Правительство Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ

О ПРАКТИЧЕСКОЙ РАБОТЕ № 7

по дисциплине «Криптографические методы защиты информации»

Криптосистемы с открытым ключом

|  |
| --- |
| Студент гр. \_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия  «\_\_\_» \_\_\_\_\_\_\_\_\_ 2025 г. |
| Руководитель  Заведующий кафедрой информационной безопасности киберфизических систем  канд. техн. наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_О.О. Евсютин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2025 г. |

Москва 2025

**СОДЕРЖАНИЕ**

[1 Задание на практическую работу 3](#_Toc155608317)

[2 Название раздела 4](#_Toc155608318)

[2.1 Название подраздела 4](#_Toc155608319)

[X Выводы о проделанной работе 5](#_Toc155608320)

[X Список использованных источников 6](#_Toc155608321)

[ПРИЛОЖЕНИЕ А. Основные требования к оформлению отчета 7](#_Toc155608322)

[ПРИЛОЖЕНИЕ Б. Пример списка использованных источников 12](#_Toc155608323)

# Задание на практическую работу

Целью работы является написать программную реализацию одной из перечисленных ниже асимметричных криптосистем (по выбору студента) с использованием больших чисел. Программная реализация должна быть выполнена студентом самостоятельно без использования готовых библиотечных функций, напрямую реализующих алгоритм шифрования. Варианты криптосистем для реализации:

- RSA;

- Рабина;

- Эль-Гамаля;

В рамках практической работы необходимо выполнить следующее:

реализация программы криптосистемы RSA на языке Python

# Теоретическая часть

## Криптография с открытым ключом

Основной проблемой симметричной криптографии является обеспечение конфиденциальности ключей шифрования при их распределении между пользователями. С данной проблемой сталкиваются все симметричные криптосистемы. Стороны–участники защищенного информационного обмена по открытому каналу связи должны каким-то образом предварительно получить общий секретный ключ, который нельзя передавать в открытом виде. Кроме того, необходимо обеспечить эффективное управление сеансовыми ключами, безопасное хранение долговременных ключей и т. д. Все перечисленные проблемы настолько важны, что в современной криптографии управление ключами выделяют в отдельный раздел.

Для решения проблемы обеспечения конфиденциальности ключей симметричного шифрования в 1976 году была предложена концепция криптографии с открытым ключом.

Криптосистемы с открытым ключом, также называемые асимметричными криптосистемами, используют два разных ключа: открытый ключ зашифрования и закрытый ключ расшифрования. Открытый ключ в общем случае доступен всем желающим, а закрытый ключ известен только законному владельцу. Оба ключа связаны между собой некоторой зависимостью. При этом данная зависимость такова, что, зная один ключ, вычислить другой практически невозможно.

Решение указанной проблемы заключается в том, что отсутствует необходимость в передаче секретной ключевой информации между пользователями. Закрытый ключ должен быть известен лишь его владельцу и не требует передачи.

Базовым понятием в криптографии с открытым ключом является понятие однонаправленной или односторонней функции. Значение такой функции для заданного аргумента достаточно легко вычислить, но практически невозможно вычислить значение аргумента для заданного значения функции. Непосредственно для шифрования однонаправленные функции не используются. Для шифрования применяются однонаправленные функции с лазейкой (ловушкой). Для такой функции вычислить обратную функцию достаточно просто, если известна некоторая секретная информация, и практически невозможно, если эта информация неизвестна.

В асимметричных криптосистемах, построенных на однонаправленных функциях с лазейкой, открытый ключ определяет конкретную реализацию функции, а закрытый ключ дает информацию о лазейке. Основными задачами, приводящими к однонаправленным функциям, являются задачи разложения на множители и дискретного логарифмирования в конечном поле.

## Криптосистемы с открытым ключом RSA

Данная криптосистема является первой криптосистемой с открытым ключом. Она основывается на сложности проблемы факторизации целых чисел, то есть разложения целых чисел на простые множители.

*Алгоритм генерации ключей.*

1. Пользователь *A* генерирует два больших простых числа и , отличных друг от друга. При этом – большое число, хотя и имеют приблизительно одинаковый битовый размер.

2. Держа и в секрете, Пользователь *A* вычисляет их произведение , которое называют модулем алгоритма.

3. Пользователь *A* вычисляет значение функции Эйлера для по формуле  
.

4. Пользователь *A* выбирает целое число , взаимно простое со значением функции . Это число называется экспонентой зашифрования.

5. Пользователь *A* применяет расширенный алгоритм Евклида к паре чисел и и вычисляет значение , удовлетворяющее соотношению. Это значение называется экспонентой расшифрования.

6. Пара публикуется в качестве открытого ключа пользователя *A*, является закрытым ключом и держится в секрете.

*Алгоритм зашифрования.*

1. Пользователь *B* получает аутентичную копию открытого ключа пользователя *A* – пару .

2. Пользователь *B* представляет сообщение в виде числа , меньшего модуля алгоритма. В общем случае сообщение может быть разбито на блоки, каждый из которых представляется своим числом.

3. Пользователь *B* вычисляет .

4. Зашифрованное сообщение отправляется пользователю *A*.

*Алгоритм расшифрования.*

1. Пользователь *A* получает криптограмму от пользователя *B*.

2. Пользователь *A* вычисляет .

## Программный код и описание варианта криптосистемы RSA

## Описание

* язык: Python;
* функции генерация ключей, шифрование/расшифрование блока, обработка файла;
* особенности реализация без библиотек;
* generate\_keypair - генерирует пару ключей RSA: открытый (e, n) и закрытый (d, n);
* encrypt\_block / decrypt\_block - шифрование и расшифрование одного блока сообщения с использованием RSA;
* process\_file – читает файл и шифрует или расшифровывает его поблочно с использованием RSA, принимает на вход ключ (e, n) для шифрования или (d, n) для расшифрования.
* print\_help - выводит инструкцию по использованию программы.

## Код

Ссылка на код:

import os  
import sys  
import random  
import math  
from typing import Tuple, Optional  
  
def is\_prime(n: int, k: int = 5) -> bool:  
 *"""Проверяет, является ли число простым, используя тест Ферма.  
 Аргументы: n (int): число для проверки; k (int): количество итераций теста (по умолчанию 5).  
 Возвращает: bool: True, если число вероятно простое, False — если составное.  
 """* if n <= 1:  
 return False  
 if n == 2:  
 return True  
 if n % 2 == 0:  
 return False  
  
 # Проводим k итераций теста Ферма  
 for \_ in range(k):  
 a = random.randint(2, n - 2)  
 # Если a^(n-1) ≠ 1 mod n, то n составное  
 if pow(a, n - 1, n) != 1:  
 return False  
 return True  
  
def generate\_prime(bits: int) -> int:  
 *"""Генерирует случайное простое число заданной битовой длины.  
 Аргументы: bits (int): битовая длина числа.  
 Возвращает: int: случайное простое число.  
 """* # Определяем диапазон для чисел заданной длины  
 min\_val = 1 << (bits - 1) # 2^(bits-1)  
 max\_val = (1 << bits) - 1 # 2^bits - 1  
  
 while True:  
 n = random.randint(min\_val, max\_val)  
 # Убедимся, что число нечётное  
 if n % 2 == 0:  
 n += 1  
 if is\_prime(n):  
 return n  
  
def extended\_gcd(a: int, b: int) -> Tuple[int, int, int]:  
 *"""Реализует расширенный алгоритм Евклида для нахождения НОД и коэффициентов.  
 Аргументы: a (int): первое число; b (int): Второе число.  
 Возвращает: Tuple[int, int, int]: НОД(a, b) и коэффициенты x, y, такие что ax + by = НОД.  
 """* if a == 0:  
 return b, 0, 1  
 gcd, x1, y1 = extended\_gcd(b % a, a)  
 x = y1 - (b // a) \* x1  
 y = x1  
 return gcd, x, y  
  
def mod\_inverse(e: int, phi: int) -> Optional[int]:  
 *"""Находит мультипликативное обратное e по модулю phi.  
 Аргументы: e (int): число, для которого ищется обратное; phi (int): модуль (функция Эйлера).  
 Возвращает: Optional[int]: обратное число или None, если оно не существует.  
 """* gcd, x, \_ = extended\_gcd(e, phi)  
 if gcd != 1:  
 return None # e и phi не взаимно простые  
 return (x % phi + phi) % phi  
  
def generate\_keypair(bits: int = 512) -> Tuple[Tuple[int, int], Tuple[int, int]]:  
 *"""Генерирует пару ключей RSA: открытый (e, n) и закрытый (d, n).  
 Аргументы: bits (int): битовая длина модуля n (по умолчанию 512).  
 Возвращает: Tuple[Tuple[int, int], Tuple[int, int]]: открытый ключ (e, n) и закрытый ключ (d, n).  
 Обработка ошибок: ValueError - если не удалось сгенерировать ключи.  
 """* # Генерируем два простых числа p и q  
 p = generate\_prime(bits // 2)  
 q = generate\_prime(bits // 2)  
 while p == q:  
 q = generate\_prime(bits // 2)  
  
 # Вычисляем модуль n  
 n = p \* q  
  
 # Вычисляем функцию Эйлера phi(n)  
 phi = (p - 1) \* (q - 1)  
  
 # Выбираем открытую экспоненту e  
 e = 65537 # Популярное значение, простое и эффективное  
 if math.gcd(e, phi) != 1:  
 # Если e не взаимно простое с phi, пробуем другое  
 for possible\_e in range(3, phi, 2):  
 if math.gcd(possible\_e, phi) == 1:  
 e = possible\_e  
 break  
 else:  
 raise ValueError("Не удалось найти подходящую открытую экспоненту")  
  
 # Находим закрытую экспоненту d  
 d = mod\_inverse(e, phi)  
 if d is None:  
 raise ValueError("Не удалось вычислить закрытую экспоненту")  
  
 return (e, n), (d, n)  
  
def add\_padding(data: bytes, block\_size: int) -> bytes:  
 *"""Добавляет PKCS#5/PKCS#7 дополнение к данным для кратности блока.  
 Аргументы: data (bytes): исходные данные; block\_size (int): размер блока в байтах.  
 Возвращает: bytes: данные с дополнением.  
 """* padding\_length = block\_size - (len(data) % block\_size)  
 padding = bytes([padding\_length] \* padding\_length)  
 return data + padding  
  
def remove\_padding(data: bytes) -> bytes:  
 *"""Удаляет PKCS#5/PKCS#7 дополнение из данных.  
 Аргументы: data (bytes): данные с дополнением.  
 Возвращает: bytes: данные без дополнения.  
  
 Raises:  
 ValueError: Если дополнение некорректно.  
 """* if not data:  
 return data  
 padding\_length = data[-1]  
 if padding\_length > len(data) or padding\_length == 0:  
 raise ValueError("Некорректное дополнение")  
 if not all(b == padding\_length for b in data[-padding\_length:]):  
 raise ValueError("Некорректное дополнение")  
 return data[:-padding\_length]  
  
def encrypt\_block(message: int, e: int, n: int) -> int:  
 *"""Шифрует один блок сообщения с использованием RSA.  
 Аргументы:  
 message (int): число, представляющее блок сообщения (меньше n).  
 e (int): открытая экспонента.  
 n (int): модуль.  
 Возвращает: int: зашифрованное число.  
 Обработка ошибок: ValueError - если message >= n.  
 """* if message >= n:  
 raise ValueError("Сообщение должно быть меньше модуля n")  
 # c = m^e mod n  
 return pow(message, e, n)  
  
def decrypt\_block(ciphertext: int, d: int, n: int) -> int:  
 *"""Расшифровывает один блок шифртекста с использованием RSA.  
 Аргументы:  
 ciphertext (int): число, представляющее блок шифртекста.  
 d (int): акрытая экспонента.  
 n (int): модуль.  
 Возвращает: int: расшифрованное число.  
 Обработка ошибок: ValueError - если ciphertext >= n.  
 """* if ciphertext >= n:  
 raise ValueError("Шифртекст должен быть меньше модуля n")  
 # m = c^d mod n  
 return pow(ciphertext, d, n)  
  
def process\_file(input\_file: str, output\_file: str, key: Tuple[int, int], mode: str = "encrypt") -> None:  
 *"""Обрабатывает файл: шифрует или расшифровывает его поблочно с использованием RSA.  
 Аргументы:  
 input\_file (str): путь к входному файлу.  
 output\_file (str): путь к выходному файлу.  
 key (Tuple[int, int]): ключ (e, n) для шифрования или (d, n) для расшифрования.  
 mode (str): режим работы ('encrypt' или 'decrypt').  
 Обработка ошибок:  
 FileNotFoundError: если входной файл не найден.  
 ValueError: если ключ или данные некорректны.  
 """* exp, n = key  
 # Определяем размер блока в байтах (чтобы число помещалось в n)  
 block\_size = (n.bit\_length() // 8) - 1 # Минус 1 байт для безопасности  
  
 with open(input\_file, 'rb') as f\_in:  
 data = f\_in.read()  
 result = b""  
  
 if mode == "encrypt":  
 # Добавляем дополнение для шифрования  
 data = add\_padding(data, block\_size)  
 # Шифруем поблочно  
 for i in range(0, len(data), block\_size):  
 block = data[i:i + block\_size]  
 # Преобразуем блок в число  
 m = int.from\_bytes(block, 'big')  
 c = encrypt\_block(m, exp, n)  
 # Преобразуем шифртекст в байты  
 c\_bytes = c.to\_bytes((n.bit\_length() + 7) // 8, 'big')  
 result += c\_bytes  
 else: # mode == "decrypt"  
 # Читаем поблочно, размер блока равен длине n в байтах  
 cipher\_block\_size = (n.bit\_length() + 7) // 8  
 if len(data) % cipher\_block\_size != 0:  
 raise ValueError("Размер входного файла для расшифровки должен быть кратен размеру блока")  
 temp\_result = b""  
 for i in range(0, len(data), cipher\_block\_size):  
 block = data[i:i + cipher\_block\_size]  
 # Преобразуем блок в число  
 c = int.from\_bytes(block, 'big')  
 m = decrypt\_block(c, exp, n)  
 # Преобразуем расшифрованное число в байты  
 m\_bytes = m.to\_bytes(block\_size, 'big')  
 temp\_result += m\_bytes  
 # Удаляем дополнение после расшифровки  
 result = remove\_padding(temp\_result)  
  
 with open(output\_file, 'wb') as f\_out:  
 f\_out.write(result)  
  
def print\_help() -> None:  
 *"""Выводит инструкцию по использованию программы."""* print("Программа шифрования/расшифрования с использованием криптосистемы RSA")  
 print("-----------------------------------------------------------")  
 print("Эта программа реализует асимметричную криптосистему RSA.")  
 print("Шифрование и расшифрование выполняются с использованием открытого (e, n) и закрытого (d, n) ключей.")  
 print("\nИспользование: python3 rsa\_cipher.py [параметры]")  
 print("Параметры:")  
 print(" -h Показать эту справку и выйти")  
 print("\nИнтерактивный режим:")  
 print("1. Запустите программу без параметров: python3 rsa\_cipher.py")  
 print("2. Выберите действие:")  
 print(" - 'generate' для генерации новой ключевой пары.")  
 print(" - 'encrypt' для шифрования файла.")  
 print(" - 'decrypt' для расшифрования файла.")  
 print("3. Следуйте инструкциям на экране:")  
 print(" - Для генерации: укажите битовую длину ключей (например, 512).")  
 print(" - Для шифрования/расшифрования:")  
 print(" - Укажите путь к входному файлу.")  
 print(" - Укажите путь к выходному файлу.")  
 print(" - Введите ключ (e и n для шифрования, d и n для расшифрования).")  
 print("\nПример ключей:")  
 print(" Открытый ключ: e=65537, n=12345678901234567890")  
 print(" Закрытый ключ: d=98765432109876543210, n=12345678901234567890")  
 print("\nПример использования:")  
 print("1. Генерация ключей:")  
 print(" - Действие: generate")  
 print(" - Битовая длина: 512")  
 print("2. Шифрование файла plaintext.txt в encrypted.bin:")  
 print(" - Действие: encrypt")  
 print(" - Входной файл: plaintext.txt")  
 print(" - Выходной файл: encrypted.bin")  
 print(" - Ключ: e=65537, n=12345678901234567890")  
 print("3. Расшифрование файла encrypted.bin в decrypted.txt:")  
 print(" - Действие: decrypt")  
 print(" - Входной файл: encrypted.bin")  
 print(" - Выходной файл: decrypted.txt")  
 print(" - Ключ: d=98765432109876543210, n=12345678901234567890")  
 print("\nПримечания:")  
 print("- Входной файл для шифрования может быть текстовым (UTF-8) или бинарным.")  
 print("- Для расшифровки используйте тот же модуль n, что при шифровании.")  
 print("- Ключи вводятся как два числа через пробел (например, '65537 12345678901234567890').")  
 print("- Результат шифрования — бинарные данные, не открывайте их как текст.")  
  
def main() -> None:  
 *"""Основная функция программы: обрабатывает параметры командной строки и запускает обработку."""* if len(sys.argv) > 1 and sys.argv[1] == "-h":  
 print\_help()  
 sys.exit(0)  
  
 print("Программа шифрования/расшифрования с использованием криптосистемы RSA")  
 print("-----------------------------------------------------------")  
  
 while True:  
 action = input("Выберите действие (generate/encrypt/decrypt): ").strip().lower()  
 if action in ["generate", "encrypt", "decrypt"]:  
 break  
 print("Ошибка: введите 'generate', 'encrypt' или 'decrypt'")  
  
 if action == "generate":  
 while True:  
 try:  
 bits = int(input("Введите битовую длину ключей (например, 512): ").strip())  
 if bits < 64:  
 print("Ошибка: битовая длина должна быть не менее 64")  
 continue  
 break  
 except ValueError:  
 print("Ошибка: введите целое число")  
 try:  
 public\_key, private\_key = generate\_keypair(bits)  
 print(f"Открытый ключ: e={public\_key[0]}, n={public\_key[1]}")  
 print(f"Закрытый ключ: d={private\_key[0]}, n={private\_key[1]}")  
 except Exception as e:  
 print(f"Ошибка при генерации ключей: {e}")  
 return  
  
 while True:  
 input\_file = input("Введите путь к входному файлу: ").strip()  
 if os.path.exists(input\_file):  
 break  
 print("Ошибка: файл не найден")  
  
 output\_file = input("Введите путь к выходному файлу: ").strip()  
  
 while True:  
 key\_input = input(f"Введите ключ ({'e n' if action == 'encrypt' else 'd n'}): ").strip()  
 try:  
 exp, n = map(int, key\_input.split())  
 if exp <= 0 or n <= 0:  
 raise ValueError("Ключи должны быть положительными числами")  
 break  
 except ValueError:  
 print("Ошибка: введите два числа через пробел (например, '65537 12345678901234567890')")  
  
 try:  
 process\_file(input\_file, output\_file, (exp, n), action)  
 print(f"Операция завершена! Результат сохранён в {output\_file}")  
 if action == "decrypt":  
 with open(output\_file, 'rb') as f:  
 decrypted\_data = f.read()  
 try:  
 decrypted\_text = decrypted\_data.decode('utf-8')  
 print(f"Расшифрованный текст: {decrypted\_text}")  
 except UnicodeDecodeError:  
 print("Результат не является текстом в кодировке UTF-8")  
 except Exception as e:  
 print(f"Произошла ошибка: {e}")  
  
# запуск  
if \_\_name\_\_ == "\_\_main\_\_":  
 main()

## Запуск

Сохранить код в файл, например <script>.py.

Запустить в терминале: python <script>.py.

Дополнительные инструкции:

* generate - генерация ключей, если пользователь не может сам предоставить ключи
* выбрать encrypt или decrypt;
* указать путь к файлу (например, plaintext.txt);
* указать имя выходного файла (например, encrypted.bin);
* предоставить ключ, например (2048 битный):

*Открытый ключ: e=65537, n=20550052083448917747637528851060681894491668833317099787075539249786242111300001572214832735775672252544567845197630828253961601227397210317954130166112013988531220202513714738620183649029238006670786314084427362301508078235214439206613697012423886086397750138904800570101364651768702438201340296418202278329727967514465481009564791443238873107136733212734411763915813542424957443510514489562843268025062159580225469258442193767639683550807412564748207328022079498432835197427361463497704340552190606945901459773537174283090128721384765490030497091167175743769032367060168825739244178512672899730836826626830414306879*

*Закрытый ключ: d=18829839291746508989782584571082670986559030854471903799589136022230398477587872414255655898440039892542439288828645328096779652948814103129582731443386065154420988210951845274713225327797347628646221049896759807949217413157496716187746755562400884742577037300934924989473992534039738622708221098619245083173798306952680590532345017234378512285807728119360008940602400755877540611254129977433030762018451849071720853291044288479133117789370431528048275085741283552625710985059227862819799275465547912902934137101550941657275486987920119674259639215773884221769583297762935588791125270521374908409851312752322695655553, n=20550052083448917747637528851060681894491668833317099787075539249786242111300001572214832735775672252544567845197630828253961601227397210317954130166112013988531220202513714738620183649029238006670786314084427362301508078235214439206613697012423886086397750138904800570101364651768702438201340296418202278329727967514465481009564791443238873107136733212734411763915813542424957443510514489562843268025062159580225469258442193767639683550807412564748207328022079498432835197427361463497704340552190606945901459773537174283090128721384765490030497091167175743769032367060168825739244178512672899730836826626830414306879*

## Пример работы

Пример вывода результата работы программы «Криптосистема RSA»:

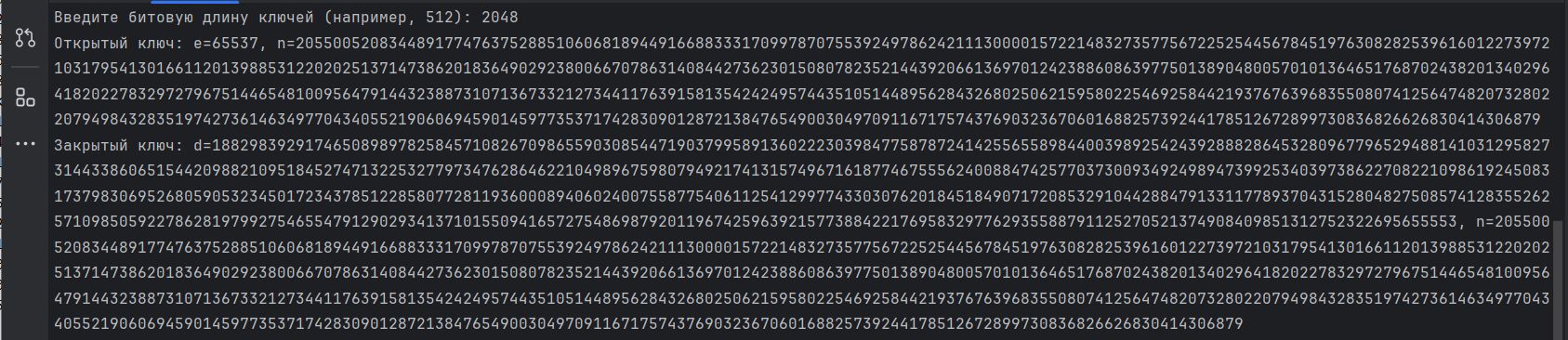


Рисунок 1 – Пример работы программы «Криптосистема RSA» - generate

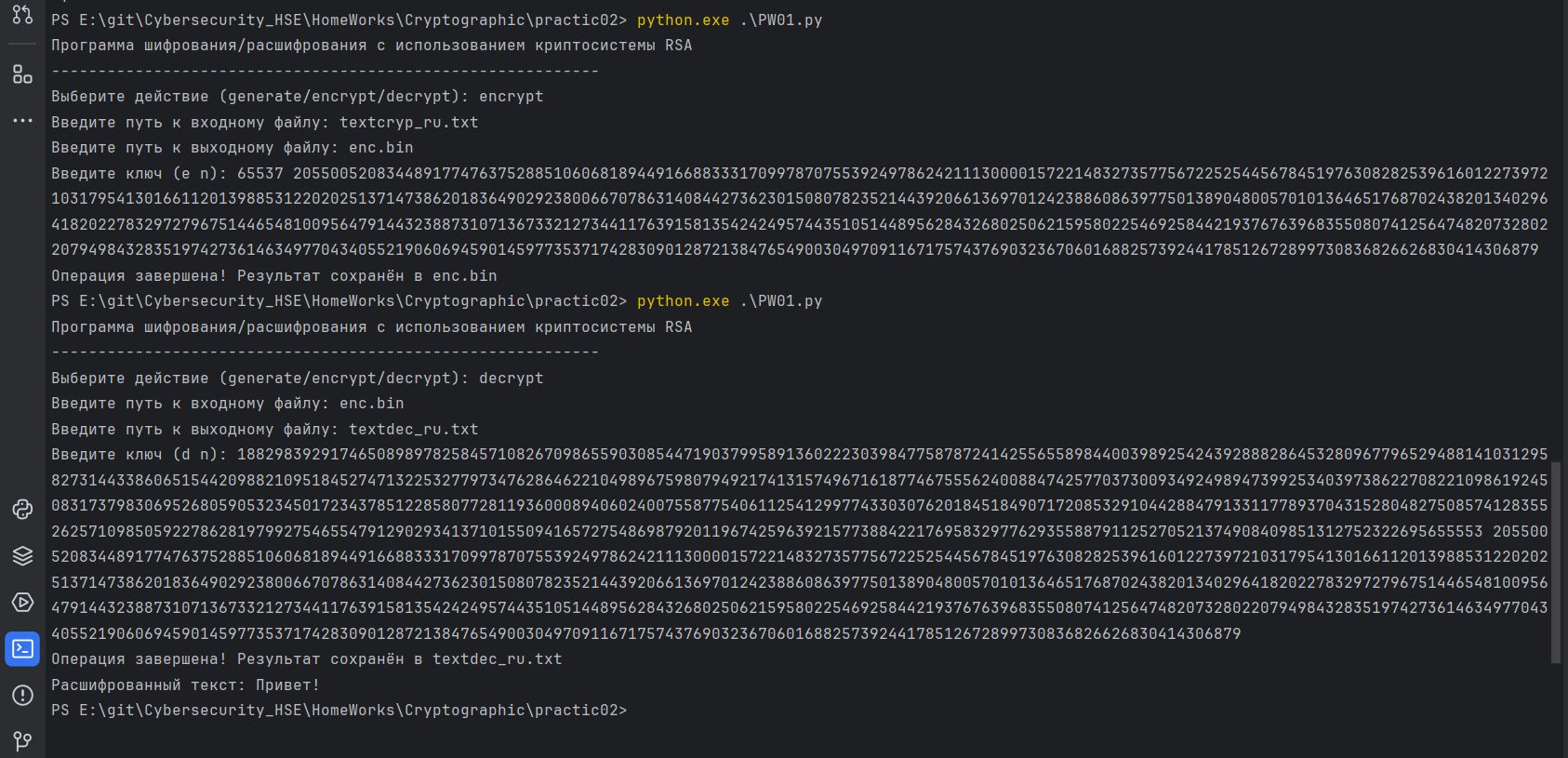


Рисунок 2 – Пример работы программы «Криптосистема RSA» - encrypt и decrypt

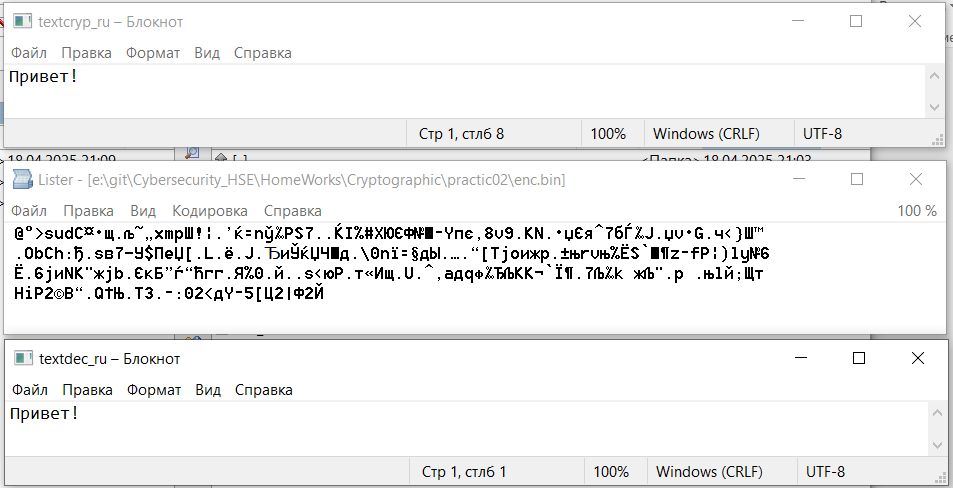


Рисунок 3 – Пример файлов: textcryp\_ru (исходное сообщение), enc.bin (зашифрованное сообщение, textdec\_ru (расшифрованное сообщение)

# X Список использованных источников

Список библиографических ссылок, оформленных по ГОСТ (примеры приведены в приложении А).

# ПРИЛОЖЕНИЕ А. Основные требования к оформлению отчета

**А.1 Общие требования к оформлению отчета**

Шрифт: единый, рекомендуемый – Times New Roman,

Цвет: черный,

Размер: не менее 12 пт., одинаковый по всему отчету,

Выравнивание текста – по ширине,

Межстрочный интервал – полуторный (исключения: оформление титула, должностей в списке исполнителей, названий рисунков и таблиц),

Абзацный отступ – 1,25 см.,

Отступы и интервалы в тексте – 0 см.

Полужирный шрифт**:** применяют только для заголовков структурных элементов отчета,для заголовков разделов и подразделов основной части отчета.

Курсив:допускается для обозначения объектов и написания терминов. Курсив также может использоваться для *акцентирования внимания, выделения текста в отчете*, но при этом текст должен быть *того же кегля и гарнитуры*. Разрешается для написания определенных терминов, формул, теорем применять шрифты разной гарнитуры.

Размеры полей:левое – 3,0 см., правое – 1,5 см., верхнее и нижнее – 2,0 см.

Номера страниц– арабскими цифрами, *внизу по центру***.** Титульный листвключают в общую нумерацию страниц отчета. *Номер* страницы на титульном листе *не проставляют*. *Приложения* должны иметь общую с остальной частью отчета сквозную нумерацию страниц.

Оформление перечислений**:** перед каждым элементом перечисления следует ставить *тире* или, при необходимости ссылки в тексте отчета на один из элементов перечисления, вместо тире ставят *строчные буквы,* начиная с буквы "а" (за исключением – е, з, й, о, ч, ъ, ы, ь), после которой ставится скобка. Простые перечисления отделяются запятой, сложные – точкой с запятой.

*НЕ*допускается использование *данных**знаков*:



При наличии конкретного числа перечислений допускается использовать *арабские*

*цифры* со скобками.

Перечисления приводятся с абзацного отступа – 1,25 пт., без отступов слева и выступов справа.

**А.2 Оформление иллюстраций**

К иллюстрациям относятся: чертежи, графики, схемы, диаграммы, фотоснимки.

Иллюстрации следует располагать в отчете *непосредственно после текста отчета*, где они упоминаются впервые, или на следующей странице (по возможности ближе к соответствующим частям текста отчета).

На все иллюстрации в отчете должны быть даны ссылки. При ссылке необходимо писать слово "рисунок" и его номер, например: "в соответствии с рисунком 2". *Не допускается*сокращение типа *Рис.5.*

Иллюстрации, за исключением иллюстраций, приведенных в приложениях, следует нумеровать арабскими цифрами сквозной нумерацией: Рисунок 1.

Допускается нумеровать иллюстрации в пределах раздела отчета. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой: Рисунок 1.1.

Если рисунок в отчете всего один, то он обозначатся: Рисунок 1.

Иллюстрации при необходимости могут иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок", его номер и через тире наименование помещают после пояснительных данных и располагают в центре под рисунком.

Пример оформления названия рисунка:

Рисунок 1.1 – Если наименование рисунка состоит из нескольких строк, то его записывают через один межстрочный интервал. Наименование рисунка приводят с прописной буквы без точки в конце. Перенос слов в наименовании рисунка не допускается

**А.3 Оформление таблиц**

Таблицу следует располагать непосредственно после текста, в котором она упоминается впервые, или на следующей странице.

На все таблицы в отчете должны быть ссылки. При ссылке следует печатать слово "таблица" с указанием ее номера***.*** *Не допускается сокращение – Табл*.5.

Допускается применять размер шрифта в таблице меньший, чем в тексте отчета.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Допускается нумеровать таблицы в пределах раздела при большом объеме отчета. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой: Таблица 2.3.

Наименование таблицы следует помещать над таблицей слева без абзацного отступа в одну строку с ее номером через тире, например,Таблица 1 – Наименование. Наименование таблицы приводят с прописной буквы без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через *один межстрочный интервал*.

Если таблица занимает больше двух страниц, то при переносе части таблицы на другую страницу пишут слова «Продолжение таблицы 1», пример оформления названия таблицы:

Таблица 1.1 – Наименование таблицы следует помещать над таблицей слева без абзацного отступа с прописной буквы в одну строку с ее номером через тире без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через один межстрочный интервал

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Продолжение таблицы 1.1

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**А.4 Оформление формул и уравнений**

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено *не менее одной свободной строки*. Если уравнение не умещается в одну строку, оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (–), умножения (×), деления (:) или других математических знаков. На новой строке знак повторяется.

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они представлены в формуле. Значение каждого символа и числового коэффициента необходимо приводить с новой строки. Первую строку пояснения начинают со слова "где" без двоеточия с абзаца.

Формулы в отчете следует располагать *посередине строки* и обозначать порядковой нумерацией в пределах всего отчета арабскими цифрами в круглых скобках в крайнем правом положении на строке. Одну формулу обозначают (1).

Ссылки в отчете на порядковые номера формул приводятся в скобках в формуле (1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой: (3.1)

Пример:

Для рядов данных *x, y* коэффициенты линейных зависимостей *a, b (y* = *a* + *bx)* рассчитываются, как решение системы уравнений (3.1):

|  |  |
| --- | --- |
| \begin{pmatrix}1&\bar{x}\\\bar{x}&\bar{x^2}\\\end{pmatrix}\begin{pmatrix}a\\b\\\end{pmatrix}=\begin{pmatrix}\bar{y}\\\overline{xy}\\\end{pmatrix}, | (3.1) |

где *x* – средние или максимальные значения температуры процессоров;

*y* – температуры на выходе бака;

, – среднее арифметическое значение элементов ряда.

**А.5 Оформление списка использованных источников**

Список должен содержать сведения об источниках, использованных при составлении отчета. Сведения об источниках приводятся в соответствии с требованиями ГОСТ 7.1, [ГОСТ 7.80](consultantplus://offline/ref=1664E79CF97BFD0858C3BB176F68BD1AE7E0C40EC8784F205FE14ABC80BBR0M), [ГОСТ 7.82](consultantplus://offline/ref=1664E79CF97BFD0858C3AD1B6D68BD1AEAEBC600CA2A18220EB444BBR9M) (пример приведен в Приложении Б).

Сведения об источниках следует располагать в порядке появления ссылок на источники в тексте отчета и нумеровать арабскими цифрами с точкой и печатать с абзацного отступа.

Список использованных источников должен включать библиографические записи на документы, использованные при составлении отчета, ссылки на которые оформляют арабскими цифрами в квадратных скобках [1], [3]–[10] в тексте отчета. На каждый источник в тексте отчета должна быть такая ссылка.

# ПРИЛОЖЕНИЕ Б. Пример списка использованных источников

1. DeRidder J.L. The immediate prospects for the application of ontologies in digital libraries// Knowledge Organization – 2007 . – Vol. 34, No. 4 . – P. 227 – 246 .

2. Прогноз научно-технологического развития Российской Федерации на период до 2030 года . – URL: http://government.ru/media/files/41d4b737638891da2184/pdf (дата обращения 15.11.2016).

3. U.S. National Library of Medicine. Fact sheet: UMLS Metathesaurus/National Institutes of Health, 2006 – 2013. – URL: http://www.nlm.nih.gov/pubs/factsheets/umlsmeta.html (дата обращения 2014-12-09).

4. U.S. National Library of Medicine. Fact sheet: Unfied Medical Language System/National Institutes of Health, 2006 – 2013. – URL: http://www.nlm.nih.gov/pubs/factsheets/umls.html (дата обращения 2009-12-09).

5. Антопольский А.Б., Белоозеров В.Н. Процедура формирования макротезауруса политематических информационных систем// Классификация и кодирование – 1976 . – N 1 (57). – С. 25 – 29 .

6. Белоозеров В.Н., Федосимов В.И. Место макротезауруса в лингвистическом обеспечении сети органов научно-технической информации// Проблемы информационных систем – 1986 . – N 1. – С. 6 – 10 .

7. Гуреев В.Н., Мазов Н.А. Использование библиометрии для оценки значимости журналов в научных библиотеках (обзор)// Научно-техническая информация. Сер. 1. – 2015 . – N 2. – С. 8 – 19 .

8. Земсков А.И., Шрайберг Я.Л. Электронные библиотеки: учебник для вузов. – М: Либерея, 2003 . – 351 с.

9. Костюк К.Н. Книга в новой медицинской среде. – М.: Директ-Медиа, 2015. – 430 с.

10. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. – URL: http://bookhamber.ru/stat\_2006.htm (дата обращения 12.03.2009).

11. Web of Science. – URL: http://apps.webofknowledge.com (дата обращения 15.11.2016).

12. Леготин Е.Ю. Организация метаданных в хранилище данных// Научный поиск. Технические науки: Материалы 3-й науч. конф. аспирантов и докторантов/отв. за вып. С.Д. Ваулин; Юж.-Урал. гос. ун-т. Т. 2. – Челябинск: Издательский центр ЮУрГУ , 2011 – С. 128 – 132 .

13. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. – 2006. – URL: http://bookhamber.ru/stat\_2006.htm (дата обращения 12.03.2009).

14. Приказ Минобразования РФ от 19 декабря 2013 г. N 1367 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры". – URL: http://www. consultant.ru/document/cons\_doc\_LAW\_159671 (дата обращения 04.08.2016).

15. ГОСТ 7.0.96-2016 Система стандартов по информации, библиотечному и издательскому делу. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М: Стандартинформ, 2016 . – 16 с.