1 Description

Title: Квадратная прецессия

Category: Crypto

Value: 100

Даны три шифротекста (ciphertext1.txt, ciphertext2.txt, ciphertext3.txt) и два открытых текста (plaintext1, plaintext2), зашифрованные одним и тем же шифром. Требуется расшифровать третий текст и найти в нем флаг.

2 Legend

Наши разведчики перехватили важную переписку с серверов противника. К сожалению, перехватить в открытом виде удалось только незначительные сообщения. Ваша цель - расшифровать все.

3 Flag

Flag regex:	simple text
Flag:	gravitationfollowsspacecreatures

4 Solution

Заметим, что частотность символов не изменяется - это шифр перестановки. Длина сообщений является точным квадратом, намекает на квадратную таблицу. Запишем шифротекст в таблицу по строкам и увидим, что открытый текст вырисовывается зигзагом. Восстанавливаем исходный текст. Более подробно можно посмотреть в файле task.py и функции test().

5 Hints

1. Заметьте, что частотность символов не изменяется.
2. Измерьте длину сообщений.
3. Это перестановка внутри квадратной таблицы.
4. Зигзаг же с левого верхнего угла!

6 Discussion

Возможно усложнить задачу путем внесения дополнительных перемешиваний. Можно упростить задачу путем уменьшения третьего текста, чтобы им не писать программу, а делать задание вручную.

7 Setup

Выдать командам архив с файлами ciphertexts/*.txt и plaintexts/{1.txt, 2.txt}.