**ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ОЛЕСЯ ГОНЧАРА**

**Факультет прикладної математики**

**Кафедра математичного забезпечення ЕОМ**

**Звіт**

з лабораторної роботи № 3

з курсу «БПтД»

на тему: «Елементи криптоаналізу»

Виконав:

Студент

групи ПЗ-21у-1

Войцехов М.О.

м. Дніпро

2023 р.

**Мета роботи**

Ознайомитись з симетричними методами шифрування та підходами до їх крипто-аналізу.

**Хід роботи**

Завдання: для кожного зашифрованого повідомлення знайти ключ та відкрите повідомлення. Повідомлення зашифровані методами: перестановки стовпців, подвійної перестановки (стовпців та рядків), заміни та шифру Віженера.

Метод перестановки стовпців(Варіант 57).

Зашифроване повідомлення: нумсілзя\_наз\_ичвйа\_ригезхе\_нитвхт\_\_о\_неи\_н.

Так як довжина зашифрованого тексту дорівнює m\*n, де m – к-ть рядків, n – к-ть стовпців, а також n<m, маємо наступні варіанти матриць 7\*6 та 14\*3. Більш підходящою є варіант з розміром матриці 7\*6.

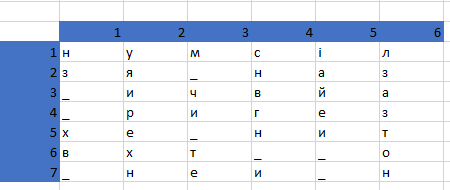


Рисунок 1 – Повідомлення в матриці

Далі, методом перестановок стовпців вийшло, наступне повідомлення.

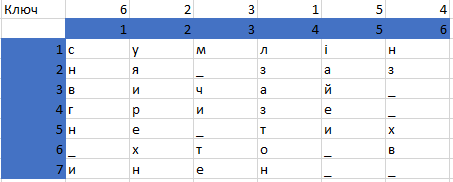


Рисунок 2 – Розшифроване повідомлення

Отже, повідомлення: сумління зазвичай гризе не тих хто винен.

Зашифроване повідомлення: нумсілзя\_наз\_ичвйа\_ригезхе\_нитвхт\_\_о\_неи\_н.

Розмір матриці: 7\*6.

Ключ(порядок шифрування): 623154.

Метод подвійної перестановки(Варіант 85).

Зашифроване повідомлення:аик\_рщгям\_і\_\_мнеід\_аил\_\_изорбтооопмгееа\_л\_

Так як довжина зашифрованого тексту дорівнює m\*n, де m – к-ть рядків, n – к-ть стовпців, а також n<m, маємо наступні варіанти матриць 7\*6 та 14\*3. Більш підходящою є варіант з розміром матриці 7\*6.

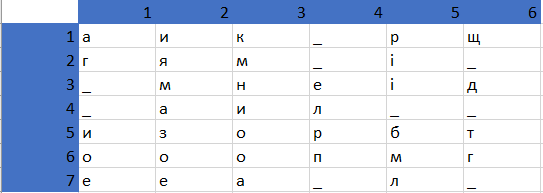


Рисунок 3 – Повідомлення в матриці

Далі, методом перестановок стовпців вийшло, наступне повідомлення.

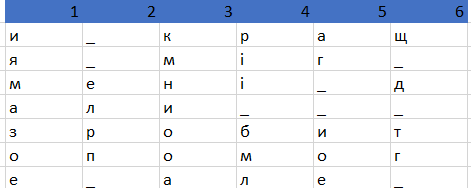


Рисунок 4 – Перестановка стовпців

Після цього, зробив перестановку рядків.

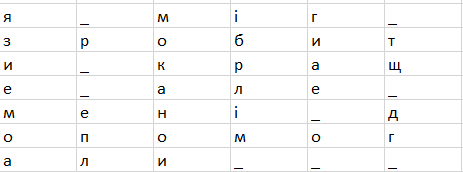


Рисунок 5 – Перестановка рядків

Отже, повідомлення: я міг зробити краще але мені допомогали.

Зашифроване повідомлення: аик\_рщгям\_і\_\_мнеід\_аил\_\_изорбтооопмгееа\_л.

Розмір матриці: 7\*6.

Ключ(порядок шифрування стовпців):513246.

Ключ(порядок шифрування рядків):3157264.