

Лабораторная работа №7

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования

Пишем код приложения

</> source code

```
1 real_string = "Что-то тут написано!!!!"
2 key_string = "С новым Годом, друзья!"
3 def xor_strings(xs, ys):
4     return "".join(chr(ord(x) ^ ord(y)) for x, y in zip(xs,ys))
5 xored = xor_strings(real_string, key_string)
6 print xored.encode("hex")
7 xored_second = xor_strings(real_string, xored)
8 print xored_second
9 xored_third = xor_strings(key_string, xored)
10 print xored_third
11
```

Код программы

Получаем результат работы приложения

0006f1526d6e9301300135f06da20110013cf0646d6e606c93f06865505061536d676fadf0ae00

С новым Годом, друзья!

Что-то тут написано!!!!

Приложение

Первая строка соответствует зашифрованной информации, вторая строка – расшифрованному тексту, а третья – ключу.

Вывод

В результате выполнения лабораторной работы мы освоили на практике применение режима однократного гаммирования.