Шифр гаммирования

Кашкин Иван Евгеньевич
19 октября, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма шифрования гаммированием

Выполнение лабораторной работы

Гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Формула

В аддитивных шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются. Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

$$Ci = (Ti + Gi) mod N$$

Пример работы программы

```
In [8]:
1 text = "ялюблюрудн"
2 len(text)

Out[8]: 10

In [9]:
1 gamma = "физматфизм"
2 len(gamma)

Out[9]: 10

In [10]:
1 main(text, gamma)

Числа текста:  [33, 13, 32, 2, 13, 32, 18, 21, 5, 15]
Числа гаммы:  [22, 10, 9, 14, 1, 20, 22, 10, 9, 14]
Числа шифровки:  [22, 23, 8, 16, 14, 19, 7, 31, 14, 29]
Расшифровка:  ялюблюрудн
шифровка:  йвхуккыйыа
```

Figure 4: Работа алгоритма гаммирования

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритм шифрования с помощью гаммирования