Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное учреждение высшего образования

«Новгородский государственный университет имени Ярослава Мудрого»

Кафедра «Информационных технологий и систем»

**Лабораторная работа №2**  
по дисциплине:

«Защита информации»

Разработал:

Студент группы 8091

Шаклеин В. В. \_\_\_\_\_\_  
 «\_\_» \_\_\_\_\_2021г

Проверил преподаватель:

Жгун Т. В. \_\_\_\_\_

«\_\_» \_\_\_\_\_2021г

**Великий Новгород**

**2021**

**Задача:**

1. Зашифровать предлагаемый фрагмент текста объемом около 500 символов (допустим диапазон 500–1000 символов). Открытый текст выбирается из текстового документа в соответствии с номером студента в прилагаемом списке. Использовать следующие способы шифрования:

1.1 с помощью способов традиционного шифрования, указанных в таблице 2 (в моем случае шифр Полибия с паролем);

1.2 с помощью ключа (пароля), где в качестве ключа используем:

1.2.1 константу, равную номеру студента в списке;

1.2.2 поговорку из табл.1, соответствующую номеру студента в списке, используя алфавит Z32 = (А…Я, е=ё );

1.2.3 псевдослучайную последовательность (ПСП), сгенерированную линейным рекуррентным генератором (*LFSR*). ПСП генерируется матрицей 5\*5. Производящий многочлен выбирает студент самостоятельно.

2. Построить гистограммы для полученных зашифрованных текстов. Проанализировать результат (четыре гистограммы)

**Описание алгоритмов:**

*Шифрование*

Шифрование происходит в несколько шагов:

1. Формирование таблицы шифрования

«Квадрат Полибия» представляет собой квадрат 5x5, столбцы и строки которого нумеруются цифрами от 1 до 5. В каждую клетку этого квадрата записывается одна буква (в русско алфавите 31 буква, Ъ и Ё исключены, кроме того, в одну клетку поместите буквы е-э, и-й, ж-з, р-с, ф-х, ш-щ). Буквы расположены в алфавитном порядке. В результате каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел. Расшифровывается путём нахождения буквы, стоящей на пересечении строки и столбца.

Для шифрования с ключом первые ячейки квадрата заполняются символами ключа, а последующие оставшимися символами алфавита.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | А | Б | В | Г | Д |
| 2 | Е/Э | Ж/З | И/Й | К | Л |
| 3 | М | Н | О | П | Р/С |
| 4 | Т | У | Ф/Х | Ц | Ч |
| 5 | Ш/Щ | Ы | Ь | Ю | Я |

Шифрование

Для шифрования на квадрате находим букву текста и вставляем в шифровку нижнюю от неё в том же столбце. Если буква находится в нижней строке, то берём верхнюю из того же столбца.

*Дешифрование*

Для дешифрования на квадрате находим букву текста и вставляем в дешифровку верхнюю от неё в том же столбце. Если буква находится в верхней строке, то берём нижнюю из того же столбца.

**Реализация**

Задача решена с помощью языка программирования Python, используются следующие дополнительные модули: numpy, matplotlib, seaborn, они необходимы для упрощения использования математических операций над массивами чисел и построения гистограмм.

**Описание интерфейса**

Все входные значения жёстко задаются в коде, так что программа не имеет пользовательского интерфейса в привычном понимании.

**Код программы**

Код программы находится в папке с отчетом в файле polybius*.ipynb* (так же код с возможностью запуска онлайн доступен по адресу ... )

**Результат работы программы**

В ходе работы программы получились следующие значения и гистограммы:

Исходный текст (для работы алгоритма удалены знаки препинания и пробелы):

«аещесторонникитоталитаризмавнаукемогутбытьобьективнорассмотренысоответствующимиинстанциямисовременныетехнологиидостиглитакогоуровнячтовыбранныинамиинновационныипутьоднозначнофиксируетнеобходимостьприоритизацииразуманадэмоциямиестьнадчемзадуматьсяпредпринимателивсетиинтернетвравноистепенипредоставленысамисебетакжекакконсультациясширокимактивомнеоставляетшансадляинновационныхметодовуправленияпроцессаминопостоянноеинформационнопропагандистскоеобеспечениенашеидеятельностипредопределяетвысокуювостребованностьукрепленияморальныхценностеи»

Используя константу (символ «с»):

«жлалчшхехффосошхшжтошжеонужифжщслухйщшзвшгхзглсшоифхежччухшелфвчххшилшчшищаоуоофчшжфьоуочхиелулффвлшлыфхтхйоокхчшойтошжсхйхщехифэшхивзежффвофжуооффхижьохффвоцщшгхкфхнфжэфхъосчоещлшфлхзыхкоухчшгцеохеошонжьооежнщужфжкдухьоуолчшгфжкэлунжкщужшгчцелкцеофоужшлтоичлшоофшлефлшиежифхочшлцлфоцелкхчшжитлфвчжуочлзлшжсмлсжссхфчщтгшжьочроехсоужсшоихуфлхчшжитлшржфчжктоффхижьохффвыулшхкхищцежитлфоцехьлччжуофхцхчшхффхлофъхеужьохффхцехцжйжфкочшчсхлхзлчцлэлфолфжрлоклшлтгфхчшоцелкхцелклтлшивчхсщихчшелзхижффхчшгщселцтлфоухежтгфвыьлффхчшло»

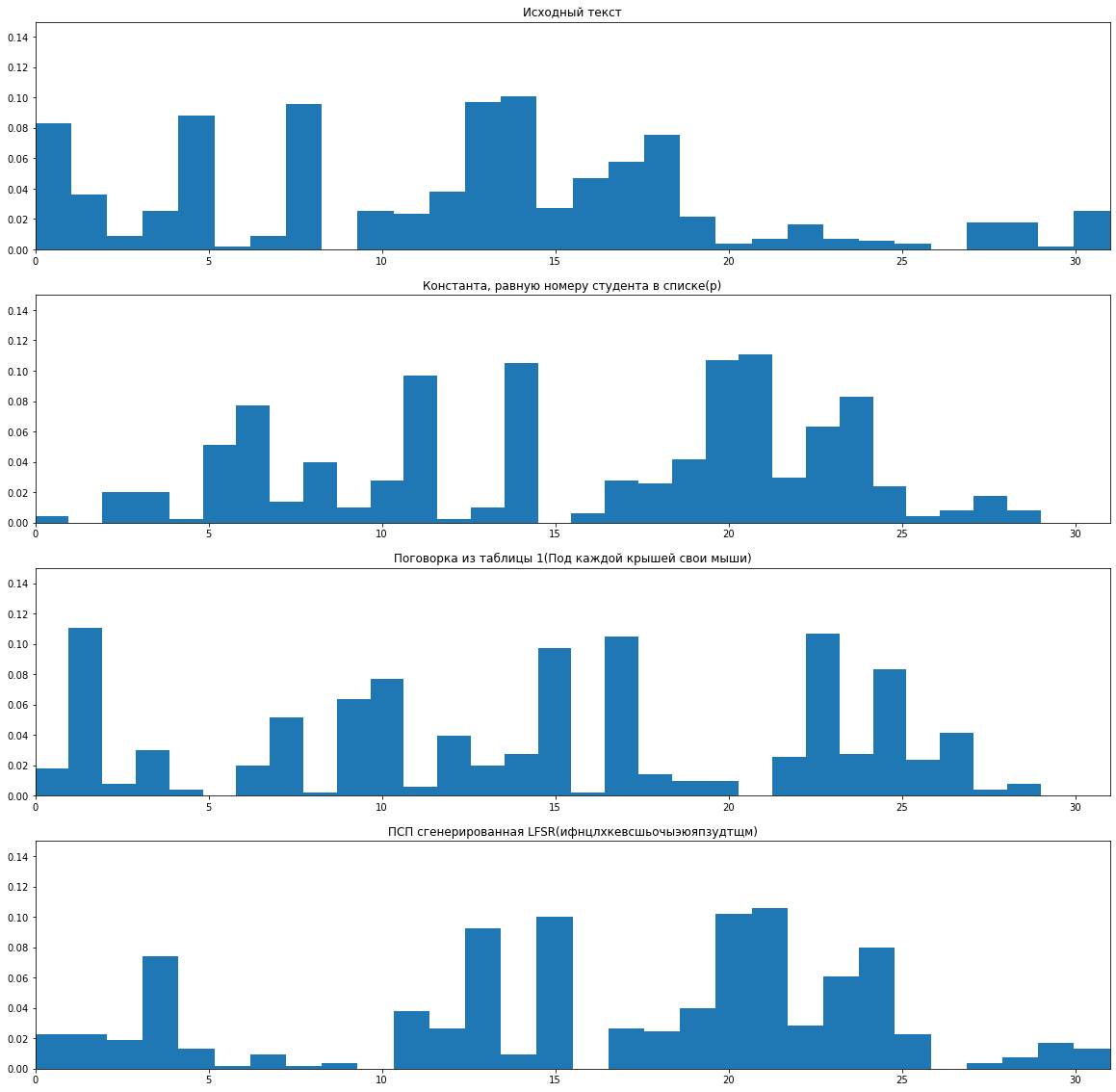
Используя ключ из таблицы (Под каждой крышей свои мыши):

«кпдпйщбзбччсшсщбщкцсщкзсфыкмчкъшпыбуъщтнщжбтжпшщсмчбзкййыбщзпчнйббщмпщйщмъдсыссчйщкчасысйбмзпыпччнпщпэчбцбуссобйщсуцсщкшбубъзбмчвщбмнтзкччнсчкыссччбмкасбччнсгъщжбочбфчквчбьсшйсзъпщчпбтэбосыбйщжгзсбзсщсфкассзкфъыкчкоиыбасыспйщжчковпыфкоъыкщжйгзпогзсчсыкщпцсмйпщссчщпзчпщмзкмчбсйщпгпчсгзпобйщкмцпчнйкысйптпщкшрпшкшшбчйъцжщкасйлсзбшсыкшщсмбычпбйщкмцпщлкчйкоцсччбмкасбччнэыпщбобмъгзкмцпчсгзбапййкысчбгбйщбччбпсчьбзыкасбччбгзбгкукчосйщйшбпбтпйгпвпчспчклпсопщпцжчбйщсгзпобгзпопцпщмнйбшъмбйщзптбмкччбйщжъшзпгцпчсыбзкцжчнэапччбйщпс»

Используя ключ, сгенерированный генератором LSFR: (ифнцлхкевсшьочыэюяпзудтщм)

«днанчшххффпспшхшдтпшдпоудлфдщснухзщшебшгхегнсшплфхдччухшнфбчххшлншчшлщйапуппфчшдфэпвупчхлнунффбншньфхтхзппмхчшпзтпшдсхзхщхлфвюшхлбедффбпфдуппффхлдэпхффбпцщшгхмфхофдюфхыпсчпщншфнхеьхмпухчшгцпхпшподэппдощудфдмжухэпвупнчшгфдмюнуодмщудшгчвцнмцпфпудшнтплчншппфшнфншлдлфхпчшнцнфпцнмхчшдлтнфбчдупчненшдсинсдссхфчщтгшдэпвчяпхспудсшплхуфнхчшдлтвншядфчдмтвпффхлдэпхффбьуншхмхлщцдлтнфпвцхэнччдупфхцхчшхвффхнпфыхудэпхффхцхцдздфмпчшчсхнхенчцнюнфпнфдянпмнвшнтгфхчшпцнмхцнмнтвншлбчхсщйлхчшнехлдффхчшгщснцтнфпвухдтгфбьэнффхчшнп

Гистограммы:



**Вывод**Для решения поставленных задач был выбран ЯП Python, также были построены гистограммы.

В качестве исходного текста был выбран не литературный текст, сгенерированный с помощью сайта fish-text.ru. Рассмотрим гистограммы, которые мы получили. Можем сделать вывод о том, что все варианты ключа, не маскируют исходную частоту встречаемости символов, это ожидаемо поскольку шифр предполагает замену символов 1-к-1. Кроме этого заметно что все гистограммы, кроме той в которой используется поговорка выглядят как сдвинутая исходная с небольшими отклонениями.