



Міністерство освіти і науки, молоді та спорту України

Національний технічний університет України

“Київський політехнічний інститут”

Фізико-Технічний інститут

# **КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

## **за семестровий курс предмету**

## **«Симетрична криптографія»**

**Роботу виконали:**

Студенти групи ФІ-03

Починок Юрій

**Приймав:**

Чорний Олег Миколайович

Київ-2023

# КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

## Криптоаналіз шифру Віженера

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини  $r = 2, 3, 4, 5$ , а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності  $I$  для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:
  - визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь  $D$  (на вибір);
  - визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;
  - визначити символи ключа за допомогою функції  $(M_i(g))$  ;
  - розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

## Хід роботи

- Труднощі: ненавиджу python і всі ці позначення в методичці. Більше труднощів не виникало.
- Таблиця порівнянь індексу відповідності:

Розмір ключа	I_r (BT)	I_r (ШТ)
r = 2	0.0465521153845514 86	0.0338280275379635 7
r = 3	0.0388174618442032 1	0.0338280275379635 7
r = 4	0.0352405168263600 15	0.0338280275379635 7
r = 5	0.0405438046189304 3	0.0338280275379635 7
r = 10	0.0341869693015986 6	0.0338280275379635 7
r = 11	0.0383340459979314 4	0.0338280275379635 7

- Значення I\_r(пошук розміру ключа відповідно до методичних вказівок):

```
0.0199224 0
0.0214691 1
0.0199859 2
0.0215245 3
0.0198609 4
0.0128192 5
0.0198478 6
0.0214635 7
0.0200349 8
0.0215068 9
0.0199012 10
0.0215627 11
0.0018895 12
0.0216649 13
0.0195957 14
0.0214411 15
0.0198032 16
0.0212205 17
0.0200511 18
0.0129847 19
0.0201309 20
0.0215423 21
0.0197462 22
0.0213874 23
...
0.0202192 28
0.0216092 29
```

Розмір ключа:  $12+2 = 14$

- Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови:

**“посняковандрей”**

- Значення ключа, одержане із використанням функції  $M_i(g)$ :

**“посняковандрей”**

6. Результат для обох ключів однаковий :

*наберегусевернойдвиныпримернополсотневерстотвпаденияеевганд  
викбелоеморесредьгустойтайгизатеряласьмихайлоархангельскаяобительо  
днаизсамыхдальнихвновгородскойземлееслинесчитатьскиитупустозерског  
оострогачтонапечоререкенудотогоскитаещедобратсьнадоакздешнемум  
онастырюпожалуйстахочешьчерезвологдуданотомпосухоневвеликийустю  
гатамидодвинырукойподатьзнайплывипотечениюахочешьнапрямикчерез  
ладогусвирьонегуд*

7. Висновки: З підібраних розмірів ключів правильних висновків зробити не вдалось, довелось все-одно шукати більш сучасним способом. Розшифрувати текст вдалось успішно, ура.