Захист інформації

Лабораторна робота 2

За темою “Захист особистих повідомлень”

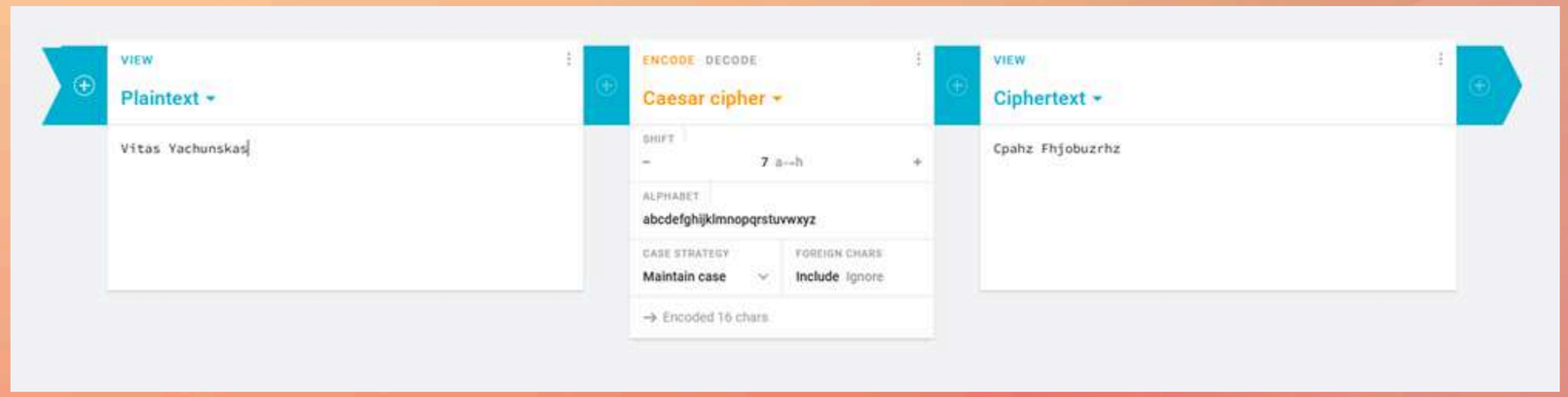
Виконав:
Студент 4 курсу
групи 6.04.122.010.22.1
факультету IT
Ячунскас Вітас

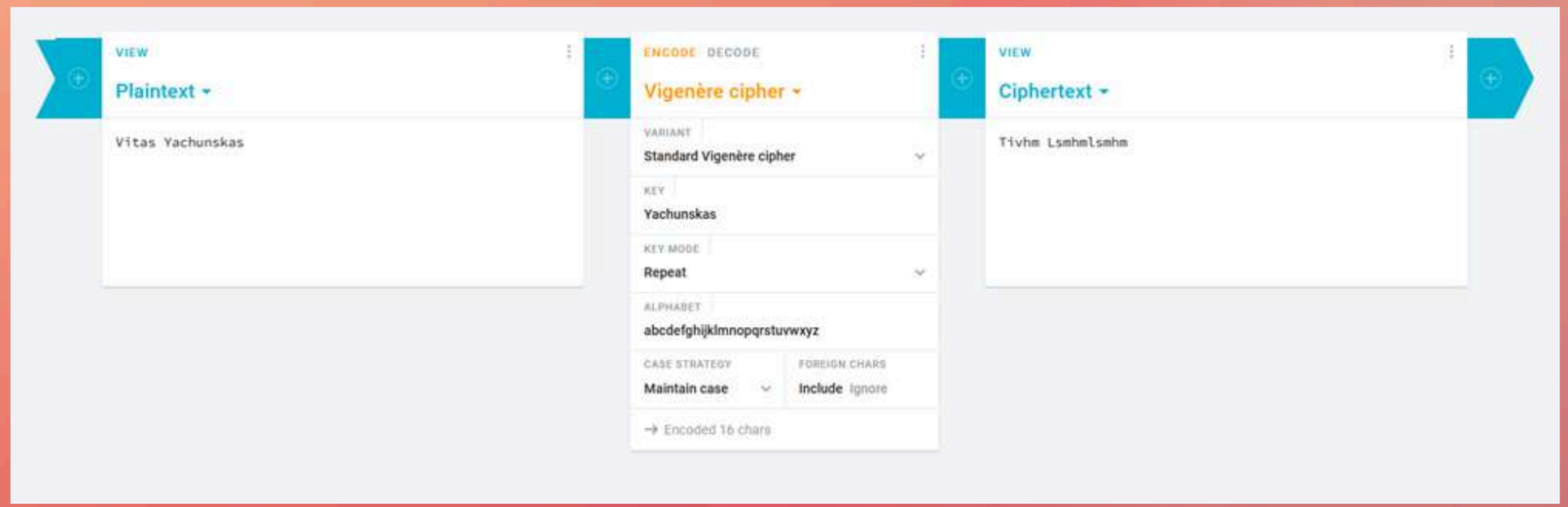
Вступ та постановка завдання

В цій лабораторній роботі завдання полягає в наступному:

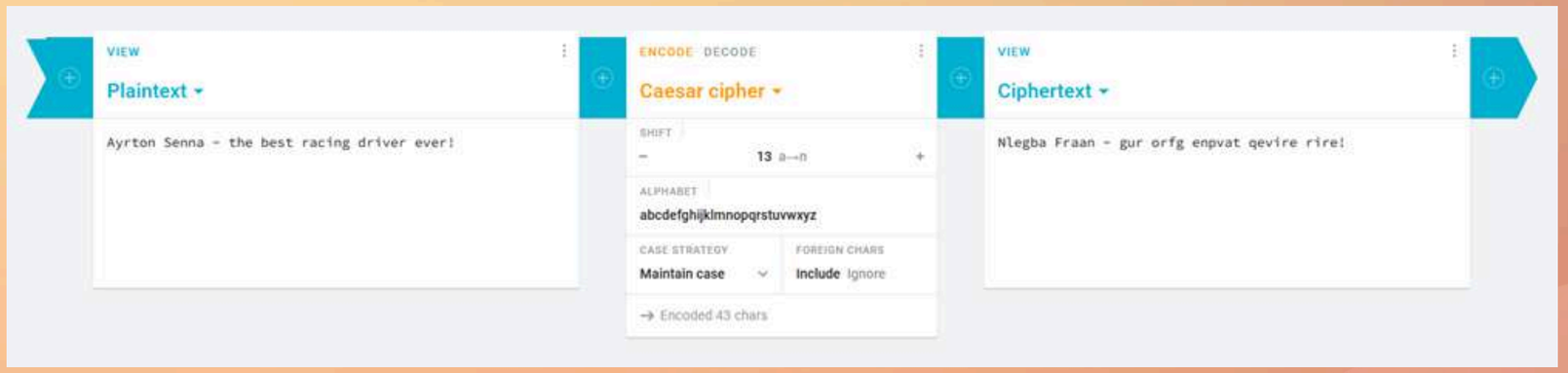
- Використати шифр Цезаря та Віженера
- Проаналізувати їх стійкість
- Зламати зашифроване повідомлення одногрупника
- Програмно реалізувати шифри Віженера та Цезаря та зробити їх порівняльний аналіз

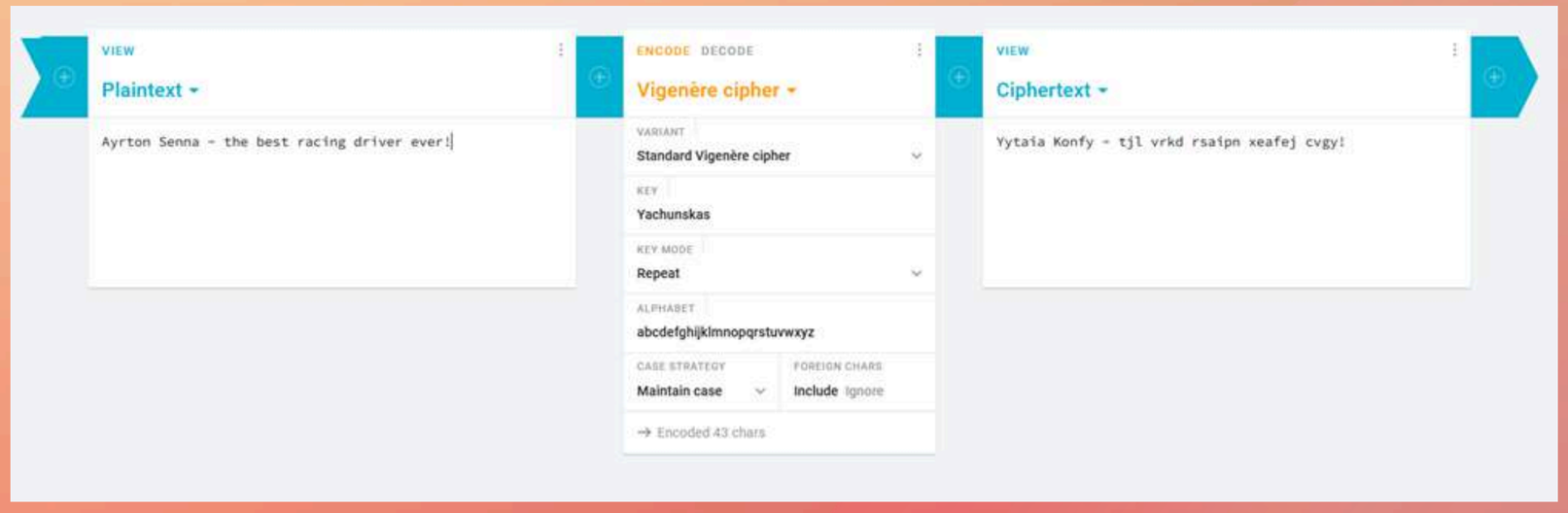
Дослідження готових інструментів шифрування

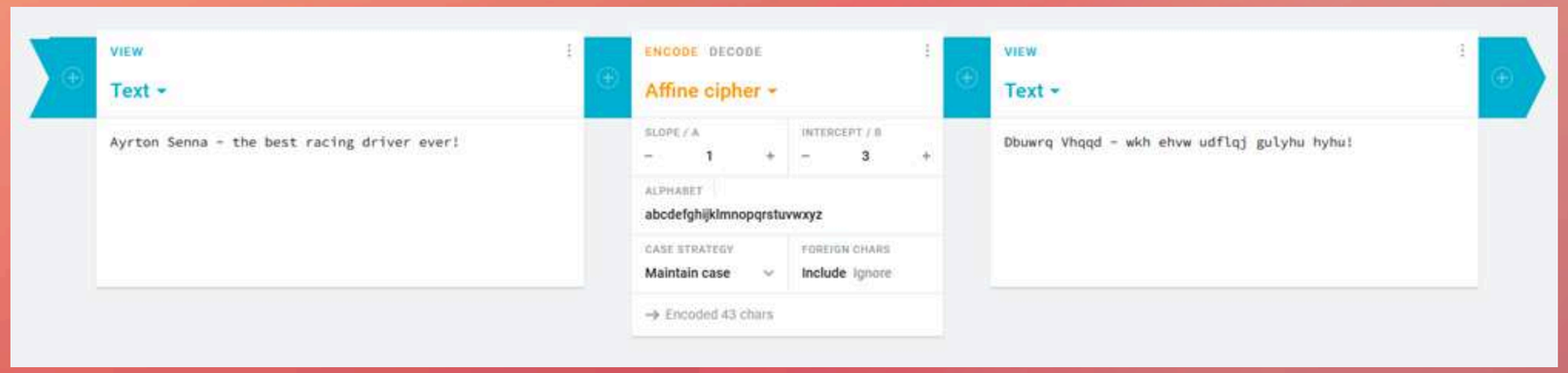




Порівняльне дослідження класичних шифрів


VIEW
Plaintext
Ayrton Senna - the best racing driver ever!
ENCODE DECODE
Caesar cipher
SHIFT
13 a→n
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Encoded 43 chars
VIEW
Ciphertext
Nlegba Fraan - gur orfg enpvat qevire rire!

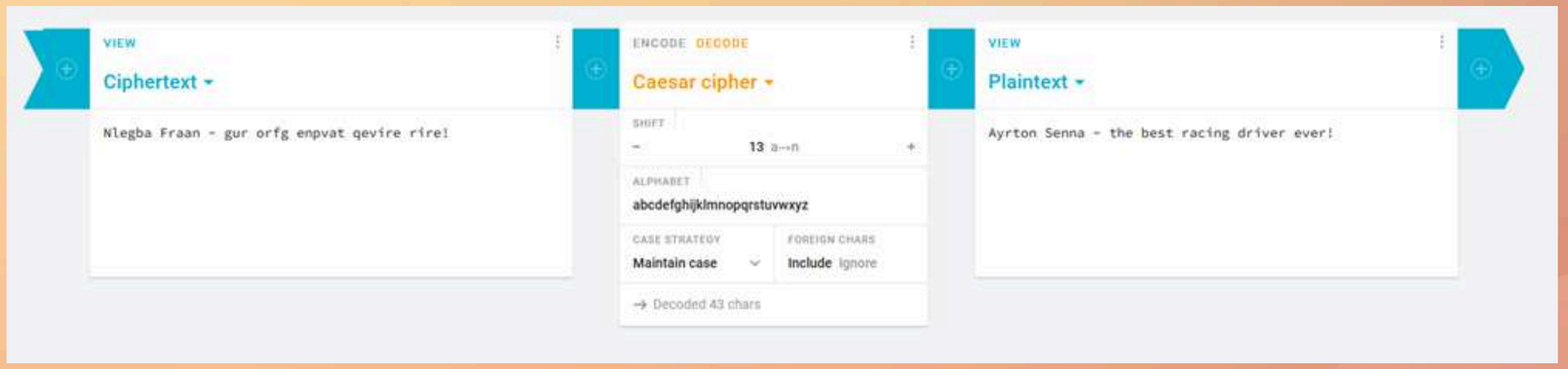

VIEW
Plaintext
Ayrton Senna - the best racing driver ever!
ENCODE DECODE
Vigenère cipher
VARIANT
Standard Vigenère cipher
KEY
Yachunskas
KEY MODE
Repeat
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Encoded 43 chars
VIEW
Ciphertext
Yytaia Konfy - tjl vrkd rsaipn xeafej cvgy!

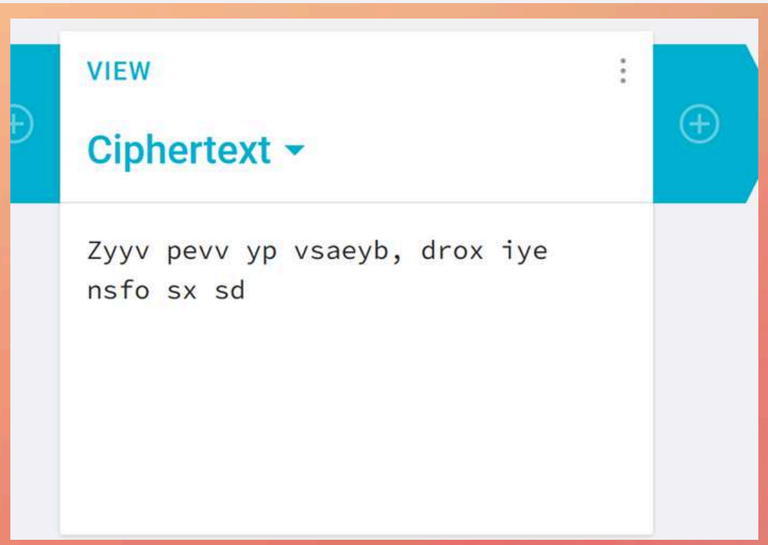

VIEW
Text
Ayrton Senna - the best racing driver ever!
ENCODE DECODE
Affine cipher
SLOPE / A
1
INTERCEPT / B
3
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Encoded 43 chars
VIEW
Text
Dbuwrq Vhqqd - wkh ehvw udflqj gulyhu hyhu!

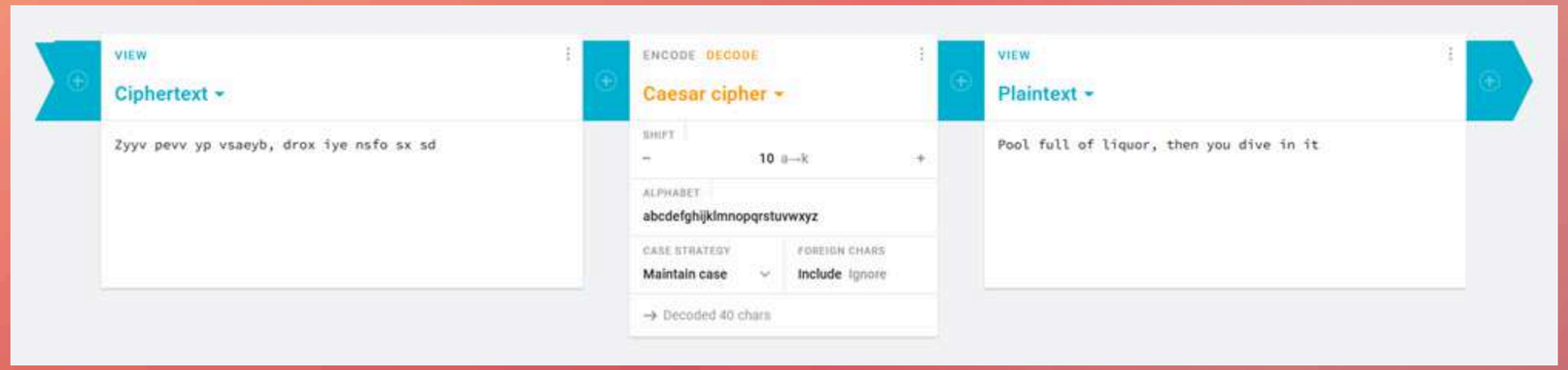
Порівняльне дослідження класичних шифрів

Кожен шифр дає приблизно схожий «нечитабельний» результат, втім жоден шифр за базових налаштувань не замінив символи «-» та «!».
Найлегший для налаштування – шифр Цезаря, адже в ньому налаштовуються в основному зсув та абетка.
Найбільша закономірність яку видно мені - «-» та «!» які трапляються в одному й тому місці. З цих символів знаючи шифр зробити припущення щодо, наприклад, слова після дефісу та працювати з ним.

Простий криптоаналіз та обмін повідомленнями


VIEW
Ciphertext
Nlegba Fraan - gur orfg enpvat qevire rire!
ENCODE DECODE
Caesar cipher
SHIFT
13 a→n
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Decoded 43 chars
VIEW
Plaintext
Ayrton Senna - the best racing driver ever!


VIEW
Ciphertext
Zyyv pevv yp vsaeyb, drox iye nsfo sx sd


VIEW
Ciphertext
Zyyv pevv yp vsaeyb, drox iye nsfo sx sd
ENCODE DECODE
Caesar cipher
SHIFT
10 a→k
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Decoded 40 chars
VIEW
Plaintext
Pool full of liquor, then you dive in it

Простий криптоаналіз та обмін повідомленнями

Отже, для шифру Цезаря найпростішим методом зламу в більшості випадків є метод повного перебору, тобто “brute force”. Втім, якщо трохи змінити абетку можна збити людину що намагається зламати повідомлення з пантелику та сильно ускладнити задачу.

Демонстрація роботи програми та технічне рішення

```
================================================================
                    ПРОГРАМА ШИФРУВАННЯ
================================================================

1. Шифрування методом Цезаря
2. Розшифрування методом Цезаря
3. Шифрування методом Віженера
4. Розшифрування методом Віженера
5. Порівняльний аналіз обох методів
0. Вихід

----------------------------------------------------------------

Виберіть опцію (0-5):
```

```
Виберіть опцію (0-5): 1

Введіть текст для шифрування: Vitas Yachunskas
Введіть ключ (зсув, число): 13

Зашифрований текст: Ivgnf Lnpuhafxnf

Натисніть Enter для продовження...
```

```
Виберіть опцію (0-5): 3

Введіть текст для шифрування: Vitas Yachunskas
Введіть ключове слово: Yachunskas

ашифрований текст: Tivhm Lsmhmlsmhm

Натисніть Enter для продовження...
```

```
Виберіть опцію (0-5): 2

Введіть текст для розшифрування: Ivgnf Lnpuhafxnf
Введіть ключ (зсув, число): 13

Розшифрований текст: Vitas Yachunskas

Натисніть Enter для продовження...
```

```
Виберіть опцію (0-5): 4

Введіть текст для розшифрування: Tivhm Lsmhmlsmhm
Введіть ключове слово: Yachunskas

Розшифрований текст: Vitas Yachunskas

Натисніть Enter для продовження...
```

```
----------------------------------------------------------------

Виберіть опцію (0-5): 5

Введіть текст для аналізу: Vitas Yachunskas
Введіть зсув для шифру Цезаря: 13
Введіть ключ для шифру Віженера: Yachunskas

================================================================
ПОРІВНЯЛЬНИЙ АНАЛІЗ РЕЗУЛЬТАТІВ ШИФРУВАННЯ
================================================================

Оригінальний текст:
   Vitas Yachunskas

Шифр Цезаря (зсув 13):
   Ivgnf Lnpuhafxnf

Шифр Віженера (ключ 'Yachunskas'):
   Tivhm Lsmhmlsmhm

СТАТИСТИКА:
   Довжина оригіналу: 16 символів
   Літер в оригіналі: 15

   Шифр Цезаря - найчастіші літери:
      N: 3 разів (20.0%)
      F: 3 разів (20.0%)
      I: 1 разів (6.7%)

   Шифр Віженера - найчастіші літери:
      M: 5 разів (33.3%)
      H: 3 разів (20.0%)
      L: 2 разів (13.3%)

ОЦІНКА СТІЙКОСТІ:
   Шифр Цезаря:
      - Можливих ключів: 25
      - Легко зламати методом перебору
      - Зберігає частотність літер

   Шифр Віженера:
      - Довжина ключа: 10
      - Можливих комбінацій: 26^10
      - Складніший для криптоаналізу
      - Розмиває частотність літер

================================================================

Натисніть Enter для продовження...
```

Висновки

Отже, в ході лабораторної роботи було опрацьовано класичні методи шифрування та розроблено програму для шифрування з використанням класичних методів шифрування