МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ІКТА

кафедра ЗІ



**З В І Т**

до лабораторноїроботи №2

з курсу: «Основи криптографічного захисту інформації»

на тему: «ДОСЛІДЖЕННЯ КЛАСИЧНИХ МЕТОДІВ ШИФРУВАННЯ»

Виконав: ст. гр. УІ-42

Симоненко Д.С.

Прийняв: Шандра З.А.

Львів – 2017

**Мета роботи:** дослідження класичних методів шифрування.

Завдання

1. Для одноалфавітного метода із заданим зміщенням потрібно:

- виконати шифрування з довільним зміщенням для вибраногов ихідного

тексту;

- проглянути та описати гістограми вихідного і зашифрованого текстів,

Визначити зміщення для кількох символів;

- розшифрувати текст за допомогою програми;

- дешифрувати зашифрований текст за допомогоюпрограми методом

підборузміщення; вказати, з яким зміщенням був зашифрований файл.

2. Для методу перестановки символів дешифрувати зашифрований файл. Для

Цього потрібно визначити закон перестановки символів відкритого тексту.

Створіть невеликий файл довжиною в декількаслів з відомим вам текстом,

зашифруйте його, прогляньте гістограми (опишіть їх; зясуйте, чи можна

витягнути із них корисну для дешифрування інформацію). Потрібно

порівняти (за допомогою редактора) вихідний і зашифрований тексти та

визначити закон перестановки символів.

Дешифруйти файл:

- вручну (поясніть ваші дії);

- за допомогою програми.

3. Для багатоалфавітного шифрування з фіксованим ключем потрібно

визначити, скільки одноалфавітних методів і з яким зміщенням застосовано в

програмі. Для цього треба створити файл, що складається із рядка однакових

символів, виконати для нього шифрування і по гістограмі визначити спосіб

шифрування.

4. Для багатоалфавітного шифрування з ключем фіксованої довжини:

- виконати шифрування і визначити по гістограмі, яке зміщення отримує

кожний символ для файла, що складається із рядка однакових символів;

- виконати шифрування і розшифрування для файла довільного тексту;

- проглянути й описати гістограми вихідного і зашифрованого текстів;

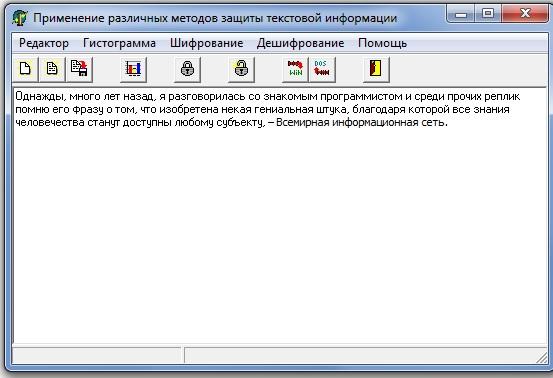
визначити, яку інформацію можна отримати із гістограми.

5. Для багато алфавітного шифрування з довільним паролем завдання

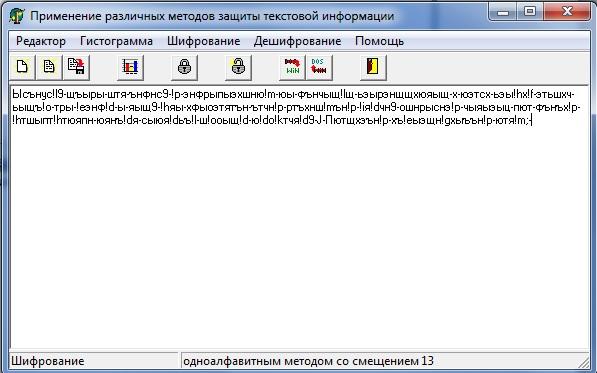
аналогічно п.4.

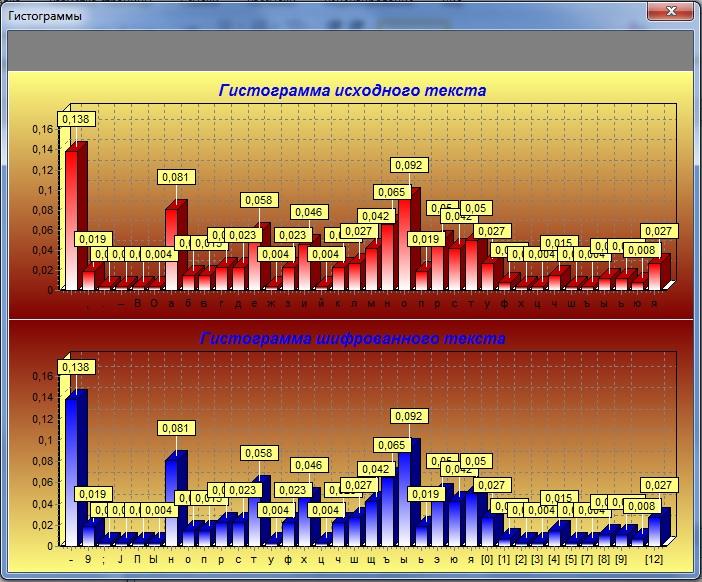
Виконання

**1.Одноалфавітний метод іззаданимзміщенням.**



В шифруванні використовувалось зміщення на 13 позицій.



Отримані наступні результати:

***Процесдешифрування вручну.***

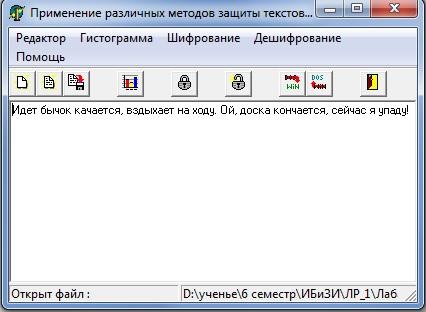
Із гістограмишифрованого текста возьмемо найбільш часто зустрічаючий символ ‘-’. В гістограмівихідного тексту йому відповідає символ ‘ ’ (пробіл), оскількивінмає ту ж частоту повторюваності 0,138. Із ASCII-таблиці код символу ‘ ’ (пробіл) рівний 32, а код символу ‘-’ рівний 45. Обчислимозміщення: 45 – 32 = 13. Знаючизміщення, можнаобчислитисимволи, що залишисяза формулою:

ASCII-код вихідного символу =ASCII-код шифруючого символу – зміщення;

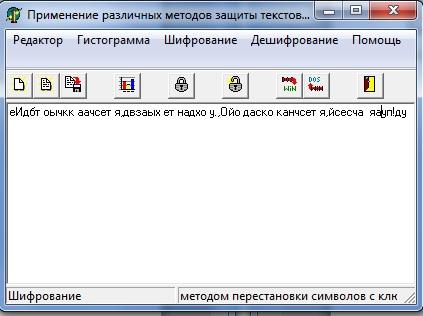
При цьому не вартозабувати про відсутність символів під номерами 176 – 223 і 240 – 255 в таблиці ASCII-кодів.

**2. Метод перестановки символів.**

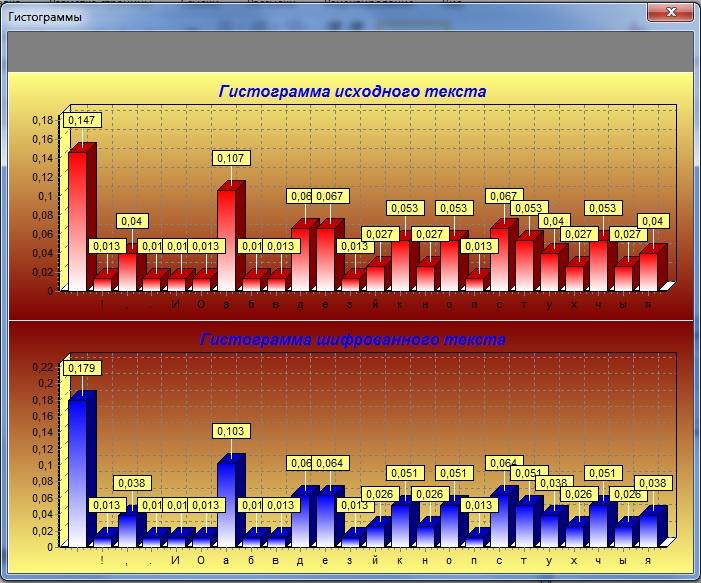
Вихіднийтекстовий файл – Барто.txt



Після шифруванняз ключем 312, отримали:



Гістограмивихідногоізашифрованого текстів схожих між собою:



Якщо кількість символів вихідного текстукратне довжині ключа, то гістограми співпадуть, інакше – не співпадуть, оскільки в кінцівихідного тексту добавляютьсявідсутні для кратності ‘ ’ (пробіли).

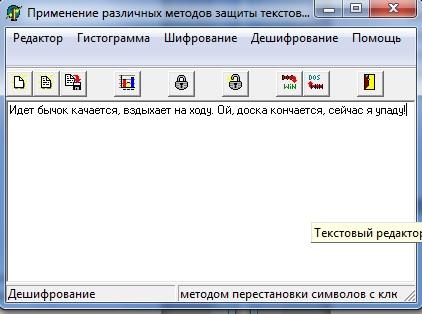
Гістограма не міститькорисної інформації для дешифрування, оскільки даний метод заснований на перестановці символів, отже, частота появиокремих символів співпадає.

***Процес дешифрування вручну.***

Довжина ключа рівна 3, значить беремоіз шифрованого тексту блок разміром в 3 символа і виконуємо над ним наступні дії: беремо символ з номером, відповідним номеру першоїпозиції ключа (символ з номером 3) іпоміщаємойого в першупозицію розшифрованого тексту. Даліробимо те ж самез символом, відповідним номеру другоїпозиції, після того – третьої, після чого переходимододешифруваннянаступного блоку.

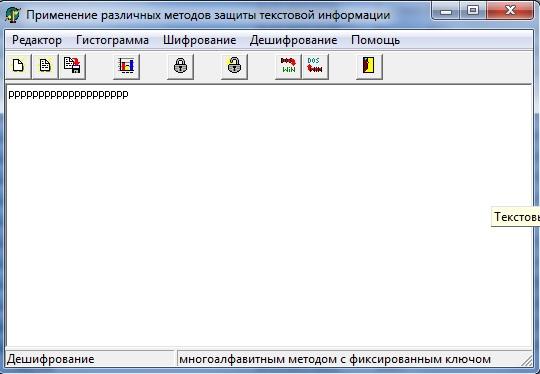
***Дешифрування з допомогою програми.***

Для розшифровки тексту, потрібноно задати той же ключ, щоі при шифруванні, тобто в нашомувипадку – 312.

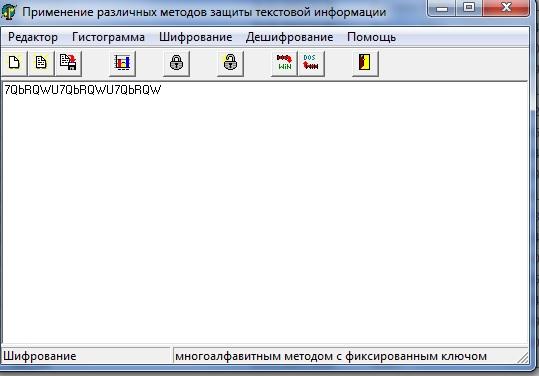


**3. Метод багатоалфавітного шифрування з фіксованим ключем.**

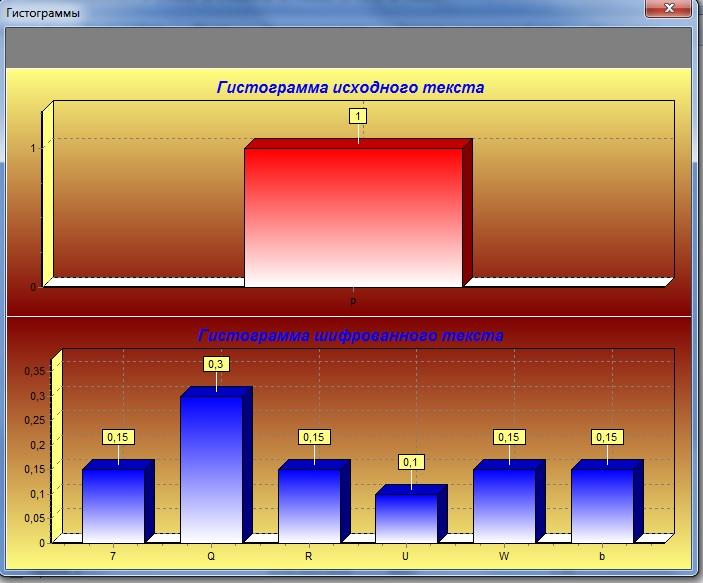
Вихідний файл – Стрічка.txt



Після шифрування отримали:



Гістограмивихідноїі зашифрованоїстрічки:



Для шифрування послідовностііз однакових символів використовуєтьсянабір із 7-и зміщень.

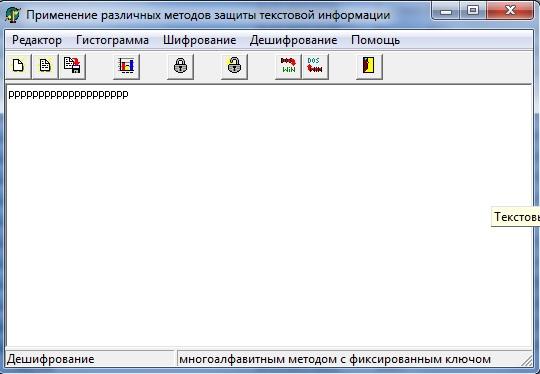
Розглянемо метод шифрування:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | рррррррррррррррррррр | ASCII-код | Зміщення | Результат |
| 1. | **7**ррррррррррррррррррр | 240 | -185 | 55 – «7» |
| 2. | **7Q**рррррррррррррррррр | 240 | -159 | 81 – «Q» |
| 3. | **7Qb**ррррррррррррррррр | 240 | -142 | 98– «b» |
| 4. | **7QbR**рррррррррррррррр | 240 | -158 | 82– «R» |
| 5. | **7QbRQ**ррррррррррррррр | 240 | -159 | 81 – «Q» |
| 6. | **7QbRQW**рррррррррррррр | 240 | -153 | 87 – «W» |
| 7. | **7QbRQWU**рррррррррррррр | 240 | -155 | 85– «U» |
|  | … |  |  |  |
| n | 7QbRQWU7QbRQWU7QbRQW |  |  |  |

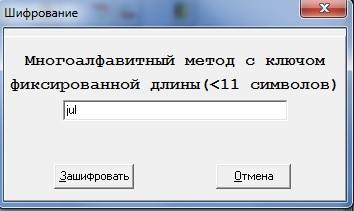
Після 7-го крокунабір зміщень повторюється. І в конці ми отримали результат шифрування.

## 4.Метод багатоалфавітного шифрування з ключем фіксованої довжини.

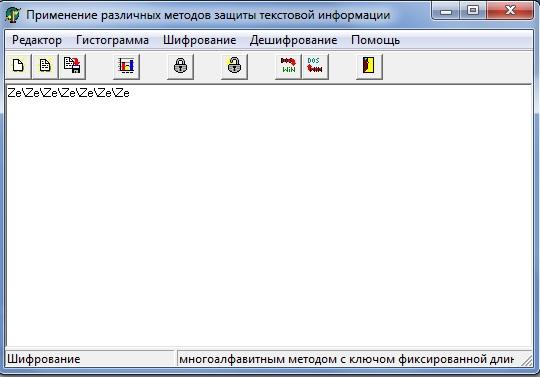
Вихідний текстовий файл – Стрічка.txt



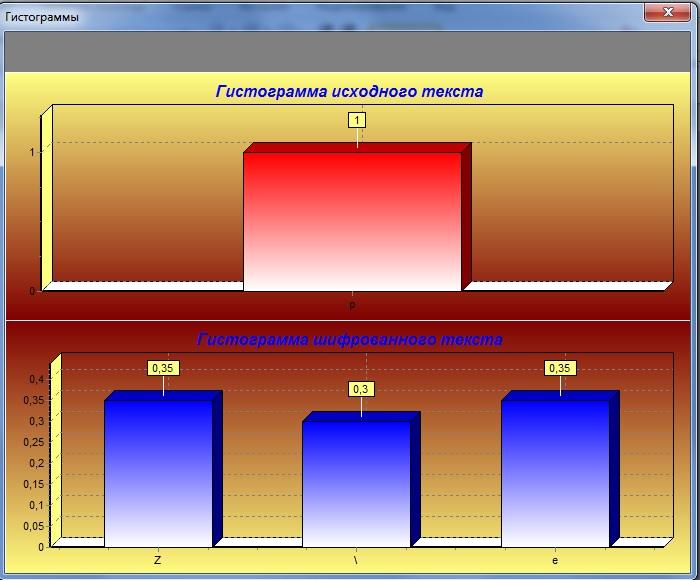
Вводимо ключ шифрування:



Отримуємо:



Гістограма вихідного і зашифрованого текстів:



По гістограміможнівизначити довжину ключа, якимзашифрувався вихідний текст. Вона відповідає кількості символів на гістограмізашифрованого тексту. В даномувипадкувикористовувався ключ довжиноюу 3 символа.

Переклад символів здопомогою ASCII-таблиці:

Вихідний символ: р – 240;

Ключ: j– 106;u– 117;l– 108;

Послідовністьіз повторюваних символів «Ze\» (ASCII-коди:Z– 090; \ – 092;e– 101) визначимоза формулою:https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-8_Nsv_.png. Деhttps://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-phdTeI.png– зашифрований символ,https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-uDufvF.png– шифруючий символ (вихідний),https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-cC4Hfz.png– задана гамма послідовність,https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-LuTgTq.png– кількість символів валфавіті (255 – в нашомувипадку).

Отже:

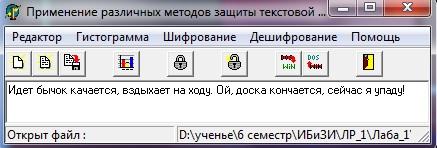
https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-Z7qeIg.png;

https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-XfbLXW.png;

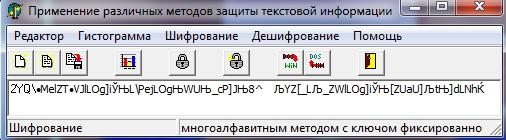
https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-mIRTuZ.png;

Як бачимо, для шифрування вихідного текстувикористовуєтся фор-ла: https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-cshY4R.png.

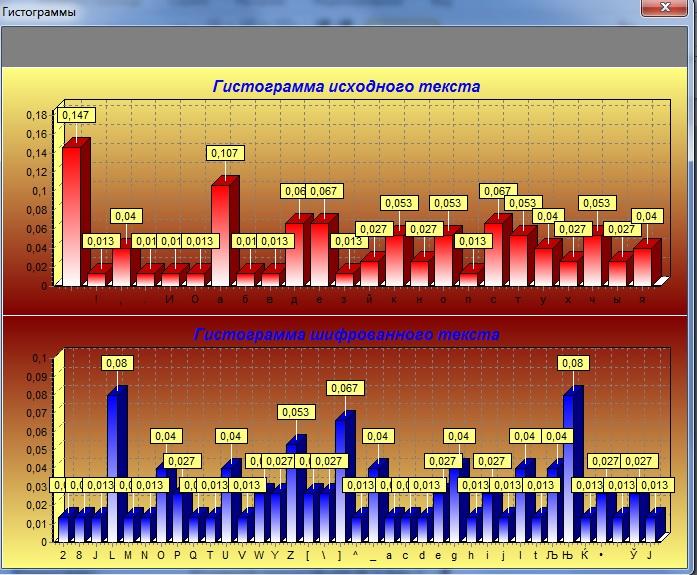
Вихідний файл: Барто.txt



Зашифруємойого:



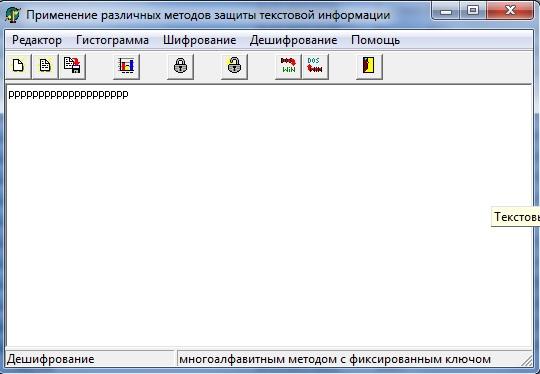
Гістограми вихідного і зашифрованого текстів:



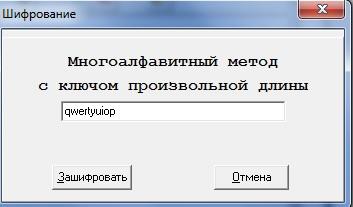
Ніякої закономірностіабоважливоїінформації гістограми не несуть.

# 5. Багатоалфавітне шифруванняздовільним паролем.

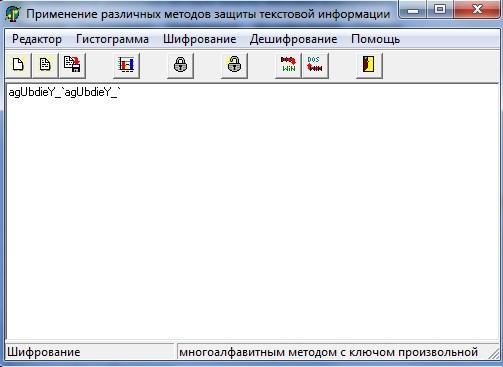
Вихідний текстовий файл – Стрічка.txt



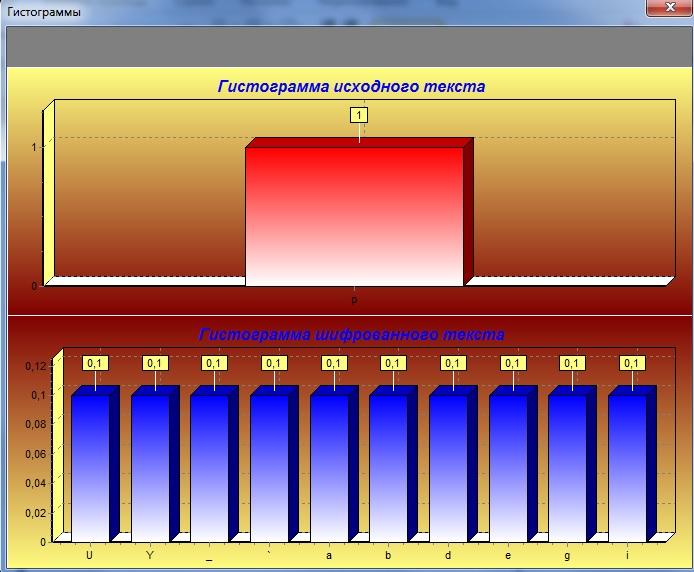
Вводимо ключ шифрування:



Отримуємо:



Гістограмавихідногоізашифрованого текстів:



Переклад символів здопомогою ASCII-таблиці:

Вихідний символ: р – 240;

Ключ: q– 113;w– 119;e– 099;r– 114;t– 116;y– 121;u– 117;i– 105;o– 111.

Отримуємопослідовністьіз повторюваних символів: «agUbdieY\_`» (ASCII-коди:a– 097;g– 103;U– 085;b– 098;d– 100;i– 105;e– 099;Y– 089; \_ - 095; ‘ - 096 ). Визначимо метод шифрування за формулою:https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-qqlsz0.png. Деhttps://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-kicW8E.png– зашифрований символ,https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-Kh4YqA.png– шифруючий символ (вихідний),https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-LicwwR.png– задана гамма послідовність,https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-N0Uzpr.png– кількість символів валфавіті (255 – в нашомувипадку).

Отже:

https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-VfnBFl.png;

https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-uMa83t.png;

https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-hc1iUZ.png

и т.д.

Можемопобачити, що для шифрування вихідного текстувикористовувалась формула: https://studfiles.net/html/2706/28/html_zWsgaN71L0.2Pua/img-OQtwLK.png.

**Висновок:** під час лабораторної роботи я дослідив класичні методи шифрування, а саме:

* метод одноалфавітного метода із заданим зміщенням;
* метод перестановки символів дешифрувати зашифрований файл;
* методбагатоалфавітного шифрування з фіксованим ключем;
* методбагатоалфавітного шифрування з ключем фіксованої довжини;
* метод багатоалфавітного шифрування з довільним паролем.