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
Гілевський Олександр,
Кузьменко Анна

Приймав:
Чорний Олег Миколайович

Київ-2023

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

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_r 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_r (на вибір);

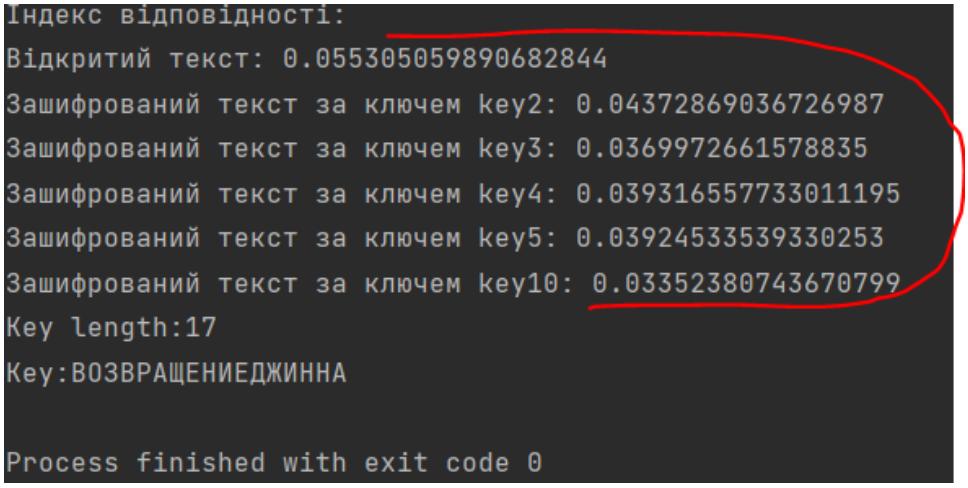
– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

– визначити символи ключа за допомогою функції M_i(g);

– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Хід роботи

1, 2. Підібравши текст, який знаходиться в файлі text.txt, шифруємо його за допомогою шифру Віженера та порівнюємо індекси відповідності:



Як бачимо, після ключа довжини 4 індекс зменшується.

3. За допомогою методу індексів відповідності розділивши на блоки текст, шукаємо при якому значенні блоку маємо максимальне значення індексу відповідності

{2: 0.5050249571158242, 3: 0.5049500142596124, 4: 0.5048817942178866, 5: 0.5050395115350288, 6: 0.5053114750139039, 7: 0.5047561753290022, 8: 0.5046525997305321, 9: 0.5049861525568289, 10: 0.5049297831200974, 11: 0.5047931222648517, 12: 0.5049628015085662, 13: 0.5051365477354467, 14: 0.5044760626337862, 15: 0.5052180302070892, 16: 0.5046478182202865, **17: 0.547763986623992**, 18: 0.505057876710928, 19: 0.5049678272100595, 20: 0.5046061475031365, 21: 0.5044993527325943, 22: 0.5046789776278419, 23: 0.5053210623680423, 24: 0.5045335749005134, 25: 0.5042870200359251, 26: 0.5052925298658617, 27: 0.5049969507727505, 28: 0.5047509543615637, 29: 0.504608714417869, 30: 0.5053427216927532, 31: 0.5046622557058992}

Бачимо, що довжину ключа: 17

```
Індекс відповідності:
Відкритий текст: 0.055305059890682844
Зашифрований текст за ключем key2: 0.04372869036726987
Зашифрований текст за ключем key3: 0.0369972661578835
Зашифрований текст за ключем key4: 0.039316557733011195
Зашифрований текст за ключем key5: 0.03924533539330253
Зашифрований текст за ключем key10: 0.03352380743670799
Key length:17
Key:ВОЗВРАЩЕНИЕДЖИННА

Process finished with exit code 0
```

І з функції M_i(g) отримаємо ключ:

```
Індекс відповідності:
Відкритий текст: 0.055305059890682844
Зашифрований текст за ключем key2: 0.04372869036726987
Зашифрований текст за ключем key3: 0.0369972661578835
Зашифрований текст за ключем key4: 0.039316557733011195
Зашифрований текст за ключем key5: 0.03924533539330253
Зашифрований текст за ключем key10: 0.03352380743670799
Key length:17
Key:ВОЗВРАЩЕНИЕДЖИННА

Process finished with exit code 0
```

Результат розшифрованого тексту в файлі result.txt

Висновок: засвоїли методи частотного криптоаналізу, здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.