Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №2**

**по курсу «СиМОИБ»**

**на тему: «Простейшие алгоритмы шифрования»**

|  |  |
| --- | --- |
| Выполнил студент группы 821703: | Веренич К.О. |
| Проверил: | Захаров В.В. |

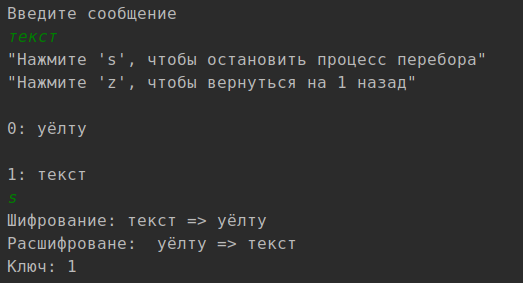
**МИНСК**

2020

**Задание:**

Реализовать систему шифрования Гая Юлия Цезаря

**Выполнение программы:**



**Вывод:**

Способы выбора ключей могут быть различны. В шифре Цезаря ключом служит произвольное число k, выбранное в интервале от 1 до 33 (Количество букв в алфавите). Малое пространство ключей (всего 25 вариантов) делает брут-форс самым эффективным и простым вариантом атаки.  
Для вскрытия необходимо каждую букву шифртекста заменить буквой, стоящей на один знак левее в алфавите. Если в результате этого не удалось получить читаемое сообщение, то необходимо повторить действие, но уже сместив буквы на два знака левее. И так далее, пока в результате не получится читаемый текст.

Достоинством системы шифрования Цезаря является простота шифрования и расшифрования. Учитывая то, что подбор ключа в автоматическом режиме практически невозможен (существует вероятность появления осмысленных сообщений при разных значениях ключа, требуется проверка оператором), при определенных условиях можно считать такую систему шифрования достаточной.

К недостаткам системы Цезаря следует отнести следующие: 1) Подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного открытого текста. 2) Сохраняется алфавитный порядок в последовательности заменяющих букв, при изменении значения ключа изменяются только начальные позиции такой последовательности. 3) Число возможных ключей мало.

Для большинства сценариев использования система с таким количеством ключей будет недостаточно стойкой, и в таких ситуациях стоит обратиться к более современным методам шифрования.