

Міністерство освіти і науки України  
Національний технічний університет України  
Київський політехнічний інститут імені Ігоря Сікорського  
Навчально-науковий фізико-технічний інститут

Симетрична криптографія  
Комп'ютерний практикум №2

Криптоаналіз шифру Віженера

Виконали:  
Медведцький Костянтин ФІ-04  
Сковрон Роман ФІ-04

Київ 2023

## 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.

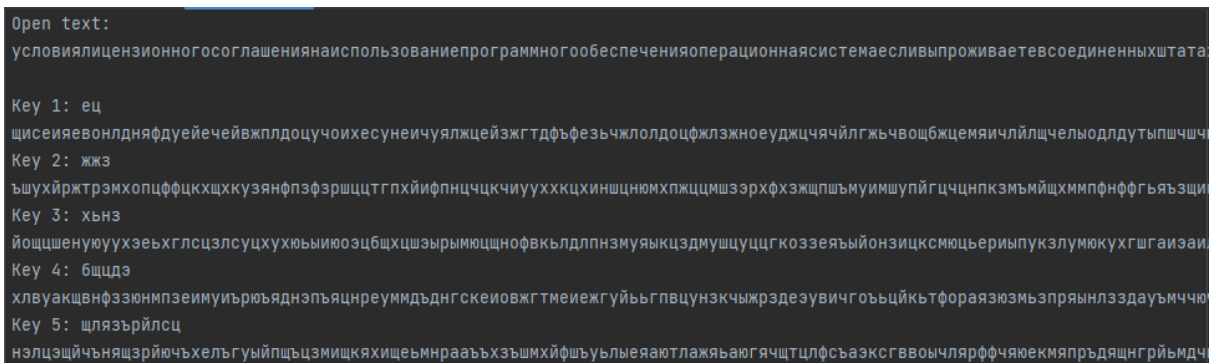
2. Підрахувати індекси відповідності  $I_r$  для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифротекст (згідно свого номеру варіанта). Зокрема, необхідно:

- визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь  $D_r$  (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

1. В якості відкритого тексту було обрано ліцензійну угоду Windows. Результати шифрування відкритого тексту ключами довжини 2, 3, 4, 5 та 10.



Open text:  
условия лицензионного соглашения на использование программного обеспечения операционной системы, если вы проживаете в соединенных штатах;  
Key 1: ец  
щисеияевонлднфдуйечейвжплдоуцхоихесунеичуялжейзжгтдфьезьжлолдоцфлжжноеуджцчйлгжьчвошбжцемяичлйлщчелыодлдутыпшчч  
Key 2: жжэ  
ъшухйржтрэмхоцфцкххкузянфлэфрщцтгпхйифпнцчкчиуухккхинщнхмхпжццишзэрхфхэжщпъмуимшупйгцчнпкзмьмйщхммпнфгьяэци  
Key 3: хьнэ  
йощещенуюуухэьхглсцлсцухухьюиоэцбщхщзырьмющнофвкьлдлпнзмюаякцздмушццгкоззеяьйонзицксмоцьериыпукэлумюкухггаиэи.  
Key 4: бщцэ  
хлвуакщвнфзюнмпзеимуьрьюяднэпьянреумдъднгскеиовжгтмеиежгуйьбгпвцунзкчжрзедезувичгоьцькьтфораязюзмьзпряынлздауьмччю  
Key 5: шлязърйлсц  
нэлцэщйчънящърйючъхельгуйпщъцмищкяхищеьмнрааъхъшмхйфшъуьлеяеяутлажяаюгящтцлфсъазксгвоычлярфчяеюкмяпръдящнгрйьмдч

(на фото зображений лише початок шифротексту тому, що ми виключили з тексту всі переноси рядків \n)

2. Індекси відповідності:

```
I (key 1) = 0.041479554  
I (key 2) = 0.04951212  
I (key 3) = 0.035179332  
I (key 4) = 0.036390767  
I (key 5) = 0.033627342
```

### 3. Визначення довжини ключа:

```
Length of key:  
2: 0.033854697  
3: 0.033890355  
4: 0.033828564  
5: 0.033948563  
6: 0.03393202  
7: 0.03388788  
8: 0.033870284  
9: 0.033925667  
10: 0.03389699  
11: 0.033697054  
12: 0.03402936  
13: 0.03382497  
14: 0.03374057  
15: 0.03389  
16: 0.034002803  
17: 0.05665287  
18: 0.033914678  
19: 0.033895157  
20: 0.033573303  
21: 0.034174807  
22: 0.03365397  
23: 0.033783223  
24: 0.03403768  
25: 0.033792783  
26: 0.03363762  
27: 0.03379104  
28: 0.033759702  
29: 0.033997703  
30: 0.034088682
```

Для пошуку довжини ключа був використаний метод індексів. В результаті ми отримали, що довжина нашого ключа зіставляє 17 символів.

Визначення символів ключа:

```
Key:
венецианскийкужец
Key via M
венецианскийкупец
```

Перший ключ був знайдений через порівняння найчастішої букви шифротексту і найчастішої букви в свино-собачій мові. Другий ключ був знайдений за допомогою функції  $Mi(g)$ . Як бачимо, другий варіант виявився найточнішим.

Розшифрований текст:

```
Decoded with first key:
антонионезнаюмчеготакпечаленмцеэтовтягостьвамялышутоженогдеягрстьпоймалнашлиледобылчтосоставляотчтородитеехотелкызн
Decoded with second key:
антонионезнаютчеготакпечаленмнеэтовтягостьвамялышутоженогдеягрстьпоймалнашлильдобылчтосоставляетчтородитеехотелбызн
```

## Висновок

Виконуючи цю лабораторну роботу, ми перечитали ліцензійну згоду Windows. Напевне ми перші хто це зробив. Також доволі цікаво було перечитувати розшифрований текст. Окремою задачею було зрозуміти, адже в ньому нема жодних роділових знаків, чи пробілів.