МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий Фізико-технічний інститут
Кафедра інформаційної безпеки

КРИПТОГРАФІЯ

Комп’ютерний практикум №2
Криптоаналіз шифру Віженера

Виконали:
Студенти ФБ-33
Дохоян Юлія
Терещенко Микола

Київ – 2025

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 для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Хід роботи

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.

Текст залишено з минулого комп'ютерного практикуму – kafka.txt.

Було підібрано наступні ключі:

```
    keys = [
        "да",
        "чай",
        "пиво",
        "водка",
        "алкоголизм",
        "пивоварение",
        "молокопровод",
        "грабительство",
        "забинтовавшись",
        "безответственно",
        "уничижительность",
        "алкоголизовавшись",
        "умиротворительница",
        "фтизиопульмонология",
        "витаминопрофилактика"
    ]
```

Рис.1

Усі ключі були підібрані випадковим чином, автори протоколу не схиляють до дій, які є небезпечними для здоров'я, крім навчання.

```
Ключ: да (довжина 2)
Зашифрований текст: уртссужшмсаоинджиычтфорптспееехптктйсозохндгфезофздмлатбсафукипчцотнчсйбгвуохтйлмпфежр
дтмлхяжсцрдшсойндсйктмтепекасауасцмрсоцвйрионсуисетнжиепсцомлтеруурмптдсяцьзопожухвтйоофиынйвяйжыууоляйфа
лдйлйнсындчгтоердзсыриыеьункдммжмвттсажефхчшоеооцофозойлйдйркапохьзоцожойвттжоцооосчдтйлантсуопзцитдйяпойг
тмсозоыихлйнсыйуеозоцоскмеуохрдвсесивстсцапьсыртйлтмсоккмбйсуороэнткттптшмлмсаусезоуефеигпалариыттстмсонспу
ыипохьуоиурапосэцосееыпохнтмйгткмсацасахттяэагрдзжеыттспиьктмрапесьоагнтоеыындяоорндтдммрсоуоооомлдсавхвти
щчйтярйхщофоьолндктмяххтйндхсаисцопоргиееыпифаллтжйнярдсуаоожасняетбфалцясчктнларздбялоормвтякефорвмсйлуо
фтфецкттряйтнсеиажнтвярйздлмзмлпюхтфифожаснтгтжчрсапамвхтдвмлжкфахижувзтлтчйнчюфаркчндптрцрйтйбялдилоердж
йнддмдврещожоншпяуембтатндсмдйлдоыесьургмтиурттггмвдлдзфицепюцякепувмйхтвчюруштчвооцофонцйлмктммсыелапайе
фуоалацервлгпяигфезофачсцрймлхяжоонтиуахмчрсагптгтддспыьнтбялткдкуокехтмптдтктнсиоахтччдтоаулмдтжияурмвйл
дезомвтвхежгфухтсойндсцртесий
_____

Ключ: чай (довжина 3)
Зашифрований текст: жрчиньщшсиьчынйэддктщемшесфьбоипчботдомесцчгщьгчзэйгэйебцчрьэифотченьиекцвшесыьлсжрощр
ййифиялитщчшцеецчсобохеефьжйдашчняярцетльрнейъжицьоцщиньлъйосвоогушзишедццтеъофевьивчакчзиаделтйлтпьблдарй
юдовецдытыумеокзардыхячопутбахяжсщоыдальрюкшуькчйощегчьлоыещэафесеъоыевчьвчйвчйоуеначтовьцесшелрйичыеивооъ
охдомечсилодндьукегчйоцбиожоъзалдецяюъесычледыхйефемцежуябоипчговдоуепчпифясекноъошьроыгфчзйгиайоъемцейъву
аялчиьшедьгафенжйоцьбдвоъдохьгчбохдаычнйитчцщйцрйювоотчилспкчгмйвецукйцнчебдонйцкчгнййахярцепчбосваъувъщос
мчойыщьхюерчпордауемдмсыьнймнйысыелчггньбдвищчзфежодыщчсшчкчщацдыоебщчзятсьбоцюахюактлуемхявчцжозохщиъълше
рызеыбоыердаощденчвцевдзерчлсюифвюъйрсзолчнцегчэущдафчилитйщифщкщчссщузюофечодуззахбуцчпчзтщьтошыфчиребщчж
оданчмйщмомолейбвяшьикеачдаъядовачоецупщцмчяпщетиъилчлйюрсйефхтиэефкюхьхчщузгуэйулбоыерчацовиуемсичоюафчео
зуучзййехщзмвянъроъощчуъйрогифиялекцеишчсхкрцчяшегчыаъвыбдоктлчбаужопьсыяпчыоуенцякйитьоаыбашвинежнцпщявов
аоъосщолиелърьитцеецчсызоодио
```

Рис.2

На рис.2 зображено частину результатів шифрування. Всі результати прикріплені у файлі результати_шифрування.txt.

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

Індекс відповідності відкритого тексту: 0.058674

Ключ	Довжина	Індекс відповідності
да	2	0.045712
чай	3	0.040665
пиво	4	0.036744
водка	5	0.036081
алкоголизм	10	0.036304
пивоварение	11	0.036386
молокопровод	12	0.038873
грабительство	13	0.032567
забинтовавшись	14	0.033126
безответственно	15	0.035123
уничижительность	16	0.034846
алкоголизовавшись	17	0.033640
умиротворительница	18	0.034205
фтизиопульмонология	19	0.034935
витаминопрофилактика	20	0.035853

Рис.3

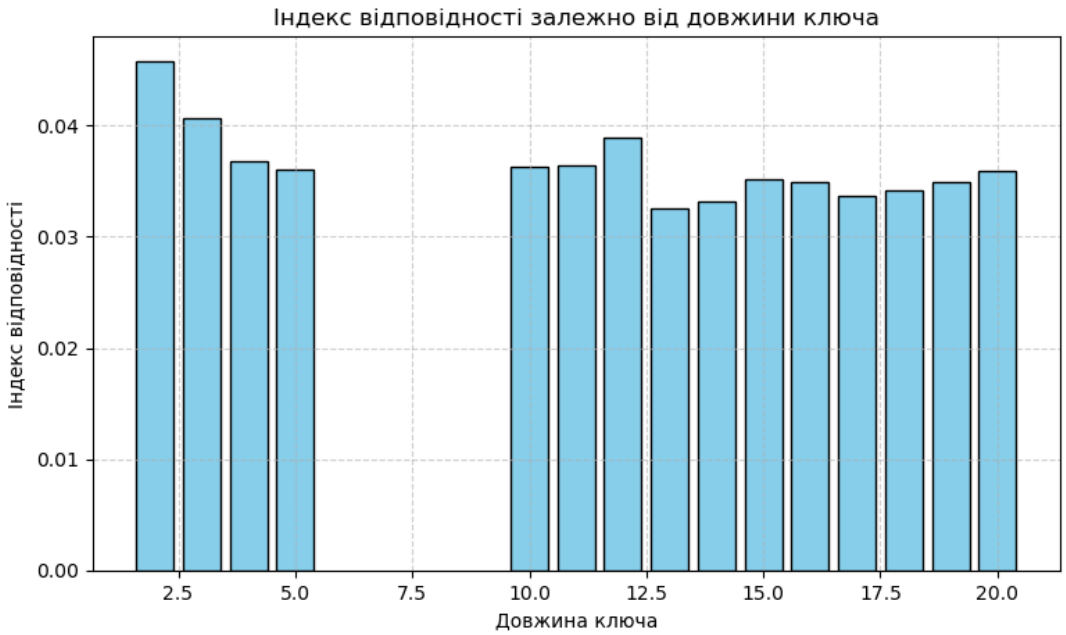

Рис.4

Скрипт для завдання 1 і 2 прикріплено разом із протоколом.

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

```
Найбільш ймовірна довжина ключа: 14
Знайдений ключ: последнийдозор
Перші 200 символів розшифрованого тексту:
какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайнейсеройравнинывзгляднефикс
ировалияркихкрасоквцелойкартиненостоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянц
```

Рис.5

Рис.6

Скрипт для 3 завдання та результати розшифрування додані разом із протоколом.

Висновок: У ході виконання лабораторної роботи було засвоєно принципи та методи частотного криптоаналізу, а також отримано практичні навички роботи з потоковими шифрами гамування адитивного типу на прикладі шифру Віженера. Під час виконання завдань було здійснено шифрування тексту шифром Віженера з використанням цих ключів, обчислено та порівняно індекси відповідності для відкритого тексту і всіх шифртекстів, що дозволило спостерігати залежність між довжиною ключа та ступенем наближення статистичних характеристик шифртексту до випадкової послідовності, виконано розшифрування шифртексту за допомогою методів частотного аналізу та визначення довжини ключа.