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)(gMi ;

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

Хід роботи

- опис труднощів, що виникали, та шляхів їх розв’язання;
- обчислені значення індексів відповідностігI для вказаних значень r (подати у вигляді таблиці та діаграми);
- обчислену послідовність D або набори значень індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера (подати у вигляді таблиці та діаграми);
- значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови;
- значення ключа, одержане із використанням функції)(gMi ;скореговане значення ключа (за необхідності);

- –фрагмент шифрованого тексту (відповідно до варіанту завдання) та результати його розшифрування усіма знайденими варіантами ключа – 5-10 рядочків;
- – висновки

1. Труднощі: ненавиджу python і всі ці позначення в методичці. Більше труднощів не виникало.
2.

Розмір ключа	Очікуване	Реальне
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

3.

Пошук розміру ключа

```
def blocks(text,r):
    y = ['']*r
    for i in range(0, len(text)):
        y[i%r]+=text[i]
    return y

def key_lenght(text):
    ind = 0.0553 #з лекції
    solutions=[]
    for r in range(2,len(alphabet)):
        solution = 0
        y = blocks(text,r)
        for i in range(r):
            solution +=index(y[i])
        solutions.append(solution/r)
    compare = [abs(ind - x) for x in solutions]
    return (compare.index(min(compare))+2)

print()
r = key_lenght(text_2)
print(r)
```

[15]

...

14

4.

Перший спосіб пошуку ключа

```
def find_key_1(text,r):
    key = ''
    y = blocks(text,r)
    for i in range(0,r):
        blocka = dict(y[i])
        letter = alphabet[get_num((blocka[0][0]) - get_num(p_govna_sort[0][0])]
        key+=letter
    return key

key = find_key_1(text_2,r)
print(key)
print(decypher(text_2,key))
```

[17] Python

посняковандрей

5.

Дугий спосіб пошуку ключа

```
def Counter(text,letter):
    count = 0
    for i in text:
        if i == letter:
            count+=1
    return count

def M_i_g (text,letter):
    summ = 0
    for t in range(0,len(alphabet)):
        probability = p_govna[alphabet[t]]
        temp = (letter+t)%len(alphabet)
        frequency = Counter(text, alphabet[temp])
        summ += probability*frequency
    return summ

def find_key_2(text,r):
    key = ""
    ans =[]
    y = blocks(text,r)
    for i in range(0,r):
        for g in range(0,len(alphabet)):
            tmp = M_i_g(y[i], g)
            ans.append(tmp)
        key += alphabet[ans.index(max(ans))]
        ans.clear()
    return key

key = find_key_2(text_2,r)
print(key)
```

[18]

```
посняковандрей
```

6. Результат для обох ключів однаковий :

наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгустойтайгизатерялась михайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслинесчитатьскитупустозерскогоострогачтонапечоререкенудотогоскитаещедобратьсянадоаказдешнемумонастырюпожалуйстахочешьчерезвологдудапотомпосухонев

великийустюгатамидодвинырукойподатьзнайплывипотечениюахочешьнапрямикчерезладогусвирьонегуд

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