Шаблон отчёта по лабораторной работе №3

Дисциплина: Математические основы защиты информации и информационной безопасности

Миличевич Александра

Содержание

# Цель работы

Познакомится с способом шифрования гаммирование

# Задание

1. Реализовать алгоритм шифрования гаммированием конечной гаммой

# Выполнение лабораторной работы

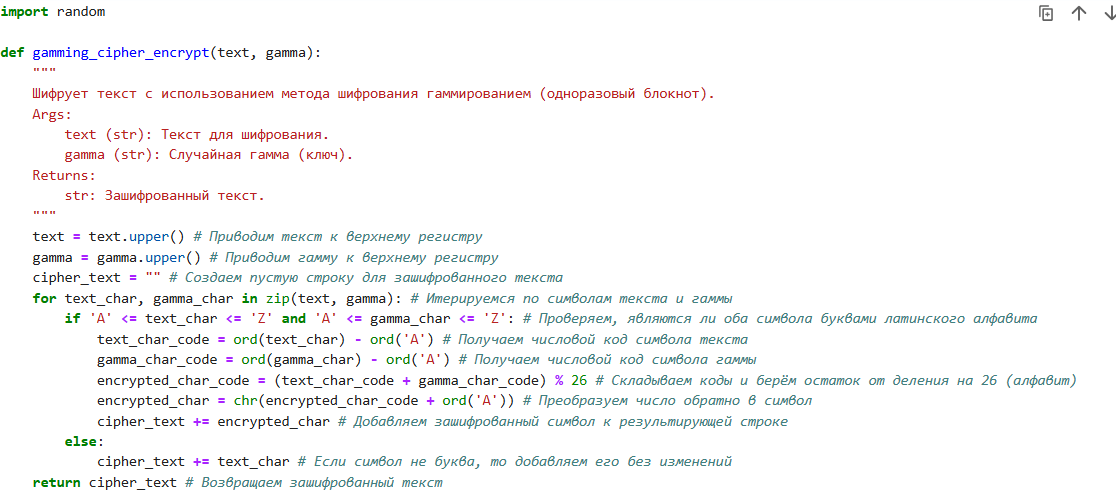
## Шифрование гаммированием (одноразовый блокнот) на русском языке

Этот код реализует шифрование гаммированием для русского языка, также известное как шифрование с использованием одноразового блокнота.

### Функция gamming\_cipher\_encrypt\_ru(text, gamma)

Эта функция выполняет шифрование текста с помощью гаммирования.

* **Вход:**
  + text: Строка - текст для шифрования (русский язык).
  + gamma: Строка - гамма (ключ) для шифрования (русский язык).
* **Выход:** Строка - зашифрованный текст (русский язык).



функция гаммирования

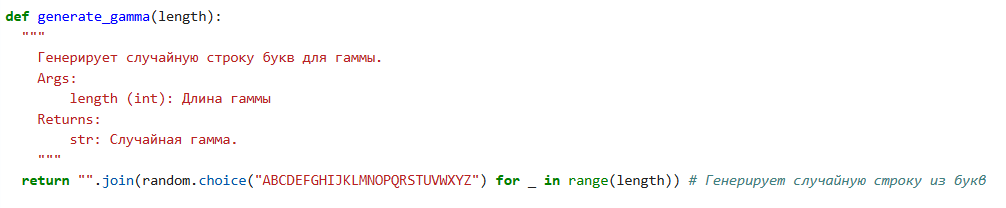
#### Логика работы:

1. Приводит текст и гамму к верхнему регистру.
2. Создает пустую строку для хранения зашифрованного текста.
3. Определяет русский алфавит и его длину.
4. Перебирает символы текста и гаммы параллельно.
5. Для русских букв:
   * Вычисляет индексы букв в алфавите.
   * Складывает индексы, берет остаток от деления на длину алфавита для получения индекса зашифрованного символа.
   * Добавляет зашифрованный символ в результирующую строку.
6. Для остальных символов:
   * Добавляет их в результирующую строку без изменений.

### Функция generate\_gamma\_ru(length)

Эта функция генерирует случайную гамму заданной длины.

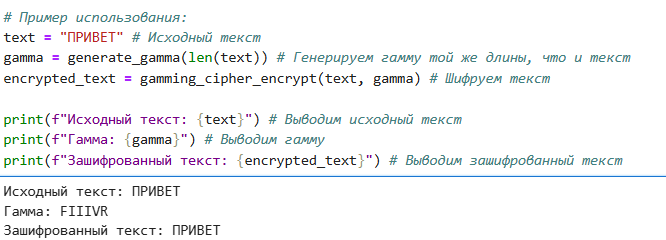
* **Вход:** length: Целое число - длина гаммы.
* **Выход:** Строка - случайная гамма (русский язык).



функция generate\_gamma

#### Логика работы:

1. Определяет русский алфавит.
2. Генерирует случайную строку заданной длины из символов русского алфавита.



пример применения

### Пример использования

1. Задается исходный текст: ПРИВЕТ.
2. Генерируется случайная гамма той же длины.
3. Выполняется шифрование текста с использованием гаммы.
4. Выводится исходный текст, гамма и зашифрованный текст.

### Важные замечания

* Для максимальной безопасности, гамма должна быть действительно случайной и использоваться только один раз для каждого сообщения.
* Этот код предназначен только для текста на русском языке.
* Шифрование гаммированием является одним из самых надежных методов шифрования при условии правильного использования.

# Выводы

Программно реализовано шифрование гаммированием.