

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.02/2/172.00.1/Б /ОКЗ1-2021
	Екземпляр № 1	Арк. 5_/1

ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»

протокол від _09_ _11_ 2020 р.
№ 4_

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

для проведення лабораторної роботи №1-3

з навчальної дисципліни

«ЗАХИСТ ІНФОРМАЦІЇ В

ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 172 «Телекомунікації та радіотехніка»
освітньо-професійна програма «Телекомунікації та радіотехніка»
факультет інформаційно-комп'ютерних технологій
кафедра біомедичної інженерії та телекомунікацій

Схвалено на засіданні кафедри
біомедичної інженерії та
телекомунікацій
31 серпня 2020 р., протокол № 9

Завідувач кафедри

Тетяна НІКІТЧУК

Розробник: к.т.н. доцент кафедри біомедичної інженерії та телекомунікацій
Дубина О.Ф.

Житомир

2021 – 2022 н.р.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.02/2/172.00.1/Б /ОКЗІ-2021
	Екземпляр № 1	Арк _5_/2

ЛАБОРАТОРНА РОБОТА № 1-3 БАЗОВІ ШИФРИ. ЧАСТОТНИЙ КРИПТОАНАЛІЗ

Мета роботи: ознайомитися з базовими шифрами. Розглянути методику частотного криптоаналізу.

Використовуване програмне забезпечення: середа розробки GNU Octave. Python та ін.

Теоретичні відомості

В криптографії здавна використовувались два види шифрів: заміна та перестановка. Історичним прикладом шифру заміни є шифр Цезаря. Його сутність така: в строку випикується алфавіт, після чого під ним випикується той же алфавіт з циклічним зсувом на 3 букви вліво.

**АБВГДЕЇЖЗИЙКЛМНОПРСТУФХЦШЩЬЪЬСЮЯ
ГДЕЇЖЗИЙКЛМНОПРСТУФХЦШЩЬЪЬСЮЯАБВ**

При зашифруванні буква відкритого тексту замінюється на букву, що знаходиться під нею в нижній строчці. Наприклад: РИМ – УЛП. Ключем в шифрі Цезаря є величина здвигу нижньої строки.

1.1. Шифр простої заміни

Подальший розвиток шифру Цезаря є очевидним: нижня строчка може бути записана з випадковим порядком букв. Такий шифр носить назву шифру простої заміни. Ключем такого шифру є порядок розташування букв в нижній строчці, так звана «таблиця заміни». Якщо в шифрі Цезаря існує тільки 33 варіанта ключів, то в шифрі простої заміни їх вже 33! (33 факторіал).

1.2. Квадрат Полібія

Одна з відомих модифікацій шифру простої заміни – квадрат Полібія. Візьмемо алфавіт з 32 букв. Виберемо ключ – будь-яке слово, в якому немає однакових букв. Запишемо його в перші клітинки квадрата розміром, наприклад, 4×8. В останні клітинки запишемо алфавіт за винятком тих букв, що зустрічаються в ключі. Для зашифрування букви повідомлення замінюються на букви, що стоять *під* ними в квадраті Полібія. Наприклад:

Ключ – «**МОСКВА**».

Повідомлення – «**НЕЛЬЗЯ ПОМОЧЬ ТОМУ, КТО НЕ ЖЕЛАЕТ СЛУШАТЬ СОВЕТОВ**».

На рис. 1.1 представлено Квадрат Полібія для ключа «**МОСКВА**».

М	О	С	К
В	А	Б	Г
Д	Е	Ж	З
И	Й	Л	Н
П	Р	Т	У
Ф	Х	Ц	Ч
Ш	Щ	Ы	Ь
Ъ	Э	Ю	Я

Рисунок 1.1 – Квадрат Полібія

Зашифроване повідомлення:

«**УЙТМНКФАВАЪМЦАВЧГЦАУЙЛЙТЕЙЦБТЧЬЕЦМБАДЙЦАД**».

Для розшифрування букви шифротексту замінюються на ті букви, що стоять *над* ними в квадраті Полібія.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.02/2/172.00.1/Б /ОКЗІ-2021
	Екземпляр № 1	Арк. 5 / 3

2.1. Шифр перестановки

Оберемо ціле додатне число, наприклад, 5. Створимо випадкову підстановку:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$$

Зашифруємо фразу:

«БАЖАСІШ БАГАТО ЗНАТИ, ТРЕБА МЕНШЕ СПАТИ».

Для цього доповнимо фразу до довжини кратної 5 випадковими символами та розіб'ємо на групи по 5 букв.

БАЖАС ШБАГА ТОЗНА ТИТРЕ БАМЕН ШЕСПА ТИВСЕ

Букви кожної групи переставимо згідно обраної підстановки.

Отриманий текст запишемо без пропусків.

«ААБСЖГБШААНОТАЗРИТЕТЕАБНМПЕШАССИТЕВ»

При розшифруванні текст розбивається на групи по 5 букв і букви переставляються в зворотному порядку. Ключом шифру є степінь підстановки (тут 5) і порядок розташування чисел в нижньому рядку підстановки.

2.2. Шифр Тритемія

В XV столітті абат Тритемії (Германія) запропонував шифр на основі “таблиці Тритемія”. Для російського алфавіту вона має наступний вигляд:

А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я
Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А
В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б
Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В
Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г
Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д
Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ь	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь
Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю
А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Ю	Я

Рисунок 1.2 – Таблиця Тритемія для російського алфавіту

Тут перша строчка є одночасно і строчкою букв відкритого тексту. Перша буква тексту шифрується по першій строчці, друга – по другій і т.д. Після останньої строчки знову повертаємось до першої. Наприклад, слово “**КРИПТОГРАФИЯ**” зміниться на “**КСКТЦУИЧЗЭТЙ**”. Однак, в такому варіанті, в шифрі Тритемія був відсутній ключ. В подальшому удосконалення шифру пішли по двом шляхам:

- введення випадкового порядку розташування букв алфавіту;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.02/2/172.00.1/Б /ОКЗ1-2021
	Екземпляр № 1	Арк _5_/4

- застосування більш складного порядку вибору строк таблиці при шифруванні (по ключу).

3.1. Частотний криптоаналіз

Частотний криптоаналіз базується на застосуванні статистики для аналізу текстової інформації. Текст складається із слів, слова із літер. Кількість літер в кожній мові обмежена. Важливими характеристиками тексту є повторюваність літер, пар літер (біграм) і, взагалі, т-грам, поєднання літер друг с другом, чередування голосних і приголосних і т.д. Всі ці характеристики є достатньо стійкими і можуть бути використані для аналізу шифртекстів. В табл. 1.1 та 1.2 приведені однобуквені ймовірності англійської та російської мов.

Таблиця 1.1 - Однобуквені ймовірності англійської мови

Літера	Ймовірність	Літера	Ймовірність
A	0.0856	N	0.0707
B	0.0139	O	0.0797
C	0.0279	P	0.0199
D	0.0378	Q	0.0012
E	0.1304	R	0.0677
F	0.0289	S	0.0607
G	0.0199	T	0.1045
H	0.0528	U	0.0249
I	0.0627	V	0.0092
J	0.0013	W	0.0149
K	0.0042	X	0.0017
L	0.0339	Y	0.0199
M	0.0249	Z	0.0008

Таблиця 1.2 - Однобуквені ймовірності української мови

Літера	Ймовірність	Літера	Ймовірність	Літера	Ймовірність
А	0,062	К	0,028	Ф	0,002
Б	0,014	Л	0,035	Х	0,009
В	0,038	М	0,026	Ц	0,004
Г	0,013	Н	0,053	Ч	0,012
Д	0,025	О	0,090	Ш	0,006
Е	0,072	П	0,023	Щ	0,003
Ж	0,007	Р	0,040	И	0,016
З	0,016	С	0,045	Ь	0,014
І	0,062	Т	0,053	Г	0,003
Й	0,010	У	0,021	Ю	0,006
				Я	0,018

Процес криптоанализу можна представити наступним чином. Криптоаналітик підраховує частоти букв в шифротексті. Далі він бере в шифртексті символ, що зустрічається найбільш часто, и припускає, що це пробіл. Потім бере наступний символ, що зустрічається найбільш часто, и припускає, що це Е (для англійської мови), и т.д. Шляхом проб і помилок такий метод може привести до рішення задачі. Крім того, при підставленні букв замість символів аналізованого шифртексту криптоаналітик враховує частоти появи сполучень із двох букв (діаграм), трьох букв (триграмм) і т.д.

4.Завдання на лабораторну роботу

Лабораторна робота №1. Розробити програми шифрування та розшифрування наступними шифрами:

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.02/2/172.00.1/Б /ОКЗІ-2021
	Екземпляр № 1	Арк _5_/5

- шифр простої заміни;
- квадрат Полібія;
(У якості ключа або сова, що аналізується, використовувати власне ім'я.)

Лабораторна робота №2. Розробити програми шифрування та розшифрування наступними шифрами:

- шифр перестановки;
- шифр Тритемія з вибором строк по ключу;
(У якості ключа або сова, що аналізується, використовувати власне ім'я.)

Лабораторна робота №3. Виконати частотний криптоаналіз отриманих зашифрованих текстів.

1.1 Зміст звіту

- 1.1.1 Титульний лист, тема і мета роботи.
- 1.1.2 Відповіді на контрольні питання.
- 1.1.3 Тексти програм.
- 1.1.4 Обране повідомлення для шифрування.
- 1.1.5 Обраний ключ.
- 1.1.6 Зашифроване повідомлення.
- 1.1.7 Розшифроване повідомлення.
- 1.1.8 Результати проведення частотного криптоаналізу.

1.2 Контрольні питання

- 1.2.1 Опишіть шифр Полібія.
- 1.2.2 Опишіть шифр простої заміни.
- 1.2.3 Опишіть шифр Тритемія.
- 1.2.4 Опишіть шифр перестановки.
- 1.2.5 Чи є шифр Полібія шифром простої заміни?
- 1.2.6 Як залежить стійкість шифру від довжини ключа?
- 1.2.7 Опишіть метод частотного криптоаналізу.
- 1.2.8 В яких випадках можна застосовувати метод частотного криптоаналізу?