

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 No2

Криптоаналіз шифру Віженера

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових 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(Mi(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 (ВТ) | I\_r (ШТ) |
| r = 2 | 0.046552115384551486 | 0.03382802753796357 |
| r = 3 | 0.03881746184420321 | 0.03382802753796357 |
| r = 4 | 0.035240516826360015 | 0.03382802753796357 |
| r = 5 | 0.04054380461893043 | 0.03382802753796357 |
| r = 10 | 0.03418696930159866 | 0.03382802753796357 |
| r = 11 | 0.03833404599793144 | 0.03382802753796357 |

* Значення I\_r(пошук розміру ключа відповідно до методичниз вказівок):



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 :

***наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгустойтайгизатеряласьмихайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслинесчитатьскитупустозерскогоострогачтонапечоререкенудотогоскитаещедобратьсянадоакздешнемумонастырюпожалуйстахочешьчерезвологдудапотомпосухоневвеликийустюгатамидодвинырукойподатьзнайплывипотечениюахочешьнапрямикчерезладогусвирьонегуд***

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