# Шифри складної заміни

## План

1 Шифр Гронсфельда
2 Система шифрування Віженера
3 Шифр “Подвійний квадрат Уітстона”

Шифри складної заміни називають *багатоалфавітними* тому, що для шифрування кожного символа вихідного повідомлення застосовують свій шифр простої заміни.

*Багатоалфавітна* підстановка послідовно й циклічно змінює використовувані алфавіти.

Загальна схема багатоалфавітної підстановки для випадку наведена в таблиці 1.

Таблиця 1

| Вхідний символ: | X0 | X1 | X2 | X3 | X4 | X5 | X6 | X7 | X8 | X9 |
|---|---|---|---|---|---|---|---|---|---|---|
| Алфавіт підстановки: | B0 | B1 | B2 | B3 | B0 | B1 | B2 | B3 | B0 | B1 |

## Шифр Гронсфельда

Шифр складної заміни, який називають шифром Гронсфельда, являє собою модифікацію шифру Цезаря за допомогою числового ключа

Наприклад, застосовуючи як ключ натуральне число 2718, одержимо для вихідного повідомлення ТАЄМНИЙ КЛЮЧ такий шифротекст:

# Шифр Гронсфельда

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |

| Повідомлення | **Т** | **А** | **Є** | **М** | **Н** | **И** | **Й** | | **К** | **Л** | **Ю** | **Ч** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ключ | **2** | **7** | **1** | **8** | **2** | **7** | **1** | | **8** | **2** | **7** | **1** |
| Шифротекст | | | | | | | | | | | | |

# Шифр Гронсфельда

Щоб зашифрувати першу букву повідомлення «Т», використовуючи першу цифру ключа 2, потрібно відрахувати другу літеру від «Т» у алфавіті:

| Т | У | Ф |
|---|---|---|
| | 1 | 2 |

виходить перша літера шифротексту Ф

| Повідомлення | Т | А | Є | М | Н | И | Й | | К | Л | Ю | Ч |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ключ | 2 | 7 | 1 | 8 | 2 | 7 | 1 | | 8 | 2 | 7 | 1 |
| Шифротекст | Ф | Є | | | | | | | | | | |

# Шифр Гронсфельда

Щоб зашифрувати першу букву повідомлення «Т», використовуючи першу цифру ключа 2, потрібно відрахувати другу літеру від «Т» у алфавіті:

| Т | У | Ф |
|---|---|---|
| | 1 | 2 |

виходить перша літера шифротексту Ф

# Шифр Гронсфельда

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |

| Повідомлення | **Т** | **А** | **Є** | **М** | **Н** | **И** | **Й** | | **К** | **Л** | **Ю** | **Ч** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ключ | **2** | **7** | **1** | **8** | **2** | **7** | **1** | | **8** | **2** | **7** | **1** |
| Шифротекст | **Ф** | | | | | | | | | | | |

# Шифр Гронсфельда

| Повідомлення | Т | А | Є | М | Н | И | Й |  | К | Л | Ю | Ч |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ключ | 2 | 7 | 1 | 8 | 2 | 7 | 1 |  | 8 | 2 | 7 | 1 |
| Шифротекст | Ф | Є | Ж | Ф | П | Н | Л |  | Т | Н | Е | Ш |

# Система шифрування Віженера

Таблиця Віженера використовується для зашифрування та розшифрування.

Таблиця має два входи:

- верхній рядок символів, який використовується для зчитування літери вихідного відкритого тексту;

- крайній лівий стовпець ключа, який використовується для зчитування літери ключа.

Таблиця Б.2 – Таблиця Віженера для українського алфавіту

| КЛ | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
| **1** | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А |
| **2** | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б |
| **3** | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В |
| **4** | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г |
| **5** | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ |
| **6** | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д |
| **7** | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е |
| **8** | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є |
| **9** | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж |
| **10** | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З |
| **11** | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И |
| **12** | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І |
| **13** | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї |
| **14** | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й |
| **15** | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К |
| **16** | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л |
| **17** | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |
| **18** | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н |
| **19** | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О |
| **20** | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П |
| **21** | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р |
| **22** | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С |
| **23** | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т |
| **24** | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У |
| **25** | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф |
| **26** | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| **27** | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц |
| **28** | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч |
| **29** | Щ | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш |
| **30** | Ь | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ |
| **31** | Ю | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь |
| **32** | Я | А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю |

# Система шифрування Віженера

Із використанням шифру Віженера виконати шифрування відкритого тексту:

***M*= “БЕЗ КАЛИНИ НЕМА УКРАЇНИ”**

**ключем *Key* =“БАРВІНОК”**

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ***M*** | Б | Е | З | К | А | Л | И | Н | И | Н | Е | М | А | У | К | Р | А | Ї | Н | И |
| ***Key*** | Б | А | Р | В | І | Н | О | К | Б | А | Р | В | І | Н | О | К | Б | А | Р | В |
| ***C*** | В | | | | | | | | | | | | | | | | | | | |

# Система шифрування Віженера

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ***M*** | Б | Е | З | К | А | Л | И | Н | И | Н | Е | М | А | У | К | Р | А | Ї | Н | И |
| ***Key*** | Б | А | Р | В | І | Н | О | К | Б | А | Р | В | І | Н | О | К | Б | А | Р | В |
| ***C*** | В | Е | Щ | М | І | Я | Ш | Ю | І | Н | Ц | О | І | Є | Я | Б | Б | Ї | Ґ | Ї |

У результаті отримаємо шифротекст, що записано блоками по п'ять букв

**ВЕЩМІ ЯШЮІН ЦОІЄЯ ББЇҐЇ.**

# Система шифрування Віженера

| А | Б | В | Г | Ґ | Д | Е | Є | Ж | З | И |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

| І | Ї | Й | К | Л | М | Н | О | П | Р | С |
|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |

| Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

| *M* | Б | Е | З | К | А | Л | И | Н | И | Н | Е | М | А | У | К | Р | А | Ї | Н | И |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 6 | 9 | | | | | | | | | | | | | | | | | |
| *Key* | Б | А | Р | В | І | Н | О | К | Б | А | Р | В | І | Н | О | К | Б | А | Р | В |
| | 1 | 0 | 20 | | | | | | | | | | | | | | | | | |
| | 2 | 6 | 29 | | | | | | | | | | | | | | | | | |
| *C* | В | Е | Щ | | | | | | | | | | | | | | | | | |

# Система шифрування Віженера

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *M* | Б | Е | З | К | А | Л | И | Н | И | Н | Е | М | А | У | К | Р | А | Ї | Н | И |
| *Key* | Б | А | Р | В | І | Н | О | К | Б | А | Р | В | І | Н | О | К | Б | А | Р | В |
| *C* | В | Е | Щ | М | І | Я | Ш | Ю | І | Н | Ц | О | І | Є | Я | Б | Б | Ї | Ґ | Ї |

# Система шифрування Віженера

За допомогою шифру Віженера виконати шифрування відкритого тексту *M* з ключем *Key*

***M* = «*НІЖНО ВПЛІТАЄТЬСЯ В ГОМІН ДНІПРА ДОБРЕ І ЩИРЕ ШЕВЧЕНКІВСЬКЕ СЛОВО*»**

*Key*=«*СКОМАРОВСЬКИЙ*».

# Система шифрування Віженера

| | Н | І | Ж | Н | О | В | П | Л | І | Т | А | Є | Т | Ь | С | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X1= | 17 | 11 | 8 | 17 | 18 | 2 | 19 | 15 | 11 | 23 | 0 | 7 | 22 | 30 | 21 | 32 |
| | С | К | О | М | А | Р | О | В | С | Ь | К | И | Й | С | К | О |
| Y1= | 21 | 14 | 18 | 16 | 0 | 20 | 18 | 2 | 21 | 30 | 14 | 10 | 13 | 21 | 14 | 18 |
| X1+Y1= | 38 | 25 | 26 | 33 | 18 | 22 | 37 | 17 | 32 | 53 | 14 | 17 | 35 | 51 | 35 | 50 |
| mod 33= | 5 | 25 | 26 | 0 | 18 | 22 | 4 | 17 | 32 | 20 | 14 | 17 | 2 | 18 | 2 | 17 |
| C= | Д | Х | Ц | А | О | Т | Ґ | Н | Я | Р | К | Н | В | О | В | Н |

| | В | Г | О | М | І | Н | Д | Н | І | П | Р | А | Д | О | Б | Р | Е |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X1= | 2 | 3 | 18 | 16 | 11 | 17 | 5 | 17 | 11 | 19 | 20 | 0 | 5 | 18 | 1 | 20 | 6 |
| | М | А | Р | О | В | С | Ь | К | И | Й | С | К | О | М | А | Р | О |
| Y1= | 16 | 0 | 20 | 18 | 2 | 21 | 30 | 14 | 10 | 13 | 21 | 14 | 18 | 16 | 0 | 20 | 18 |
| X1+Y1= | 18 | 3 | 38 | 34 | 13 | 38 | 35 | 31 | 21 | 32 | 41 | 14 | 23 | 34 | 1 | 40 | 24 |
| mod 33= | 18 | 3 | 5 | 1 | 13 | 5 | 2 | 31 | 21 | 32 | 8 | 14 | 23 | 1 | 1 | 7 | 24 |
| C= | О | Г | Д | Б | Й | Д | В | Ю | С | Я | Ж | К | У | Б | Б | Є | Ф |

# Система шифрування Віженера

| | І | Щ | И | Р | Е | Ш | Е | В | Ч | Е | Н | К | І | В | С | Ь | К | Е | С | Л | О | В | О |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X1= | 11 | 29 | 10 | 20 | 6 | 28 | 6 | 2 | 27 | 6 | 17 | 14 | 11 | 2 | 21 | 30 | 14 | 6 | 21 | 15 | 18 | 2 | 18 |
| | В | С | Ь | К | И | Й | С | К | О | М | А | Р | О | В | С | Ь | К | И | Й | С | К | О | М |
| Y1= | 2 | 21 | 30 | 14 | 10 | 13 | 21 | 14 | 18 | 16 | 0 | 20 | 18 | 2 | 21 | 30 | 14 | 10 | 13 | 21 | 14 | 18 | 16 |
| X1+Y1= | 13 | 50 | 40 | 34 | 16 | 41 | 27 | 16 | 45 | 22 | 17 | 34 | 29 | 4 | 42 | 60 | 28 | 16 | 34 | 36 | 32 | 20 | 34 |
| mod 33= | 13 | 17 | 7 | 1 | 16 | 8 | 27 | 16 | 12 | 22 | 17 | 1 | 29 | 4 | 9 | 27 | 28 | 16 | 1 | 3 | 32 | 20 | 1 |
| C= | Й | Н | Є | Б | М | Ж | Ч | М | Ї | Т | Н | Б | Щ | Ґ | З | Ч | Ш | М | Б | Г | Я | Р | Б |

## Зашифроване повідомлення:

Д Х Ц А О Т Ґ Н Я Р К Н В О В Н  О Г Д Б Й Д В Ю С Я Ж К У Б Б Є Ф

Й Н Є Б М Ж Ч М Ї Т Н Б Щ Ґ З Ч Ш М Б Г Я Р Б

# Шифр “Подвійний квадрат Уітстона”

Вихідне повідомлення розбивають на біграми. Кожна біграма шифрується окремо.

Першу літеру біграми знаходять у лівій таблиці, а другу – у правій таблиці. Потім будують уявний прямокутник так, щоб літери біграми знаходились у його протилежних вершинах. Інші дві вершини цього прямокутника дають літери біграми шифротексту.

Якщо обидві літери біграми повідомлення *розміщені в одному рядку*, то й літери шифротексту беруть із цього самого рядка. Першу літеру біграми шифротексту беруть із лівої таблиці в стовпці, що відповідає другій літері біграми повідомлення. Друга літера біграми шифротексту береться із правої таблиці в стовпці, що відповідає першій літері біграми повідомлення.

## Шифр “Подвійний квадрат Уітстона”

Наприклад, використовуючи подвійний квадрат Уітстона, зашифрувати повідомлення

**«НЕ ЦУРАЙТЕСЬ ТОГО СЛОВА, ЩО МАТИ СПІВАЛА».**

# Шифр “Подвійний квадрат Уітстона”

Розбиваємо текст на біграми:

**НЕ | _Ц | УР | АЙ | ТЕ | СЬ | _Т | ОГ | О_ | СЛ | ОВ | А, | _Щ | О_ | МА | ТИ | _С | ПІ | ВА | ЛА**

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | І | Р | Ч | Ю | Я | | Ь | Ш | З | А | В | Б |
| И | Б | Ї | С | Ш | , | | Р | Ю | Щ | Ж | Ґ | Г |
| П | З | В | Й | Т | Щ | | С | П | Я | Ч | Є | Д |
| Ц | Ж | О | Г | К | У | | Й | О | Т | _ | Е | Ц |
| _ | Х | Є | Н | Ґ | Л | | Ї | К | Н | У | Ф | Х |
| . | Ь | Ф | Д | Е | М | | І | И | Л | М | , | . |

# Шифр “Подвійний квадрат Уітстона”

Відповідно до алгоритму виконаємо відповідні перетворення:

| | | | | |
|---|---|---|---|---|
| НЕ→ФГ | ТЕ →ЄК | О_ →ГТ | _Щ→НИ | _С→ЇП |
| _Ц→ХЦ | СЬ→РЧ | СЛ →ЩД | О_→ГТ | ПІ→С. |
| УР→Й, | _Т→НЦ | ОВ→ЕР | МА→МЯ | ВА→ЧР |
| АЙ→ЬЦ | ОГ→ЦЇ | А, →В. | ТИ→ПЕ | ЛА→УЯ |

Отже, маємо шифротекст, записаний блоками по 5 символів:

**ФГХЦЙ ,ЬЦЄК РЧНЦЦ ЇГТЩД**
**ЕРВ.Н ИГТМЯ ПЕЇПС .ЧРУЯ .**

# Шифр “Подвійний квадрат Уітстона”

Розшифрування виконується так само, як і шифрування. Єдина відмінність полягає в тому, **що при розшифруванні таблиці міняються місцями** (рис. 1).

Шифрування методом подвійного квадрата досить стійкий до розкриття та простий у застосуванні шифр

| | | | | | |
|---|---|---|---|---|---|
| Ь | Ш | З | А | В | Б |
| Р | Ю | Щ | Ж | Ґ | Г |
| С | П | Я | Ч | Є | Д |
| Й | О | Т | _ | Е | Ц |
| Ї | К | Н | У | Ф | Х |
| І | И | Л | М | , | . |

| | | | | | |
|---|---|---|---|---|---|
| А | І | Р | Ч | Ю | Я |
| И | Б | Ї | С | Ш | , |
| П | З | В | Й | Т | Щ |
| Ц | Ж | О | Г | К | У |
| _ | Х | Є | Н | Ґ | Л |
| . | Ь | Ф | Д | Е | М |

Рисунок 1 – Таблиці для розшифрування в шифрі “Подвійний квадрат Уітстона”

# Шифр “Подвійний квадрат Уітстона”

Розшифруйте наступне слово:

**ФГХЦЙ ,ЬЦЄК РЧ**

| | | | | | |
|---|---|---|---|---|---|
| Ь | Ш | З | А | В | Б |
| Р | Ю | Щ | Ж | Ґ | Г |
| С | П | Я | Ч | Є | Д |
| Й | О | Т | _ | Е | Ц |
| Ї | К | Н | У | Ф | Х |
| І | И | Л | М | , | . |

| | | | | | |
|---|---|---|---|---|---|
| А | І | Р | Ч | Ю | Я |
| И | Б | Ї | С | Ш | , |
| П | З | В | Й | Т | Щ |
| Ц | Ж | О | Г | К | У |
| _ | Х | Є | Н | Ґ | Л |
| . | Ь | Ф | Д | Е | М |

Шифрування методом подвійного квадрата досить стійкий до розкриття та простий у застосуванні шифр