

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Варіант №6

Криптоаналіз шифру Віженера

Мета роботи

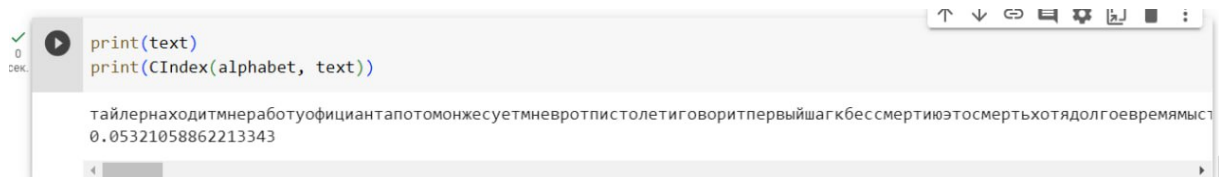
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

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 r 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_r (на вибір); – визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові; – визначити символи ключа за допомогою функції $M(g)$ і ; – розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Хід роботи:

Відкритий текст та його індекс:



```
print(text)
print(CIndex(alphabet, text))
```

тайлернаходитмнеработуофициантапотомонжесуетмневротпистолетиговоритпервыйшагкбессмертиээтосмертьхотядолгоевремямыс
0.05321058862213343

Шифротекст та його індекс

```
print(text)
print(CIndex(alphabet, text))
```

жчрдеврйкужояхвфчэьоьашгтмцифавицопшнюфйтнижуфтмцървяихьонпцтоонкязиекчхмкхєхшефюзгютцършуфжйщсфюхкведбъцооф
0.034119477929863806

Зашифрований відкритий текст з ключом довжини 3,4,5,10

```
print(result)
print(CIndex(alphabet, result))
```

тюзагглюєцргнюацгхгоудиггтмцнгеюрцагбюоцтгуоцфгююцггаюцтггаюцпоцгтюоцмгоюцнцгююсцугеюцтгмгнюецвгрюоцтгпюицсгтлюцлге
0.10157445599459179

```
print(result)
print(CIndex(alphabet, result))
```

ткарйшляекррншаяхкордишаткмрншеяркарбшояткурошфяикциришаянктрашпяоктрошмяокрнжшеяскурештямкрншевьяркортшпаяиксртшоялке
0.0917226804307897

```
print(result)
print(CIndex(alphabet, result))
```

тоацйфлжлронцафхжолдоицтфмжнлеорцафбжолтоуоцфжлциоцафнжтлаоцпоцфжолмооцнфжлсоуецфжмлноецвфржолтопцифсжтлоолце
0.07894595188051216

```
print(result)
print(CIndex(alphabet, result))
```

тхаййюлречрбнваяхтождхийтюрнчеврбаябтожтхуйоюфричбиваянттжахпюютрочмбовняжтежсхуйеютрмчнбеввяртожтхпийюсртчоблве
0.051212265991370146

Знайшли довжину ключа(17) та сам ключ(возвращениеджинна)

Висновок:

Під час виконання цієї лабораторної роботи було обрано текст і ключі, якими цей текст було зашифровано шифром Віженера