Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Варіант - 10

Виконав:

Студент групи ФБ-35

Кохта Андрій

Київ – 2025

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

Постановка задачі: 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. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру **варіанта - 10**)

Очищення тексту

Початковий:

```
Криптогра́фия — первоначально наука о методах обеспечения конфиденциальности сообщений (шифрование). В настоящее время к
Современная криптография делится на два больших раздела: симметричную криптографию и асимметричную криптографию (крипто
Основными задачами, которые решаются криптографией, являются: обеспечение конфиденциальности, обеспечение целостности д
Для решения этих задач используются различные криптографические методы и системы. Например, для обеспечения конфиденциа
```

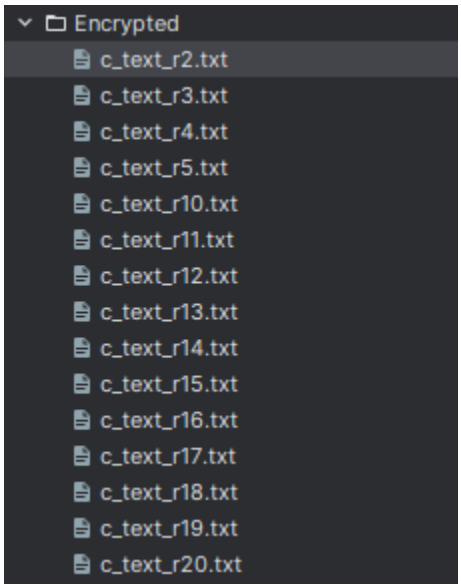
Очищений:

```
криптографияпервоначальнонаукаометодахобеспеченияконфиденциальностисообщенийшифрованиевнастоящеевремякриптографиявключаетвсебям
```

Ключі шифрування:

```
keys = {2: "кр", 3: "кри", 4: "крип", 5: "крипт", 10: "криптограф", 11: "криптографи", 12: "криптография", 13: "криптографиял", 14: "криптографияла", 15: "криптографиялаб",
        16: "криптографиялабо", 17: "криптографиялабор", 18: "криптографиялабора", 19: "криптографиялаборат", 20: "криптографиялаборато"}
```

Результат шифрування:

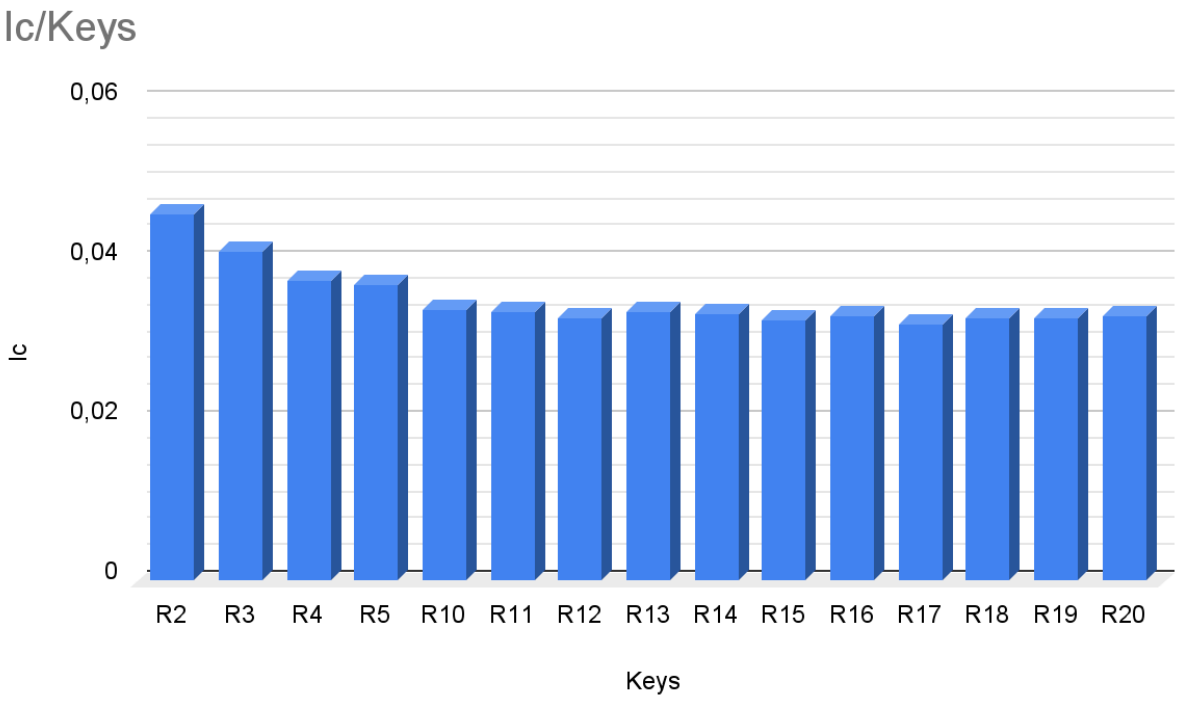


Обчислені значення індексів відповідності для вказаних значень r:

Індекс відповідності ВТ: 0.05668706181388319

Індекс відповідності теоретичне(рос. мови): 0.056119108006076446

Key	Ic
R2	0.04600706003836063
R3	0.041338136589081004
R4	0.03756631927166196
R5	0.03711542999184661
R10	0.033845898659714095
R11	0.033651992907254645
R12	0.033028223799945335
R13	0.033619285912863894
R14	0.03340902666320907
R15	0.032586679375670204
R16	0.033272358150933434
R17	0.03222223000960184
R18	0.03281212401557788
R19	0.03296865034587647
R20	0.03318591823718645



Обчислену послідовність Dr або набори значень індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера:

Перший алгоритм:

Довжина ключа	Середній ІС блоків	Відхилення
2	0.032878	0.023242
3	0.035515	0.020604
4	0.032861	0.023258
5	0.038953	0.017166
6	0.035550	0.020569
7	0.032812	0.023308
8	0.032864	0.023255
9	0.035534	0.020585
10	0.039067	0.017052
11	0.032882	0.023237
12	0.035520	0.020600
13	0.032756	0.023363
14	0.032723	0.023397
15	**0.054125**	**0.001995**
16	0.032808	0.023311
17	0.032849	0.023270
18	0.035573	0.020546
19	0.032595	0.023524
20	0.039074	0.017045
21	0.035220	0.020900
22	0.032950	0.023169
23	0.032954	0.023165
24	0.035418	0.020701
25	0.038955	0.017164
26	0.032851	0.023268
27	0.035261	0.020858
28	0.032531	0.023588
29	0.032564	0.023555
30	**0.054126**	**0.001993**

Найбільший іс спостерігаємо у ключа з довжиною 30, тому довжина ключа для розшифрування = 15

```
r: 30
Найменше відхилення: 0.0019930323542455206
```

шифрований та відповідний розшифрований тексти (відповідно до варіанту завдання - 10), знайдене значення ключа:

Ключ: крадущяйгявтени **символ**: “о”

Щось не те, спробуємо поміняти частіші символи:

символ: “о”: **крадущ**яйгявтени

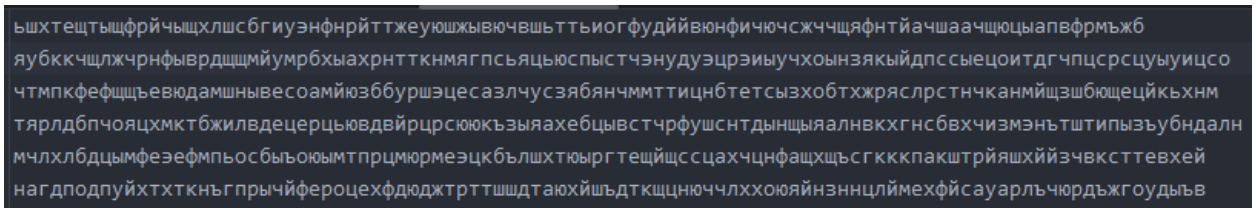
символ: “е”: ущйньв**и**тмилыоцс

символ: “и”: рцжкщяепйеишлуо

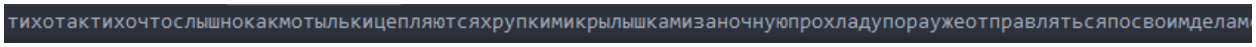
символ: “а”: шюотбзнч**с**нрауыц

Ключ: крадущийсявтени

Шифрований текст:



Розшифрований текст:



Висновки: У процесі виконання лабораторної роботи з шифром Віженера я дізнався про два методи знаходження ключа, я зашифрував випадково підібраний текст шифром віженера з випадково підібраними ключами, проаналізував індекси відповідності для кожного з підібраних ключів,а також за допомоги підбору ключа, розшифрував наданий зашифрований текст.