НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра прикладної математики

Звіт

з лабораторної роботи №*1*

з дисципліни «Криптографічні методи захисту інформації»

на тему:

*Розробка криптосистем на основі шифрів Цезаря та Тритемія*

|  |  |
| --- | --- |
| Виконав: | Керівник: |
| студент групи КМ-01 | *ст. викладач Бай Ю. П.* |
| *Шевцов М. В.* |  |

Київ — 2022

ЗМІСТ

[ЗАВДАННЯ 2](#_Toc94713306)

[Основні теоретичні відомості з шифру Цезаря 3](#_Toc94713307)

[Завдання з шифру Цезаря 3](#_Toc94713308)

[Основні теоретичні відомості з шифру Тритемія 4](#_Toc94713309)

[Завдання з шифру Тритемія 4](#_Toc94713310)

[Список літератури 6](#_Toc94713311)

[Додаток 1 7](#_Toc94713312)

[Додаток 2 8](#_Toc94713313)

# ЗАВДАННЯ

***Мета роботи:*** розробити криптосистеми на основі шифрів Цезаря та Тритемія.

1. Зашифрувати текст довжиною від 10 до 50 символів, користуючись шифром Цезаря з певним ключем *K*. Результат записати в [Таблицю\_1](https://docs.google.com/spreadsheets/d/1vg-aCHGGX2oZDjuAWWRWecRBWjwAYLmkgonEp1CFBGA/edit?usp=sharing), в СВІЙ РЯДОК, стовпчик AG (*1 бал*).

2. Дано криптотекст *C*, одержаний шифруванням Цезаря з невідомим ключем *K* (див. [Таблицю\_1](https://docs.google.com/spreadsheets/d/1vg-aCHGGX2oZDjuAWWRWecRBWjwAYLmkgonEp1CFBGA/edit?usp=sharing), рядок НАД СВОЇМ, стовпчик AG). Методом повного перебору всіх потенційних рішень (методом «грубої сили») дешифрувати заданий криптотекст. У відповіді навести дешифрований текст *P* та ключ *K*. (*2 бали*).

3. Зашифрувати текст довжиною від 10 до 20 символів, користуючись шифром Тритемія за лінійним законом *y = (x + A\*p + B) mod N*. Записати початковий текст та криптотекст в [Таблицю\_2](https://docs.google.com/spreadsheets/d/19vV6-YDYE9fHXQ3q9iaDqeYQlLHj69xGzTOhQase2zI/edit?usp=sharing), в СВІЙ РЯДОК, стовпчики AG, AH (*1 бал*).

4. Уявіть, що Ви перехопили початковий текст та криптотекст (див. [Таблицю\_2](https://docs.google.com/spreadsheets/d/19vV6-YDYE9fHXQ3q9iaDqeYQlLHj69xGzTOhQase2zI/edit?usp=sharing), рядок НАД СВОЇМ, стовпчики AG, AH). Необхідно визначити ключ: знайти параметри *A, B*, але не методом «грубої сили», а розв’язуючі систему двох рівнянь. Відповідь записати в стовпчик AI (рядок НАД СВОЇМ) (*2 бали*).

5. Зашифрувати текст довжиною від 10 до 50 символів, користуючись шифром Тритемія **за квадратичним законом** **(*A, B, C*****від 1 до 5)**. Записати зашифрований текст в [Таблицю\_2](https://docs.google.com/spreadsheets/d/19vV6-YDYE9fHXQ3q9iaDqeYQlLHj69xGzTOhQase2zI/edit?usp=sharing), в СВІЙ РЯДОК, стовпчик AJ (*1 бал*).

6. Методом "brute force" дешифрувати текст, що знаходиться в стовпчику AJ, в рядку НАД СВОЇМ (відомо, що був використаний шифр Тритемія, за квадратичним законом, *A, B, C* від 1 до 5). Відповідь записати в стовпчик AK, знайдений ключ - в AL (рядок НАД СВОЇМ) (*2 бали*).

7. Оформити звіт (*1 бал*).

# Основні теоретичні відомості з шифру Цезаря

Суть шифру Цезаря полягає у тому, щоб зашифрувати текст змінивши букви у словах за певним законом. Цей закон являє собою зміщення відповідних букв слова в алфавіті на деяку кількість позицій, ця кількість називається ключем.

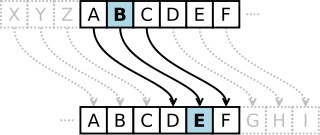


Рис. 1 – Шифр Цезаря

Нехай x – позиція букви початкового слова в алфавіті, а y – позиція зміщеної букви початкового слова в алфавіті, і K – ключ, тоді маємо таку залежність:

*,* де N – кількість букв у алфавіті.

Ділення по модулю застосовується для того, щоб індекс нової позиції не вийшов за межі кількості букв у алфавіті.

У випадку дешифрування, то відбувається все навпаки:

Ми віднімаємо ключ.

# Завдання з шифру Цезаря

1. Зашифруємо текст «**you my heart you my soul**», користуючись шифром Цезаря з ключем *К* = **4**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 | 🡫 |
| e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d |

Результат шифрування:

**csy qc lievx csy qc wsyp**

2. Дано криптотекст, одержаний шифруванням Цезаря:

**xn anx ufhjr ufwf gjqqzr**

Одержимо всі варіанти його дешифрування:

|  |
| --- |
| K = 0 - xn anx ufhjr ufwf gjqqzr |
| K = 1 - wm zmw tegiq teve fippyq |
| K = 2 - vl ylv sdfhp sdud ehooxp |
| K = 3 - uk xku rcego rctc dgnnwo |
| K = 4 - tj wjt qbdfn qbsb cfmmvn |
| K = 5 - **si vis pacem para bellum** |
| K = 6 - rh uhr ozbdl ozqz adkktl |
| K = 7 - qg tgq nyack nypy zcjjsk |
| K = 8 - pf sfp mxzbj mxox ybiirj |
| K = 9 - oe reo lwyai lwnw xahhqi |
| K = 10 - nd qdn kvxzh kvmv wzggph |
| K = 11 - mc pcm juwyg julu vyffog |
| K = 12 - lb obl itvxf itkt uxeenf |
| K = 13 - ka nak hsuwe hsjs twddme |
| K = 14 - jz mzj grtvd grir svccld |
| K = 15 - iy lyi fqsuc fqhq rubbkc |
| K = 16 - hx kxh eprtb epgp qtaajb |
| K = 17 - gw jwg doqsa dofo pszzia |
| K = 18 - fv ivf cnprz cnen oryyhz |
| K = 19 - eu hue bmoqy bmdm nqxxgy |
| K = 20 - dt gtd alnpx alcl mpwwfx |
| K = 21 - cs fsc zkmow zkbk lovvew |
| K = 22 - br erb yjlnv yjaj knuudv |
| K = 23 - aq dqa xikmu xizi jmttcu |
| K = 24 - zp cpz whjlt whyh ilssbt |
| K = 25 - yo boy vgiks vgxg hkrras |

Аналізуючи одержані результати, робимо висновок щодо початкового тексту та ключа:

*P* = ‘**si vis pacem para bellum**’, *K* = **5**

# Основні теоретичні відомості з шифру Тритемія

Суть шифру Тритемія схожа до шифру Цезаря, але недоліком другого є повторення букв, за яким можна швидко відгадати слово. Шифр Тритемія запобігає цьому. У шифрі Цезаря ключ є константним, тобто не змінюється. В той час як у шифрі Тритемія ключ може змінюватися за лінійним або квадратичним законами.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| F | A | C | U | L | T | Y |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| F | B | E | X | P | Y | E |

Таб. 1 – Простий шифр Тритемія

У даному випадку ключ залежить від позиції букви у слові, що при повторенні букв видасть різні вихідні букви.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | F | A | C | U | L | T | Y |
|  | x= |  | 5 | 0 | 2 | 20 | 11 | 19 | 24 |
|  | p= |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| K = p + 4 | K= |  | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  | y= |  | 9 | 5 | 8 | 1 | 19 | 2 | 8 |
|  |  |  | J | F | I | B | T | C | I |

Таб. 2 – Шифр Тритемія за лінійним законом

Функцією за якою визначається ключ є: , де параметрами А і В слугують числа – 1 і 4. На таблиці показано як із початкового положення букв у алфавіті(х) відбувається перетворення до кінцевого(y). Спочатку розпишемо позиції(рядок p), застосуємо функцію K(p), додамо значення функції до x, і поділимо результат за модулем на кількість букв у алфавіті.

Розглянемо задачу перехоплення параметрів А і В за відомими початковим текстом та зашифрованим.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | F | A | C | U | L | T | Y |
|  | x= |  | 5 | 0 | 2 | 20 | 11 | 19 | 24 |
|  | p= |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| K = Аp + В | K= |  | 5 | 7 | 9 | 11 | 13 | 15 | 17 |
|  | y= |  | 10 | 7 | 11 | 5 | 24 | 8 | 15 |
|  |  |  | K | H | L | F | Y | I | P |

Таб. 3 – Дано два тексти

Складемо систему двох рівнянь:

де y0 – розміщення першої букви зашифрованого слова у алфавіті,

х0 – розміщення першої букви початкового слова у алфавіті,

y1 – розміщення другої букви зашифрованого слова у алфавіті,

х1 – розміщення другої букви початкового слова у алфавіті,

p0 – позиція першої букви – дорівнює нулю,

p1 – позиція другої букви – дорівнює одиниці,

Усі потрібні значення відомі, підставивши у систему знайдемо коефіцієнти:

звідси маємо: А = 2, B = 5

Розглянемо шифр Тритемія за квадратичним законом. В цьому випадку ключ задається за формулою:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | F | A | C | U | L | T | Y |
| x= |  | 5 | 0 | 2 | 20 | 11 | 19 | 24 |
| p= |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| K= |  | 3 | 6 | 11 | 18 | 1 | 12 | 25 |
| y= |  | 8 | 6 | 13 | 12 | 12 | 5 | 23 |
|  |  | I | G | N | M | M | F | X |

Таб. 4 – Шифр Тритемія за квадратичним законом.

У прикладі вище коефіцієнти такі: А = 1, B = 2, C = 3

У вирішенні задачі дешифрування шифру Тритемія за квадратичним законом можна перебрати усі варіанти доступних коефіцієнтів або розв’язати систему трьох рівнянь.

# Завдання з шифру Тритемія

3. Зашифруємо текст «…», користуючись шифром Тритемія за лінійним законом з параметрами *A* = …, *B* = …

Результат шифрування:

…

4. Дано початковий текст та криптотекст, одержаний шифруванням Тритемія за лінійним законом з невідомими параметрами *A*, *B* ( *A*, *B* – цілі числа від 1 до 5):

*plaintext* = '…', *cryptotext* = '…'

Визначимо параметри *А, В*:

5. Зашифруємо текст «…», користуючись шифром Тритемія за квадратичним законом з параметрами *A* = …, *B* = …, *С* = … (*A*, *B*, *С* ϵ [1; 5]):

Результат шифрування:

…

6. Дано криптотекст, одержаний шифруванням Тритемія за квадратичним законом з невідомими параметрами *A*, *B*, *С* ( *A*, *B*, *С* – цілі числа від 1 до 5):

…

Одержимо всі варіанти його дешифрування для *A*, *B*, *С* ϵ [1; 5]:

…

Аналізуючи одержані результати, робимо висновок щодо початкового тексту та значень параметрів *A*, *B*, *С*:

*P* = '…', *A* = …, *B* = …, *С* = …

# Список літератури

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Диалектика, 2003. – 610 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.
4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: «Вильямс», 2001. – 672 с.
5. Сингх С. Книга шифров. Тайная история шифров и их расшифровки, Пер. с англ. – М.: «Астрель», 2007. – 447 с.

# Додаток 1

Текст програми, що реалізує криптосистему Цезаря

# Додаток 2

Текст програми, що реалізує криптосистему Тритемія