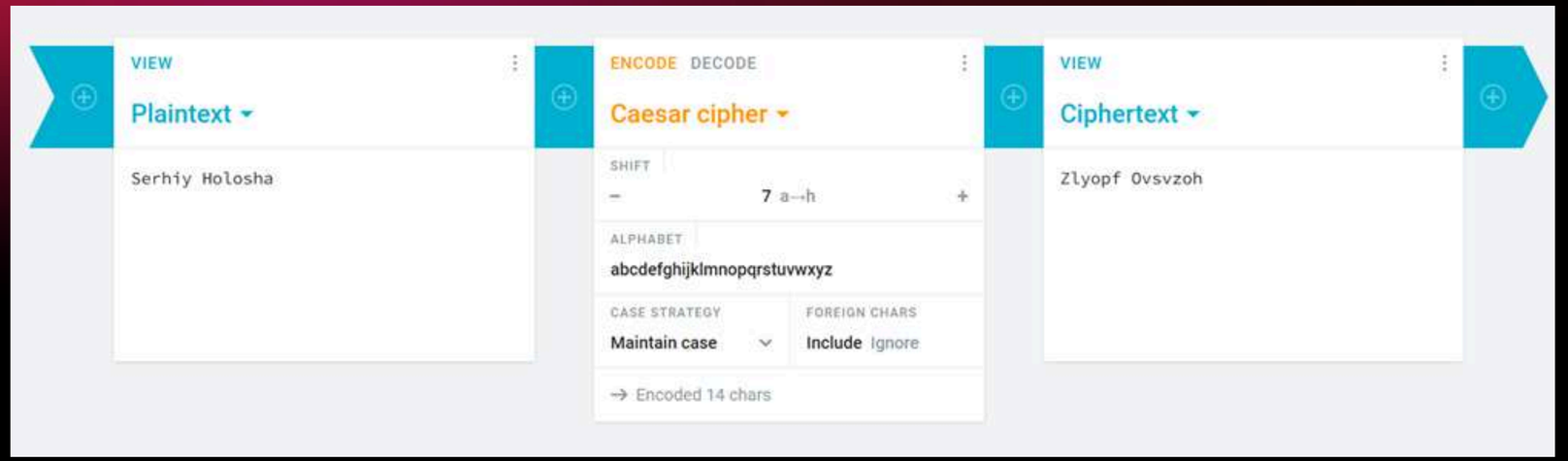
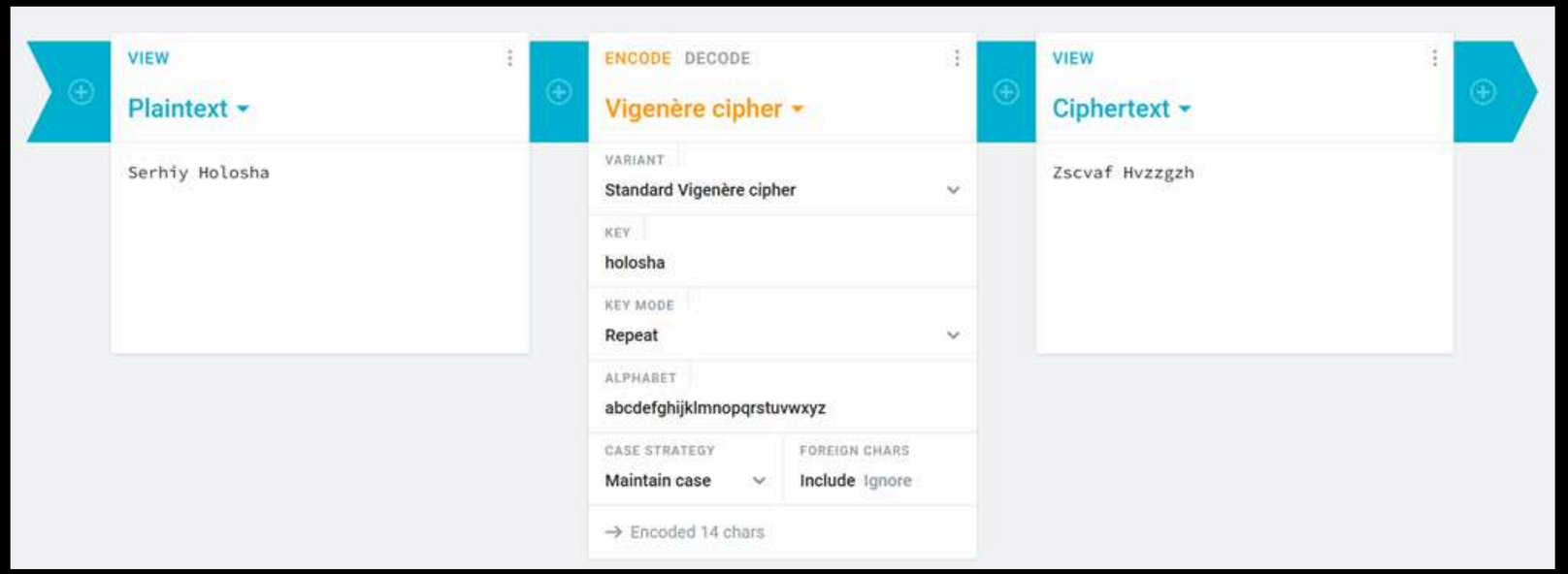
ЛАБОРАТОРНА РОБОТА 2

Захист особистих повідомлень

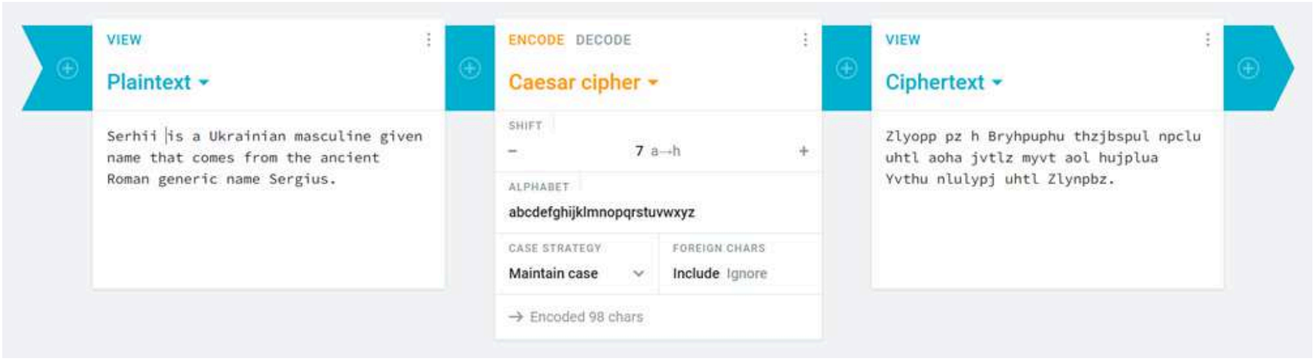
Виконав Холоша Сергій

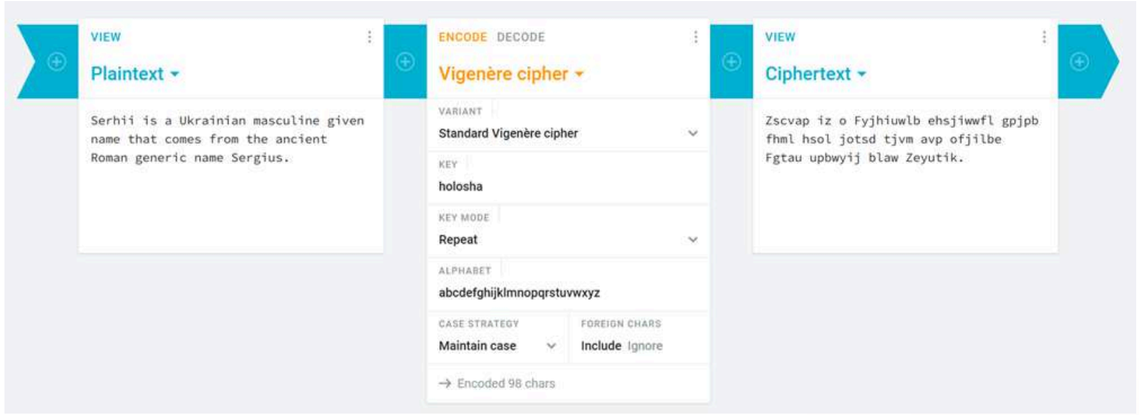
Дослідження готових інструментів шифрування

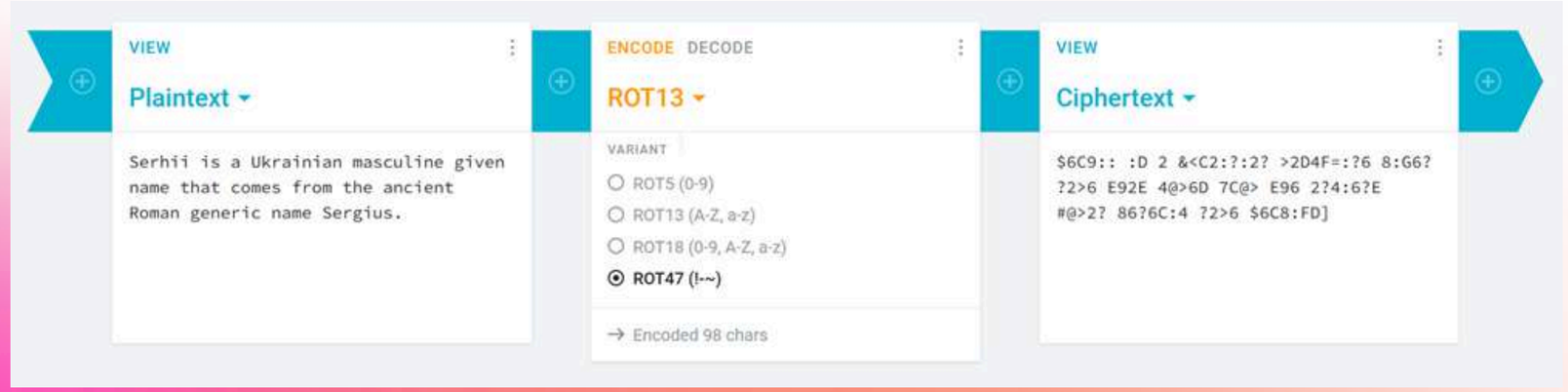

VIEW
Plaintext
Serhiy Holosha
ENCODE DECODE
Caesar cipher
SHIFT
7 a→h
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
Encoded 14 chars
VIEW
Ciphertext
Zlyopf Ovsvzoh


VIEW
Plaintext
Serhiy Holosha
ENCODE DECODE
Vigenère cipher
VARIANT
Standard Vigenère cipher
KEY
holosha
KEY MODE
Repeat
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
Encoded 14 chars
VIEW
Ciphertext
Zscvaf Hvzzgzh

Порівняльне дослідження класичних шифрів

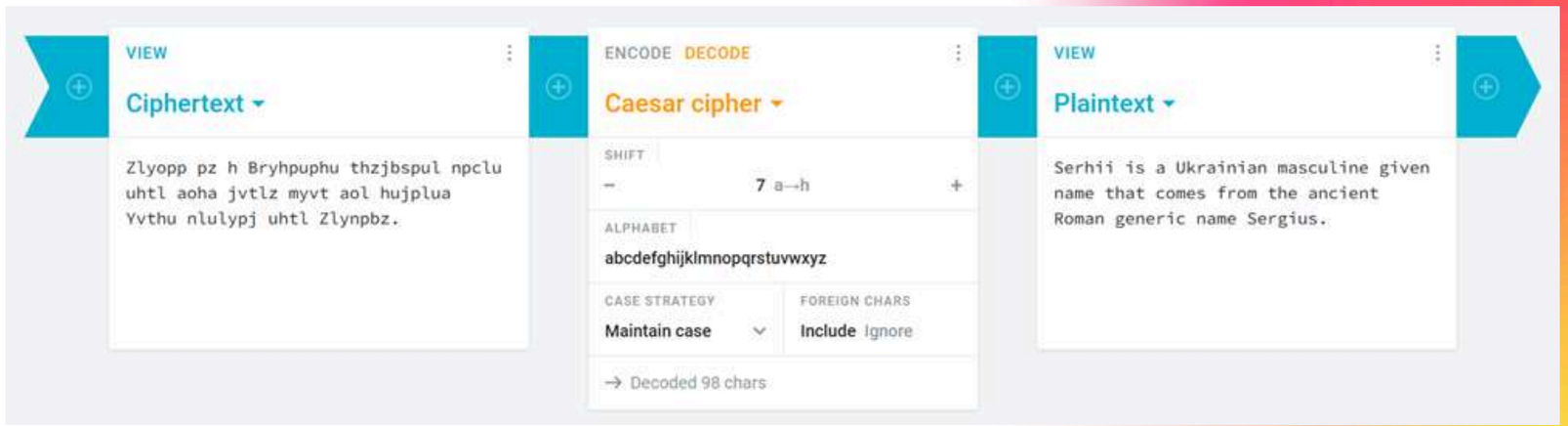

VIEW
Plaintext
Serhii is a Ukrainian masculine given name that comes from the ancient Roman generic name Sergius.
ENCODE DECODE
Caesar cipher
SHIFT
7 a→h
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Encoded 98 chars
VIEW
Ciphertext
Zlyopp pz h Bryhpuphu thzjbspul npclu uhtl aoha jvtlz myvt aol hujplua Yvthu nlulypj uhtl Zlynpbz.


VIEW
Plaintext
Serhii is a Ukrainian masculine given name that comes from the ancient Roman generic name Sergius.
ENCODE DECODE
Vigenère cipher
VARIANT
Standard Vigenère cipher
KEY
holosha
KEY MODE
Repeat
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Encoded 98 chars
VIEW
Ciphertext
Zscvap iz o Fyjhiuwlb ehsjiwwfl gpjpb fhml hsol jotsd tjvm avp ofjilbe Fgtau upbwyij blaw Zeyutik.


VIEW
Plaintext
Serhii is a Ukrainian masculine given name that comes from the ancient Roman generic name Sergius.
ENCODE DECODE
ROT13
VARIANT
ROT5 (0-9)
ROT13 (A-Z, a-z)
ROT18 (0-9, A-Z, a-z)
ROT47 (!~~)
→ Encoded 98 chars
VIEW
Ciphertext
$6C9:: :D 2 &<C2:?:2? >2D4F=:?6 8:G6? ?2>6 E92E 4@>6D 7C@> E96 2?4:6?E #@>2? 86?6C:4 ?2>6 $6C8:FD]

- 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.

Простий криптоаналіз та обмін повідомленнями



- 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

```
ДЕМОНСТРАЦІЯ РОБОТИ ШИФРІВ
======================================================================

Вихідний текст: Захист інформації – цікава дисципліна

--- ШИФР ЦЕЗАРЯ (зсув = 19) ---
Зашифровано: шпіщєж ьгиґевпїью – їьапсп фщєїшдбьгп
Розшифровано: захист інформації – цікава дисципліна

--- ШИФР ВІЖЕНЕРА (ключ = 'Холоша') ---
Зашифровано: боєшмт гвеглмхіць – сіеоно аийіхґиізо
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                   ∞
```

Дякую за увагу!

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