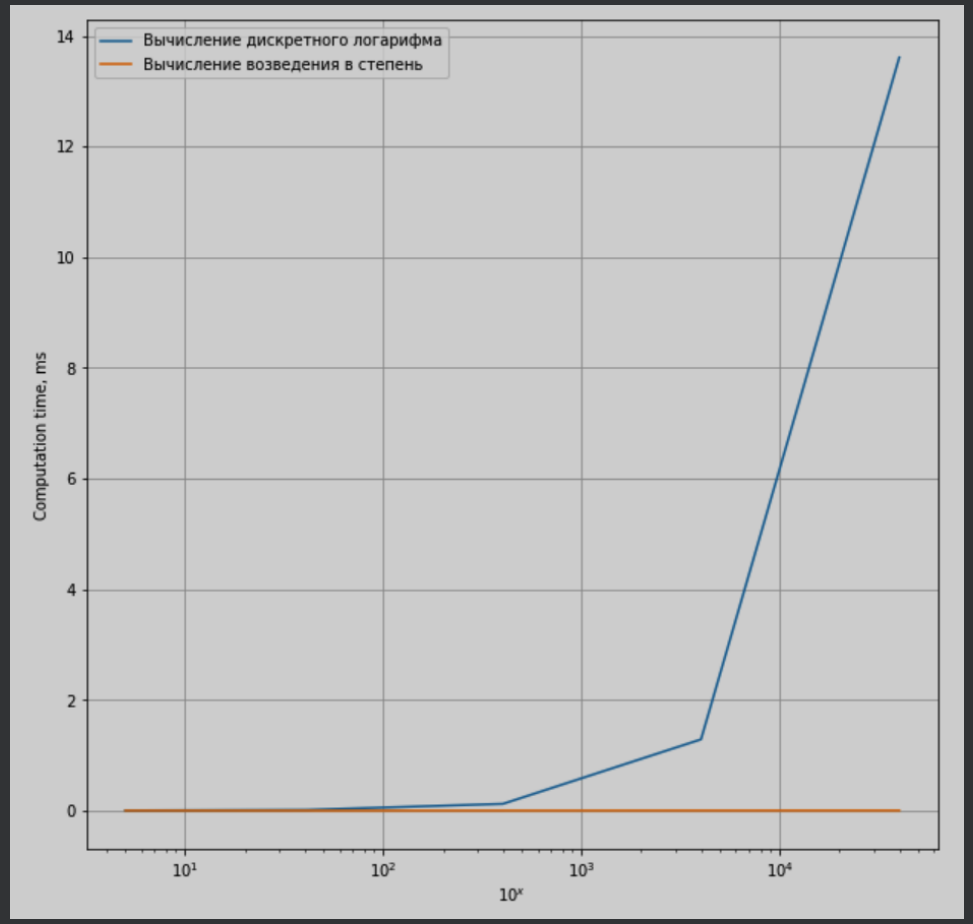
- Реализовать алгоритм
- Построить график времени выполнения
- Охарактеризовать темпы роста времени вычисления

Алгоритм быстрого возведения в степень



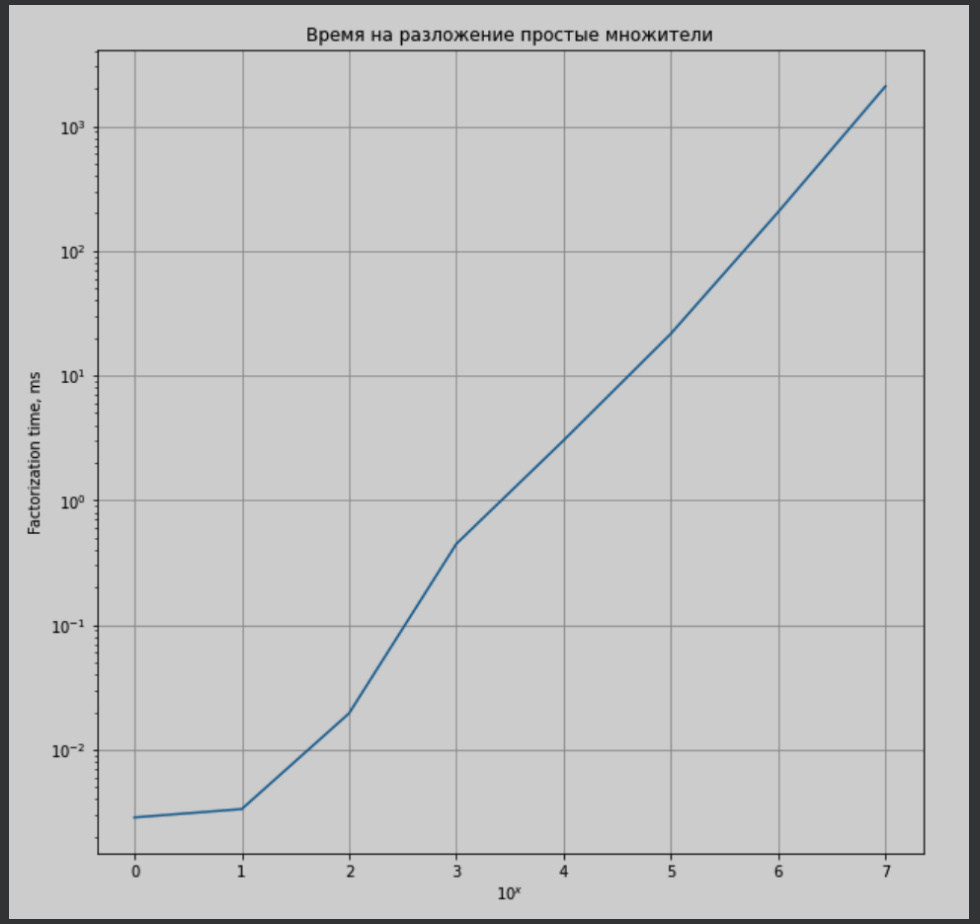
Логарифмический рост

Проблема дискретного логарифмирования



Экспоненциальный рост

Разложение на простые числа, факторизация



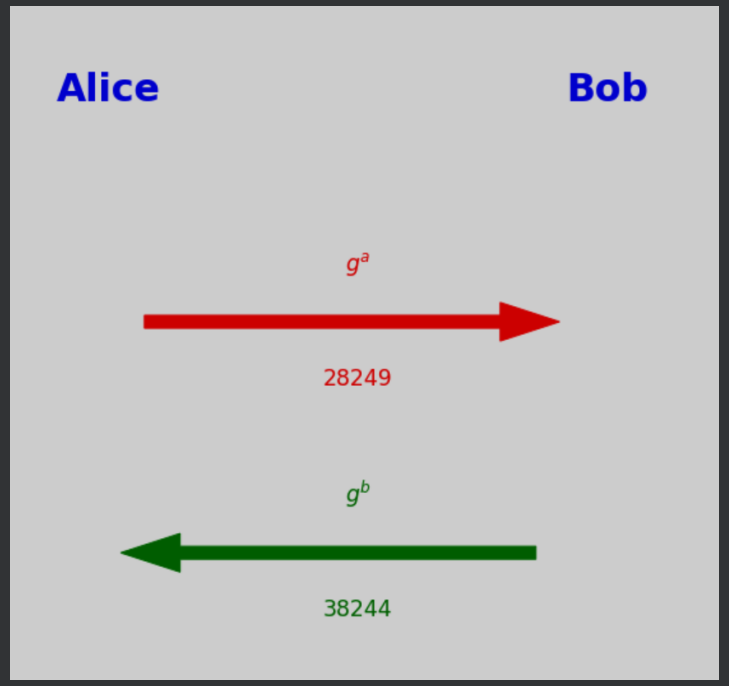
Экспоненциальный рост

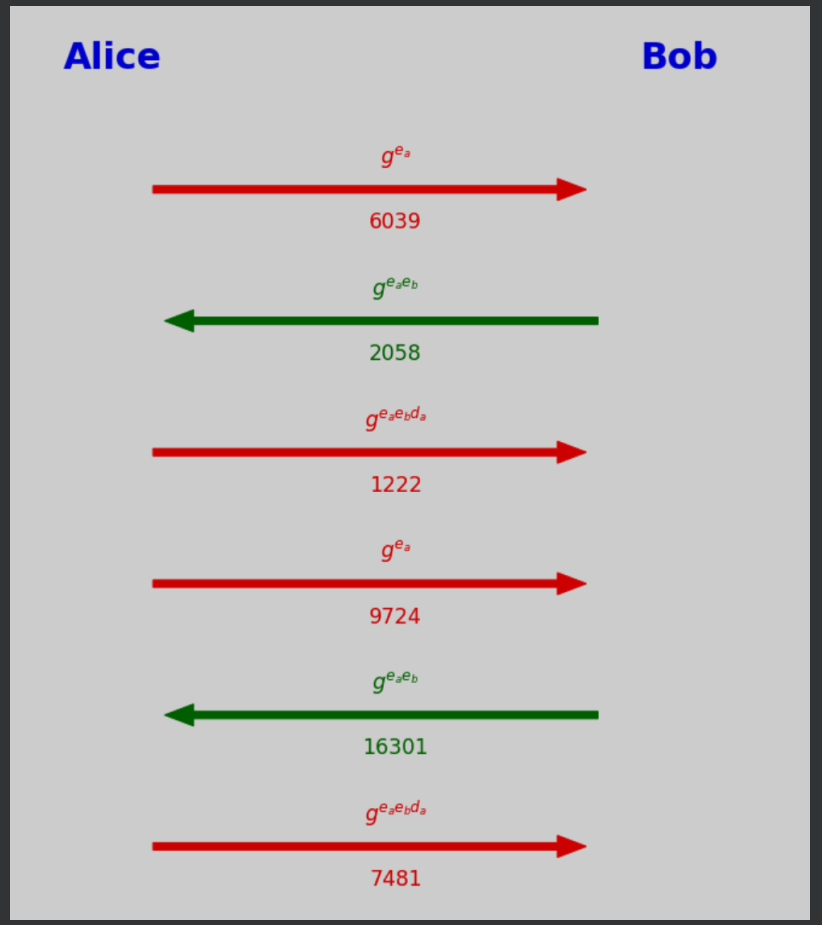
Протокол Диффи-Хеллмана, криптосистема Месси-Омуры, схема Эль-Гамаля

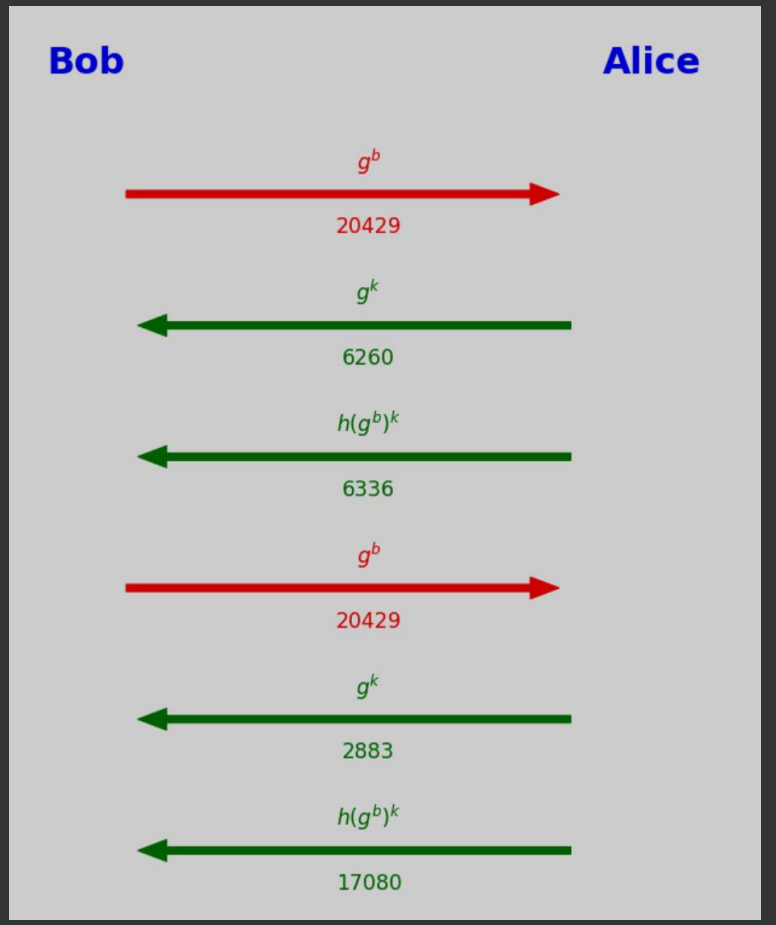
- В данном блоке студентам предложено реализовать криптосистемы, основанные на вычислительной сложности дискретного логарифма.
- То есть, передать элемент a по открытому каналу опасно, но передать g^a достаточно надёжно
- Общая схема вызова функций из блока:

```
alice, bob = Person('Alice'), Person('Bob')
log = diffie_hellman(alice, bob)
visualize(log)
```

Протокол Диффи-Хеллмана, криптосистема Месси-Омуры, схема Эль-Гамаля



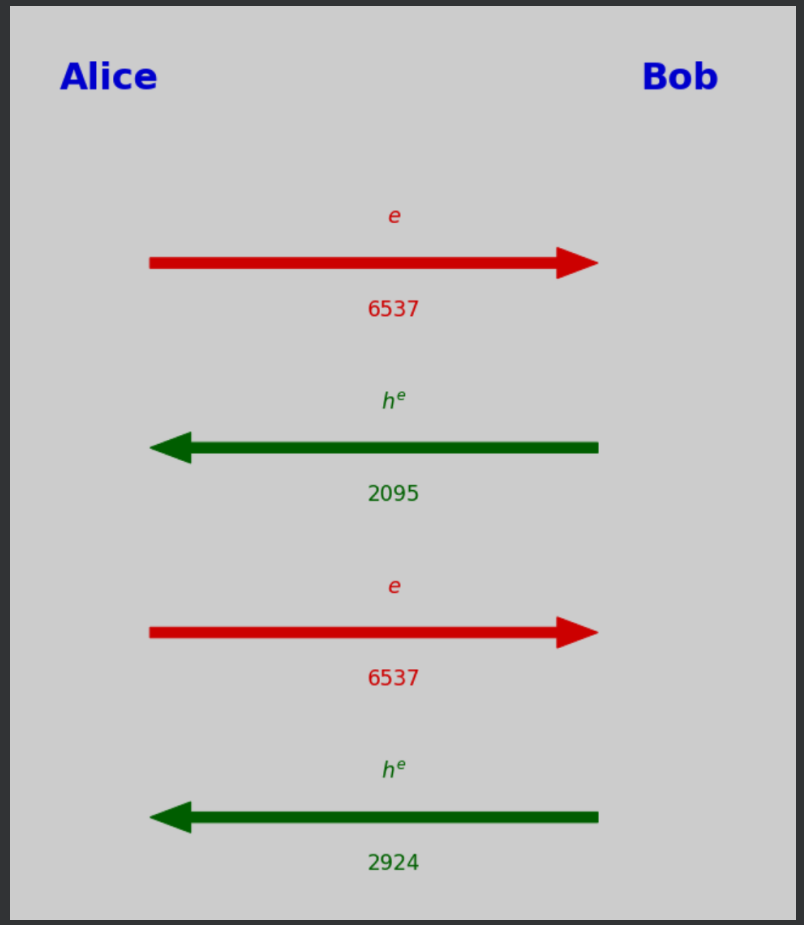




 # Также студенты получают сообщения success при правильной передаче информации

Криптосистема RSA

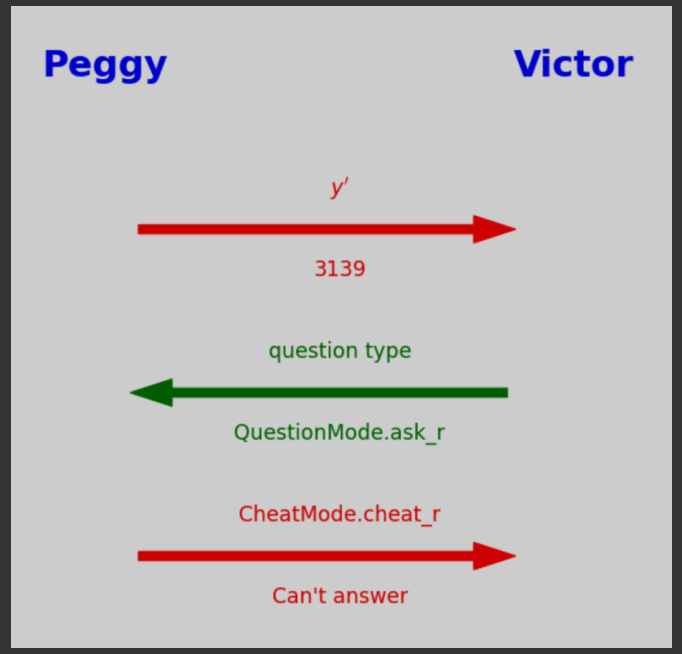
- В данном блоке необходимо написать криптосистему RSA, которая основана на вычислительной сложности факторизации больших чисел



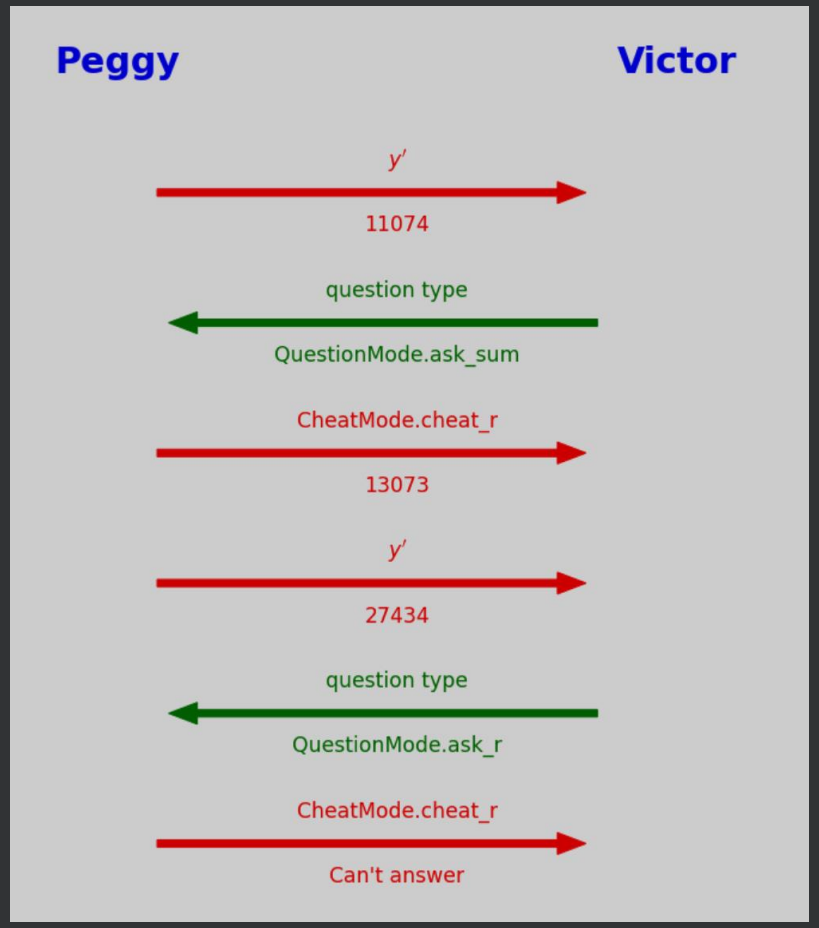
Протоколы с нулевым разглашением

- Приведён пример протокола взаимодействия между Пегги и Виктором
- Задание для студентов:
  - доказать, что протокол является протоколом с нулевым разглашением
  - описать, как Пегги может обманывать Виктора
  - реализовать в коде общение Пегги и Виктора

Протоколы с нулевым разглашением



У Пегги не удалось обмануть Виктора ни разу



Пегги удалось обмануть Виктора только один раз

Диск Альберти

class Disk - 100+ строк кода

-Заготовленные методы:

- match(inner_letter, outer_letter)
- turn_by_N_letters(N)
- get_inner_by_outer(outer_letter)
- get_outer_by_inner(inner_letter)
- animate()

Диск Альберти

class Disk - 100+ строк кода

-Необходимо реализовать:

- encrypt_mode1(s)
- decrypt_mode1(x)
- encrypt_mode2(s)
- encrypt_mode1(x)

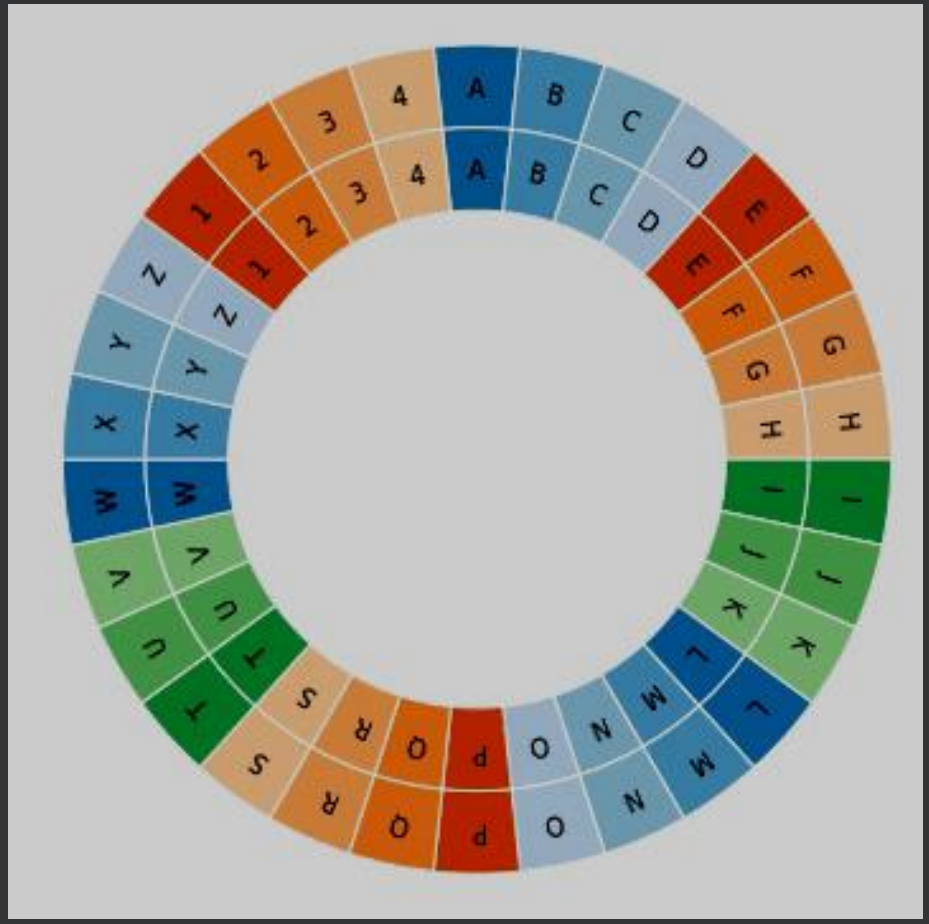
Диск Альберти, 1 режим

Input:

```
d = Disk()
x = 'RSA'
s = d.encrypt_mode1(x.upper())
print(s)
d.reset()
s = d.decrypt_mode1(s)
print(s)
d.reset()
d.animate()
```

Output:

```
RR3
RSA
```



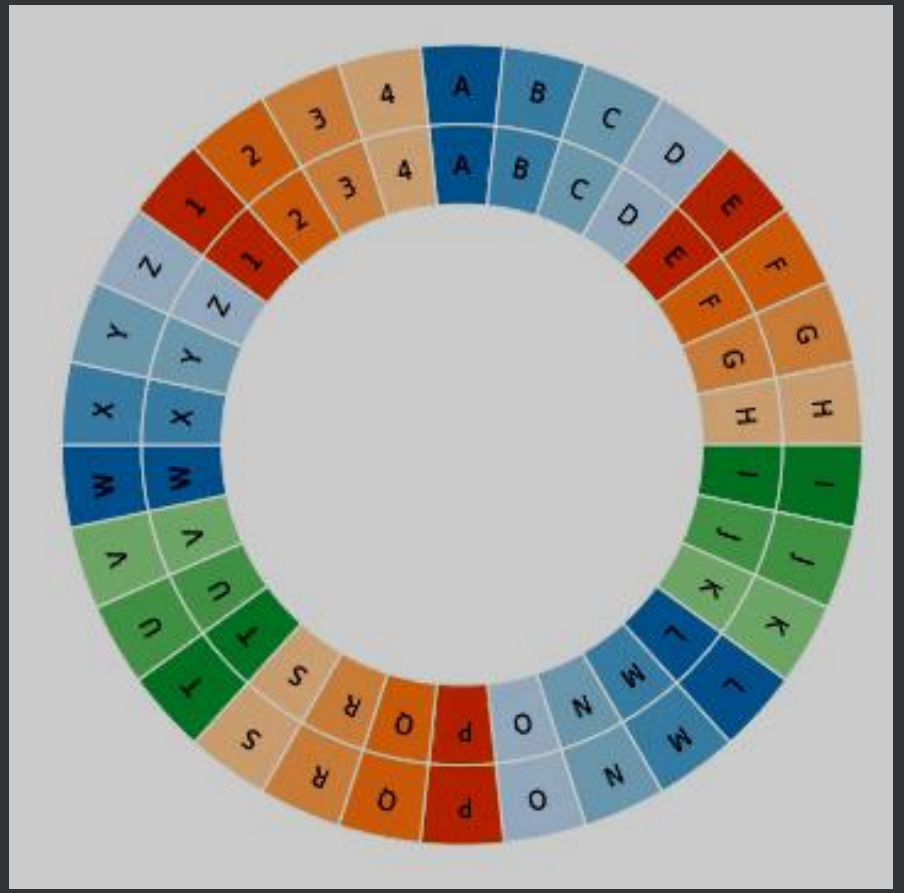
Диск Альберти, 2 режим

Input:

```
d = Disk()
x, password = 'NFT', 'Z1X'
s = d.encrypt_mode2(x.upper(),
password)
print(s)
d.reset()
s = d.decrypt_mode2(s, password)
print(s)
d.reset()
d.animate()
```

Output:

```
IBM
NFT
```



Частотный анализ

-По заданному шифротексту необходимо произвести частотный анализ и декодировать текст, закодированный с помощью шифра Цезаря

$тисдкия$жйхстђ0$ж$ыдх$сйеяждп
т$кдфотзт$лдодцд0$ж$ртхожй0$сд
$удцфмдфьмщ$уфчидщ0$утґжмпмхѐ$
ижд$зфдкидсмсд2$уйфжян$мл$смщ0
$тийцян$ж$пйцсђђ$хйфйсѐочђ$удф
ч0$еяп$рдпйсѐотзт$фтхцд0$чумцд
с0$пях0$хжтђ$уфмпмысчђ$ьпґуч$у
мфткотр$сйх$ж$фчой0$д$сд$щтфть
т$жяефмцтр$пмъй$йзт$утрйэдпмхѐ
$хжйфщюйхцйхцжйссящ$фдлрйфтж$т
ыом$ж$ыйфстн$фтзтжтн$туфджй2$ж
цтфтн$_$упйымхцян0$

Буква	Частота
space	0.174
о	0.090
е	0.072
а	0.062
и	0.062
н	0.053
т	0.053
с	0.045
р	0.040
в	0.038
л	0.035
к	0.028
м	0.026
д	0.025
п	0.023
у	0.021
я	0.018
з	0.016
...	...

[4, 4, 4, 4, 4, 4, 4, 4, -1, 18,
-5, 4, -1036, 19, 1, 0, -23, 4]

Частотный анализ

-По заданному шифротексту необходимо произвести частотный анализ и декодировать текст, закодированный с помощью шифра Цезаря

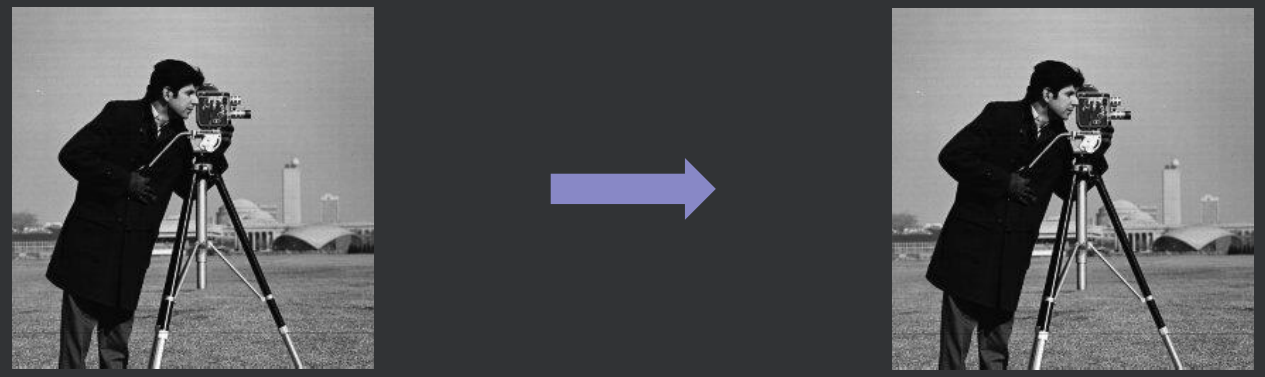
[4, 4, 4, 4, 4, 4, 4, 4, -1, 18,
-5, 4, -1036, 19, 1, 0, -23, 4]

Сдвиг +4

Однажды весною, в час небывало жаркого заката, в Москве, на Патриарших прудах, появились два гражданина. Первый из них, одетый в летнюю серенькую пару, был маленького роста, упитан, лыс, свою приличную шляпу пирожком нес в руке, а на хорошо выбритом лице его помещались сверхъестественных размеров очки в черной роговой оправе. Второй - плечистый, рыжеватый, вихрастый молодой человек в заломленной на затылок клетчатой кепке

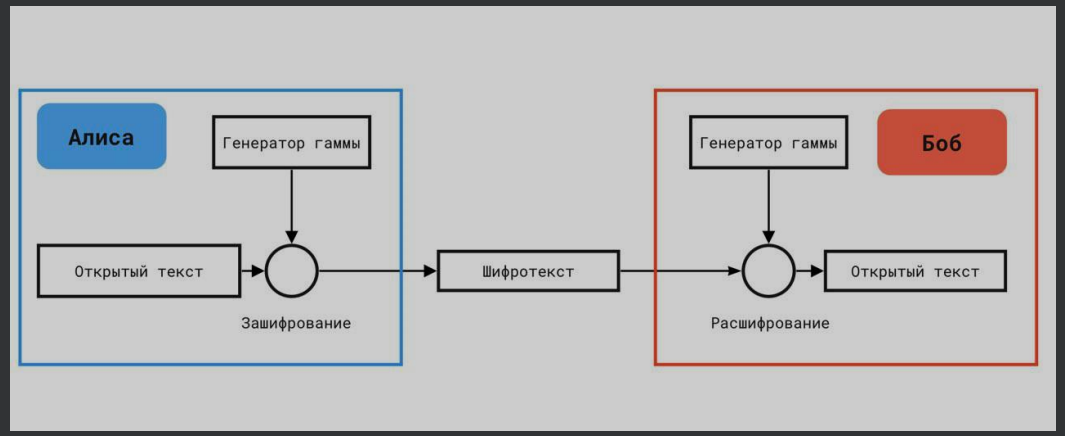
Хэширование

- Студентам предложено:
  - Вычислить хэш-функцию для заданного изображения
  - Изменить один бит в исходном изображении
  - Снова посчитать хэш-функцию
  - Удостоверится в том, что незаметное для человеческого глаза изменение полностью меняет значение хэша



Потоковое шифрование

- Студентам предложено:
  - Написать свой простой генератор псевдослучайных чисел
  - С помощью ранее реализованного Диффи-Хеллмана обменятся ключами
  - Запустить потоковый обмен данным с помощью общих гамма-ключей, которые генерирует ГПСЧ



Отзыв руководителя

Критерии оценки	Оценка научного руководителя (по 10-балльной шкале)
Четкость и корректность формулировки целей и задач работы	10
Полнота использования источников информации (книги, статьи, электронная библиотека НИУ ВШЭ, интернет-ресурсы и пр.)	10
Сложность и/или объемность проведенного исследования / теоретической составляющей работы	10
Сложность и/или объемность программной реализации / предложенных технологических решений	10
Достижение намеченной цели и поставленных задач работы	10
Оформление отчета	10

Проект в цифрах

- 10 итоговая оценка от руководителя за проект
- 7 блоков с заданиями и теорией
- 3 механизма визуализации
- 10+ библиотек Python
- 4 заинтересованные образовательные программы
- 1100 строчки кода и теории