

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ  
ІМЕНИ СЕМЕНА КУЗНЕЦЯ

ЗВІТ  
о виконанні лабораторної роботи №2  
з дисципліни «Захист інформації»  
за темою «Захист особистих повідомлень»

Виконав:  
Студент 4 курсу  
групи 6.04.122.010.22.1  
факультету ІТ  
Холоша Сергій

Перевірив:  
Професор кафедри  
кібербезпеки та ІТ  
Тютюнник В. В.

## Порядок виконання практичної частини

### Крок 1. Дослідження готових інструментів шифрування

- 1) Перейти на веб-сайт Cryptii ([cryptii.com/pipes/caesar-cipher](http://cryptii.com/pipes/caesar-cipher));
- 2) Спробувати зашифрувати власне ім'я за допомогою шифру Цезаря зі зсувом 7;
- 3) Перейти на сторінку шифру Віженера ([cryptii.com/pipes/vigenere-cipher](http://cryptii.com/pipes/vigenere-cipher)) та протестувати з ключем на основі власного прізвища;
- 4) Зафіксувати результати та зрозуміти принципи роботи алгоритмів.

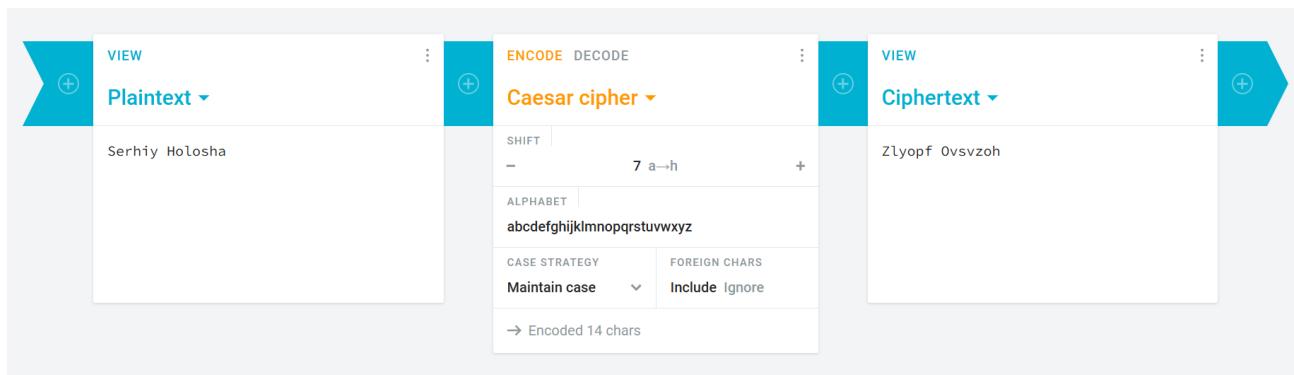


Рис. 1. Ім'я зашифроване шифром Цезаря

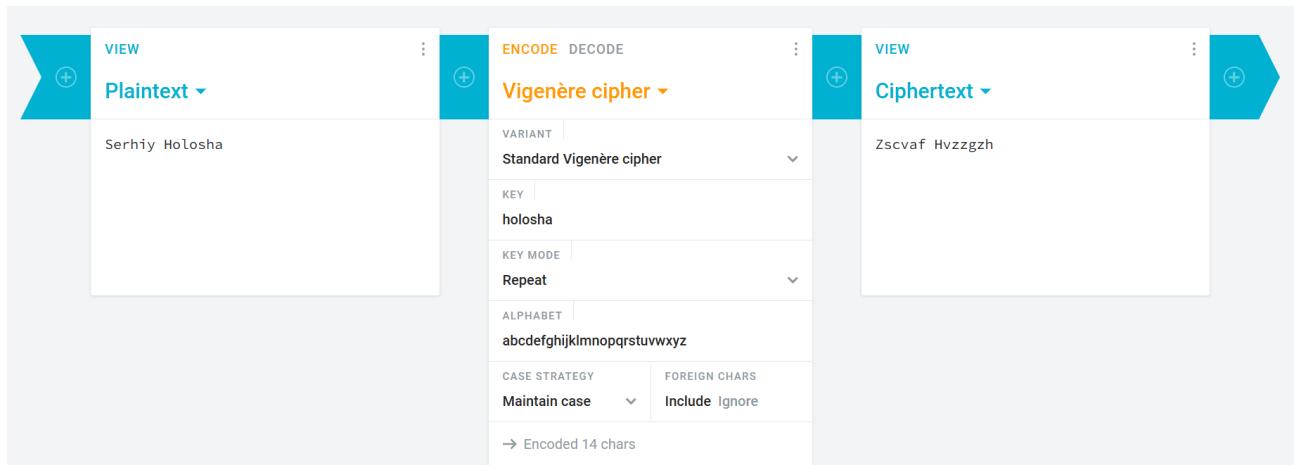


Рис. 2. Ім'я зашифроване шифром Віженера

## Крок 2. Порівняльне дослідження класичних шифрів

- 1) Обрати власний текст для шифрування (мінімум 20–30 символів) – це може бути цитата, вірш, особисте повідомлення тощо;
- 2) Зшифрувати обраний текст за допомогою трьох різних алгоритмів з сайту Cryptii:
  - Шифр Цезаря (Caesar cipher);
  - Шифр Віженера (Vigenère cipher);
  - Один додатковий шифр на вибір (ROT13, Affine, Atbash тощо);
- 3) Для кожного шифру використати ключ на основі власних даних (ім'я, дата народження);
- 4) Провести короткий порівняльний аналіз:
  - Який шифр дає найбільш “нечитабельний” результат?
  - Який найлегше налаштувати?
  - Чи видно якісь закономірності у зашифрованому тексті?
- 5) 2.5. Задокументувати результати та зробити висновки.

The screenshot shows the Cryptii interface with three main sections: Plaintext, Caesar cipher settings, and Ciphertext.

**Plaintext:** Serhii is a Ukrainian masculine given name that comes from the ancient Roman generic name Sergius.

**Caesar cipher settings:** SHIFT: 7 (a→h), ALPHABET: abcdefghijklmnopqrstuvwxyz, CASE STRATEGY: Maintain case, FOREIGN CHARS: Include, IGNORE: Ignore. Status: Encoded 98 chars.

**Ciphertext:** Zlyopp pz h Bryhpuphu thzjbspul npclu uhtl aoha jvtlz myvt aol hujplua Yvthu nlulypj uhtl Zlynpbz.

Рис. 3. Шифр Цезаря

The screenshot shows the Cryptii interface with three main sections: Plaintext, Vigenère cipher settings, and Ciphertext.

**Plaintext:** Serhii is a Ukrainian masculine given name that comes from the ancient Roman generic name Sergius.

**Vigenère cipher settings:** VARIANT: Standard Vigenère cipher, KEY: holosha, KEY MODE: Repeat, ALPHABET: abcdefghijklmnopqrstuvwxyz, CASE STRATEGY: Maintain case, FOREIGN CHARS: Include, IGNORE: Ignore. Status: Encoded 98 chars.

**Ciphertext:** Zscvap iz o Fyjhieulb ehsjiwwfl gpjpb fhml hsol jotsd tjvm avp ofjilbe Fgtau upbwijj blaw Zeyutik.

Рис. 4. Шифр Віженера

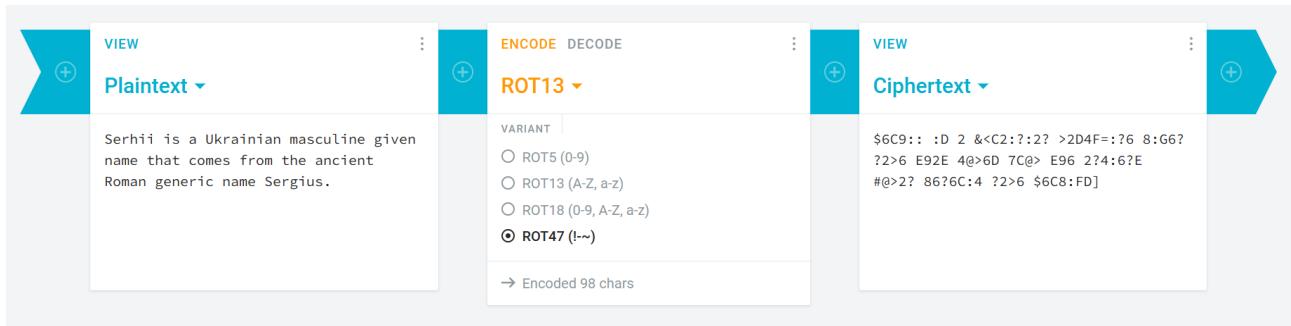


Рис. 5. Шифр ROT47

Нечитабельність результату: ROT47 дає найбільш нечитабельний результат, оскільки використовує розширений набір ASCII-символів (!, ~, цифри, спецсимволи). Vigenère та ROT13 залишають текст у читабельному алфавітному вигляді, що полегшує частотний аналіз.

Налаштування: ROT13 найпростіший — взагалі не потребує ключа, це фіксоване зміщення на 13 позицій. Vigenère вимагає ключа ("holosha") та вибору режиму повторення, що робить його складнішим у налаштуванні, але й безпечнішим. ROT47 також без ключа, але охоплює більший діапазон символів.

Закономірності: У Vigenère помітна періодичність — слово "Serhii" перетворюється на "Zscvap", де однакові літери (два "i") дають різні результати через циклічний ключ. ROT47 змішує літери з цифрами та символами, що маскує структуру тексту.

### **Крок 3. Простий криптоаналіз та обмін повідомленнями**

- 1) Спробувати “зломати” шифр Цезаря методом brute force:
  - Перебрати всі можливі зсуви (1–25) для власного зашифрованого тексту;
  - Визначити, який зсув дає читабельний результат;
- 2) Обмінятися одним зашифрованим повідомленням з одногрупником (без передачі ключа);
- 3) Спробувати розшифрувати повідомлення одногрупника будь-яким способом;
- 4) Обговорити, який метод виявився найлегшим для злому.

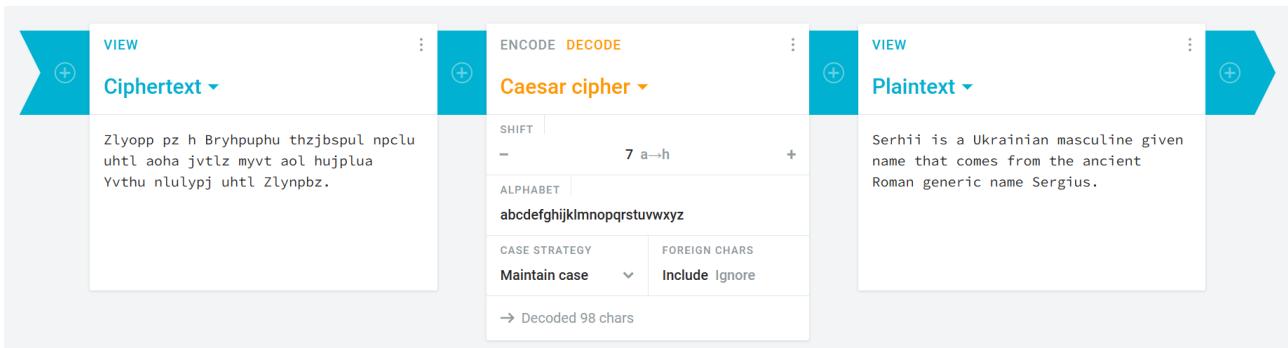


Рис. 6. Розшифроване повідомлення шифром Цезаря

Для шифру Цезаря метод brute force за стандартних умов (стандартної абетки) є найбільш простим та ефективним, адже необхідно перевірити всього 25 налаштувань які можна досить швидко прокрутити доки не отримаєш результат схожий на реальний текст.

### Технічне завдання

**Завдання:** Реалізувати програму для демонстрації та порівняння двох класичних алгоритмів шифрування.

### Обов'язкові функціональні вимоги:

- реалізація двох різних класичних алгоритмів шифрування (наприклад, Цезарь та Віженер);
- генерація ключів на основі персональних даних для кожного алгоритму;
- функції шифрування та розшифрування для обох методів;
- простий порівняльний аналіз результатів;
- демонстрація роботи на власному тексті.

ДЕМОНСТРАЦІЯ РОБОТИ ШИФРІВ

---

Вихідний текст: Захист інформації – цікава дисципліна

--- ШИФР ЦЕЗАРЯ (зсув = 19) ---

Зашифровано: шпіщєж ьги'евлію – ївапсп фщєїшдбъгп

Розшифровано: захист інформації – цікава дисципліна

--- ШИФР ВІЖЕНЕРА (ключ = 'Холоша') ---

Зашифровано: боєштм гвеглмхіць – сіеоно аийіх'гіізо

Розшифровано: захист інформації – цікава дисципліна

ПОРІВНЯЛЬНИЙ АНАЛІЗ ШИФРІВ

---

Параметр	Цезар	Віженер
Ключ	19	Холоша
Довжина ключа	1	6
Довжина шифротексту	37	37
Унікальні символи	19	21
Складність злому	Дуже низька	Низька
Можливі ключі	33	$\infty$

Рис. 7. Результат виконання програми

Посилання на GitHub: [zahist-informaciji/lab2 at main · serhiikholosha57/zahist-informaciji](https://github.com/serhiikholosha57/zahist-informaciji)

Висновок: в ході лабораторної роботи я навчився створювати системи захищеного листування з використанням класичних методів шифрування