**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: 33-68 64-35-61-12-52-15-12 61-12 39-12-41-18-50-68-55-55-19 42-50-18-62-34-18-19-55-62-34-52-35 72-14-50-35-48-55-57-69 55-12-62-18-70-18 55-35-34-69-70-26-55-69 42-50-68-62-34-18-14-18, 19-14-69 52-52-35-59-35-70-18-62-26 12-11-68-50-68-15-12-20 52-69-61 47-12-50-55-18-42 62-18-70 (64-35-50-35-64 48-42 20-12-59-55-35 39-12-11-35-47-18-34-18 55-35 64-15-35-50-61-35-42 – 39-50-18-14-50-35-62-69, 39-12-41-18-50-68-55-55-69 55-35 64-35-14-35-50-39-35-34-34-69, 33-12 62-14-70-35-61-35-70-35-62-26 64 14-69-70-26-14-12-42 55-18-64-12-14 42-50-68-62-34-69-52 39-68-50-68-20-68-59-12-52-35-55-18-42 14-12-50-35-70-19-20-18 47-18 62-14-70-19-55-14-35-20-18, 39-68-50-41-72 64-15-35-50-61-72 61-69-52-47-18-55-14-35 12-34-50-18-20-72-52-35-70-35 55-35 39-68-50-41-69 69-20-68-55-18-55-18, 35 52 55-35-62-34-72-39-55-69 50-12-14-18 64-15-35-50-61-18 61-35-50-72-52-35-70-18-62-26 52-59-68 39-35-50-35-20-18). 42-50-68-62-34-12-20 39-50-18-14-50-35-41-35-70-18 39-12-62-72-61. 55-35-39-50-18-14-70-35-61, 15-70-68-47-18-14-18 64 42-50-68-62-34-35-20-18, 52-18-15-12-34-12-52-70-68-55-55-69 55-35 60-68-61-12-50-12-52-72 62-72-11-12-34-72 (39-68-50-41-35 62-72-11-12-34-35 52-68-70-18-14-12-15-12 39-12-62-34-72) 39-69-61 47-35-62 52-69-61-39-50-35-52-18, 52-52-35-59-35-70-18-62-26 12-11-68-50-68-15-12-20. 72 57-18-42 15-70-68-47-18-14-35-42 64-11-68-50-69-15-35-70-18 62-52-19-47-68-55-72 52-12-61-72, 35 33-68 52-52-35-59-35-70-12-62-26, 33-12 19-14-33-12 64-11-68-50-69-15-35-34-18 52 55-26-12-20-72 20-12-70-12-14-12, 34-12 57-68 72-11-68-50-68-59-68 14-12-50-12-52-72 52-69-61 52-69-61-26-12-20. 64 39-12-41-18-50-68-55-55-19-20 42-50-18-62-34-18-19-55-62-34-52-35, 42-50-68-62-34 62-34-35-52 35-34-50-18-11-72-34-12-20 50-68-70-69-15-69-48 34-35 48-48 64-35-42-18-62-34-72 52-69-50-72-73-47-18-42. 42-50-68-62-34-18 62-34-35-52-18-70-18 12-11-35-11-69-47 61-12-50-12-15-18, 55-35 72-64-70-69-62-62-69, 11-69-70-19 14-12-70-12-61-19-64-69-52 34-35 62-34-35-52-14-69-52, 33-12-11 64-35-42-18-62-34-18-34-18 39-12-62-68-70-68-55-55-19 52-69-61 64-70-18-42 70-73-61-68-43 34-35 64-52-69-50-69-52, 35 34-35-14-12-59 62-34-50-35-41-55-18-42 42-52-12-50-12-11. 42-50-68-62-34 62-72-39-50-12-52-12-61-59-72-52-35-70-35 70-73-61-18-55-72 52-69-61 61-18-34-18-55-62-34-52-35 (55-35-34-69-70-26-55-18-43 42-50-68-62-34-18-14, 12-61-19-15-55-68-55-18-43 39-69-61 47-35-62 12-11-50-19-61-72 42-50-68-33-68-55-55-19) 69 61-12 64-35-52-68-50-41-68-55-55-19 41-70-19-42-72 (20-12-15-18-70-26-55-18-43 42-50-68-62-34, 64 52-18-11-18-34-18-20 47-18 52-18-50-69-64-35-55-18-20 55-35 55-26-12-20-72 69-20-68-55-68-20 39-12-14-69-43-55-12-15-12).

Для розшифрування повідомлення було прийнято відштовхуватися від слів що складаються з 1 або 2 літер. Таким чином було знайдено слово 48-48, було взято що 48 – це літера ї. Так як ця літера зустрічається всього 5 разів. Після цього було знайдено літеру х в слові їх. Далі аналізуючи текст було знайдено інші літери.

Розшифроване повідомлення: ще задовго до поширення християнства українцi носили натiльнi хрестики, якi вважались оберегом вiд чорних сил (зараз їх можна побачити на згардах – прикрасi, поширеннi на закарпаттi, що складалась з кiлькох низок хрестiв перемежованих коралями чи склянками, першу згарду дiвчинка отримувала на першi iменини, а в наступнi роки згарди дарувались вже парами). хрестом прикрашали посуд. наприклад, глечики з хрестами, виготовленнi на федорову суботу (перша субота великого посту) пiд час вiдправи, вважались оберегом. у цих глечиках зберігали свячену воду, а ще вважалось, що якщо зберiгати в ньому молоко, то це убереже корову вiд вiдьом. з поширенням християнства, хрест став атрибутом релiгiї та її захисту вiруючих. хрести ставили обабiч дороги, на узлiссi, бiля колодязiв та ставкiв, щоб захистити поселення вiд злих людей та звiрiв, а також страшних хвороб. хрест супроводжувала людину вiд дитинства (натiльний хрестик, одягнений пiд час обряду хрещення) i до завершення шляху (могильний хрест, з вибитим чи вирiзаним на ньому iменем покiйного.

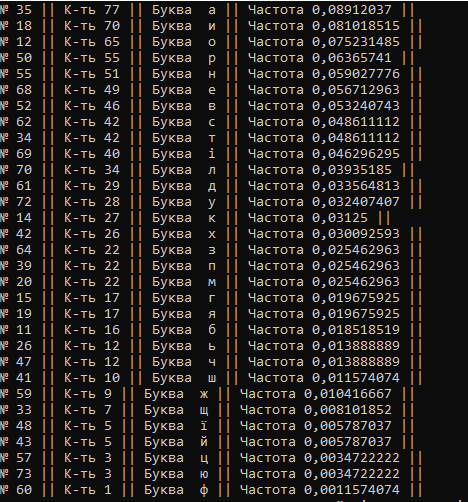


Рисунок 1 – Частота літер