МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ
УКРАЇНИНАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ

ІНСТИТУТ»ФІЗИКО-ТЕХНІЧНИЙ

ІНСТИТУТ

Криптографія

Комп’ютерний практикум №2

Виконали:

студенти групи ФБ-95

Товстенко Артем, Тараканов Егор

Перевірив(ли):

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потоковихшифрів 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.

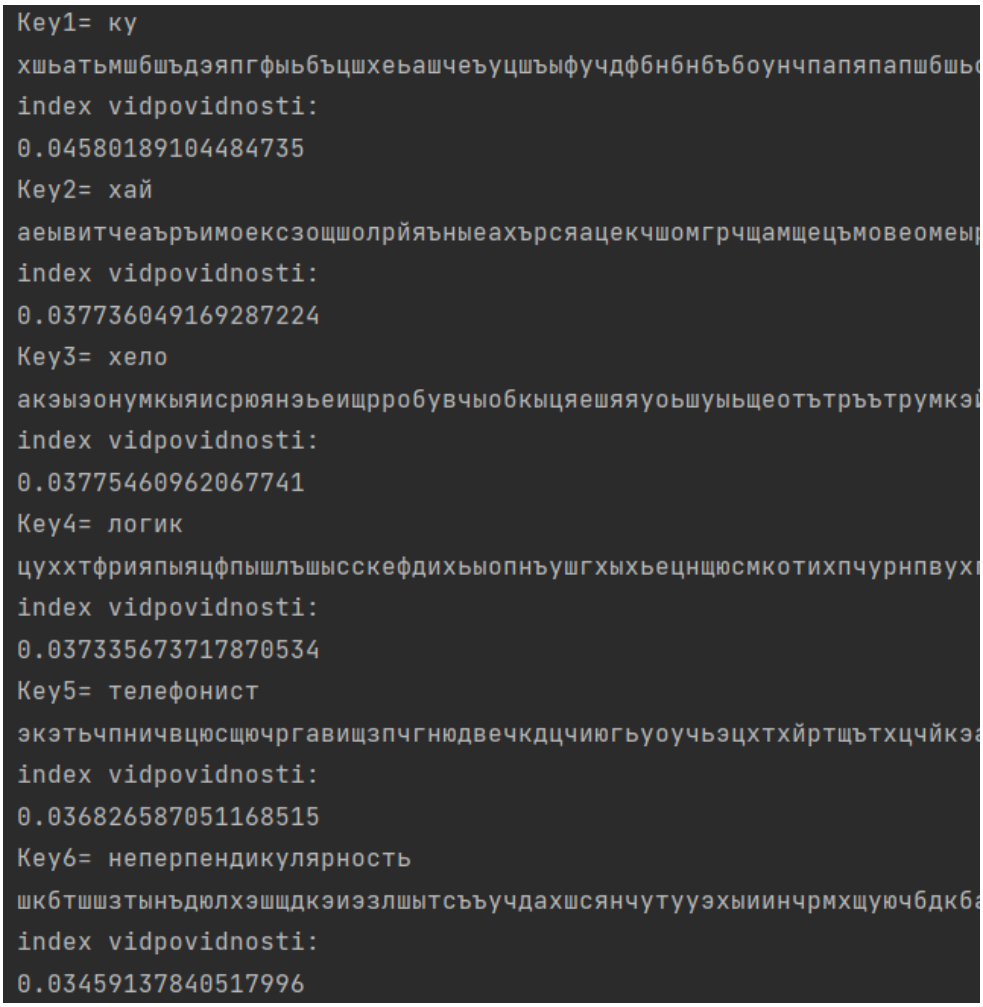
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів іпорівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідносвого номеру варіанта).

Хід роботи:

1. Перед виконанням роботи були уважно прочитані методичні вказівки.
2. Для виконання першого завдання створення текстовий файл **text.txt**. Для шифрування даного тексту обрано ключи **«ку», «хай», «хело», «логик», «неперпендикулярность»**.
3. **Encode_function** - функція шифрування методом Віженера.
4. **Conformity_index** – функція знаходження індексу відповідності.
5. Перевірямо ключі довжиною **2 <= r <=32**: розбиваэмо текст на фрагменти, які складаються з елементів тексту з періодом **r**. Просумовуємо індекси відповідності фрагментів для кожного з ключів да ділимо їх на довжину ключа. Порівнюємо з теоретичним значенням, яке дорівнює 0.055. Обираємо ключ, у якого індекс відповідності найближчий до теоретичного. Шукаємо значення ключа за допомогою найбільш частих літер у кожному фрагменті для цього ключа та найбільш частої літери російського алфавіту.
6. **Decrypt_function -** надалі розшифровуємо текст за допомогою функції. Далі проводитьсякорегування вручну.

Значення індексів відповідності для різних значеннях ключа:



Візьмемо уривок вже розшифрованого тесту:

Иыутяьвиделмоятцикшйрвисящцйнйдолмойнитиьпувеннчй –воно потребує корегування.
Ключ був подвійним – значення індексів відповідності ключів довжиною 14 та 28 – приблизно рівні, отже, ми оберемо коротший.

ВТ Иыутяьвиделмоятцикшйрвисящцйнйдолмойнитиьпувеннчй

Ключ эбомацтникфуьо эбомацтникфуьо эбомацтникфуьо эбомацт

ШФ

еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнны

На початку мало б бути «и тут я увидел». Тобто елемент ключа (б) змінюємо на (к) та елемент (ц) змінюємо на (я).
Ключ має вигляд «экомаятникфуьо». Не важко здогадатись, що ключем буде «экомаятникфуко», але потрібно виконати перетворення ключа формально, адже незавжди ключі є змістовними.

Після виконаних змін отримуємо: ВТ

ИтутяувиделмоятникшйрвисящцйнйдолмойнитиьпувеннчйКлюч

экомаятникфуьоэкомацтникфуьо эбомацтникфуьо эбомацт

ШФ еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнны

Легко читається « и тут я увидел маятник…». Тобто нам потрібно змінити (ь) на (к), щоб отримати слово маятник, а не моятник, у відкритому тексті. Тому ми вручну вводимо правильний ключ і отримуємо правильний ШТ
КЛЮЧ – «экомаятникфуко»

ШТ
еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвачьймучицъхцщьдерэхшълдунхтутс
ыэхыъибгмттэбгбптщныоасякдуццйпющоибаужеуацебаъпдвхцоюбхуюкыфйнбэнощюпыльыъшдяхнцюхктнкащовачцъб
тощечйщисъчятеюэюзшаърнчхшъфйтьккщиннчсуйгбощрчызхтюыкщдшощеаьшбнштщьцшчылуюмцзаънэюбыыеьучьма
юцщдтновььцртшъцыжыытекъстптщрхтфегоэзсссфажгьифюрньокяьхкъщяйэвъушешчърйму
ъолььрннхычшясыозщюътз
фычшябрылцбырдцюъкцюйупъууукояиьжууылуяъосятщпбашяптымиаашнпцапрнпъснмнвф
пдшоцкыаоемяыщььешезтш
ьеоэтхтучмьжыаоемяыщььуляпъоцтмарцтыяпювчцлтпахячвдьцфтячаоъютъпешчфпаоепъдх
шеетшяктьасяылшюбъыьыьо
епктхыжхкшнэсмешчмпчфюбалчоцомитцьцшыылущфнзъпцыеекылмщснмаццьжббшефюспк
чърйбуяьбйзфйрсьцоауйакт

ВТ
Итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличии описывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременныхмерединственноститочкикрепленияздвойственностиабстрактногоизмерениятроичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеязналчтонаконцеотвеснойлинииивосстановленной

Висновок:

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