**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ**

**ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ**

**им. проф. М.А. Бонч-Бруевича»**

**(СПбГУТ)**

**Санкт-Петербургский колледж телекоммуникаций**

**Отчет о выполнении  
практического занятия №29**

Выполнил: Обучающиеся 4 курса, 581 группы,

Филипович Валерий Анатольевич

Состав бригады: -

Проверил: преподаватель  
Баталов Дмитрий Иннокентьевич

Санкт-Петербург

2021 г.

**Постановка задачи**

Реализовать приложение для шифрования, позволяющее выполнять следующие действия (согласно варианту):

I. Реализовать приложение для шифрования, позволяющее выполнять следующие действия:

1. Шифровать данные в режиме однократного гаммирования:

1) шифруемый текст должен храниться в файле;

2) ключ шифрования должен задаваться случайным образом;

3) зашифрованный текст должен сохраняться в один файл, а использовавшийся при шифровании ключ – в другой;

4) в процессе шифрования предусмотреть возможность просмотра ключа, шифруемого и зашифрованного текстов в двоичном, шестнадцатиричном и символьном виде.

2. Шифровать данные при помощи каждого заданного в варианте скремблера:

1) шифруемый текст должен храниться в одном файле, начальное значение скремблера – в другом;

2) зашифрованный текст должен сохраняться в файл;

3) в процессе шифрования предусмотреть возможность просмотра начального значения скремблера, шифруемого и зашифрованного текстов в двоичном, шестнадцатиричном и символьном виде.

II. Реализовать приложение для дешифрования, позволяющее выполнять следующие действия:

1. Дешифровать данные в режиме однократного гаммирования:

1) зашифрованный текст должен храниться в одном файле, ключ – в другом;

2) расшифрованный текст должен сохраняться в файл;

3) в процессе дешифрования предусмотреть возможность просмотра ключа, зашифрованного и расшифрованного текстов в двоичном и символьном виде.

2. Расшифровать данные при помощи каждого заданного в варианте скремблера:

1) зашифрованный текст должен храниться в одном файле, начальное значение скремблера – в другом;

2) зашифрованный текст должен сохраняться в файл;

3) в процессе дешифрования предусмотреть возможность просмотра начального значения скремблера, зашифрованного и расшифрованного текстов в двоичном и символьном виде.

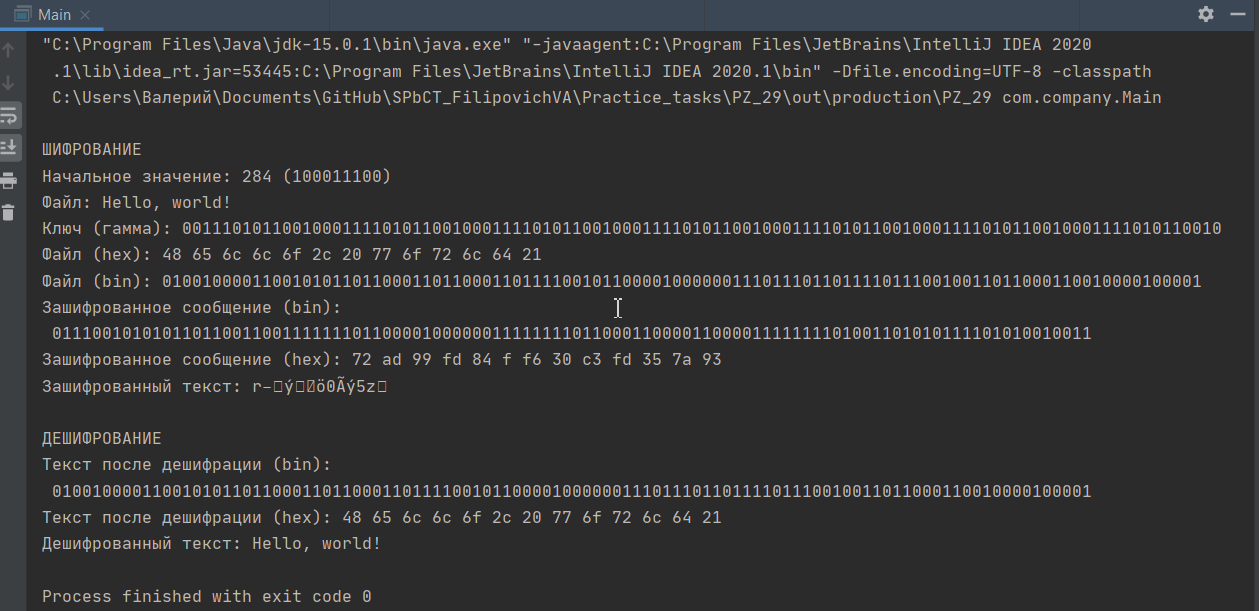
Вариант = 38 % 10 + 1 = 9

*X9+x5+x2*

**Ход выполнения работы**

1. Ознакомился с теоретической частью данной работы.
2. Создал новый консольный проект «PZ\_29» в среде разработки «IntelliJ IDEA 2020».
3. На языке программирования Java разработал алгоритм выполнения задач, описанных в пункте «Постановка задачи».

**Скриншоты выполнения программы**



*Рис. 1. Результат выполнения программы «PZ\_29»*

**Ссылка на GitHub**

<https://github.com/ValeriyFilipovich/SPbCT_FilipovichVA/tree/master/Practice_tasks/PZ_29>

**Контрольные вопросы**

1. **Преимущества и недостатки однократного гаммирования.**

Преимущество данного метода заключается в том, что для организации канала связи в открытых сетях этот метод организовывает хорошую конфиденциальность.

Недостаток – это необходимость иметь огромные объемы данных, которые можно было бы использовать в качестве гаммы.

1. **Почему размерность открытого текста должна совпадать с ключом?**

Размерности открытого текста и ключа должны совпадать, тогда полученный шифротекст будет такой же длины.

1. **Как по открытому тексту и шифротексту получить ключ?**

Надежность алгоритмов криптографии основана именно на неприемлемой трудоемкости их взлома. Ведь любую криптосистему можно вскрыть так называемым лобовым методом - получить образец шифротекста и, выполняя его дешифрование перебором возможных ключей, проверять осмысленность полученного открытого текста. Однако если взлом алгоритма обойдется дороже, чем ценность зашифрованной информации, или время, потраченное на его взлом, превосходит срок секретности данных, можно считать себя в относительной безопасности.

1. **Необходимые и достаточные условия абсолютной стойкости шифра?**

Необходимые и достаточные условия абсолютной стойкости шифра:

* полная случайность ключа;
* равенство длин ключа и открытого текста;
* однократное использование ключа.

1. **Как, зная текст одного из сообщений (P1 или P2), определить другое, не пытаясь определить ключ?**

Задача нахождения открытого текста по известному шифротексту двух телеграмм, зашифрованных одним ключом, может быть решена, используя (4). Для этого нужно сложить по модулю 2 оба равенства (4). Учитывая такие свойства операции xor, как



можно получить:



Предположим, что одна из телеграмм является "рыбой", т.е. имеет фиксированный формат, в который вписываются значения полей, и злоумышленнику доподлинно известен этот формат. Тогда он получает достаточно много пар Y1 Y2 (известен вид обоих шифротекстов) и, предположим, P1. Тогда с учётом (5) получается:



1. **Преимущества и недостатки использования скремблера.**

Основным же преимуществом таких цифровых систем кодирования и шифрования остается высокая степень закрытия речи, получаемая посредством использования широкого набора криптографических методов, применяемых для защиты передачи данных по каналам связи.

Главным недостатком использования данного метода является возникновение в системе большой задержки сигнала (до 300 мс), обусловленной необходимостью использования весовых функций. Это приводит к затруднениям в работе дуплексных систем связи.

1. **Свойства, которыми должна обладать псевдослучайная последовательность, генерируемая скремблером.**

Данная последовательность извлеченных бит должна обладать тремя свойствами:

* Сбалансированность: для каждого интервала последовательности количество двоичных единиц должно отличаться от числа двоичных нулей не больше, чем на несколько процентов от их общего количества на интервале.
* Цикличность: непрерывную последовательность одинаковых двоичных чисел называют циклом. Появление иной двоичной цифры автоматически начинает новый цикл. Длина цикла равна количеству одинаковых цифр в нём. Необходимо, чтобы половина всех «полосок» (подряд идущих идентичных компонентов последовательности) имела длину 1, одна четвертая – длину 2, одна восьмая – длину 3, и т.д.
* Корреляция: если часть последовательности и её циклично сдвинутая копия поэлементно сравниваются, желательно, чтобы число совпадений отличалось от числа несовпадений не более чем на несколько процентов от длины последовательности.