ЛАБОРАТОРНА РОБОТА №2

Тема: КЛАСИЧНІ ШИФРИ ПЕРЕСТАНОВКИ.

Дидактична мета заняття: Набути уміння та навички розробки та описання програм для створення криптограм шифрами перестановки

Розвиваюча мета заняття: Розвивати творчість та культуру написання програм. Розвивати логічне мислення, увагу, уяву, кмітливість

Виховна мета заняття: Виховувати охайність, культуру спілкування, ввічливість , дисциплінованість, наполегливість у навчанні, дбайливе ставлення до програмного забезпечення та ПК.

Програмне забезпечення: Builder C++, PHP

Технічні засоби навчання: комп'ютер.

I. Вступний інструктаж

Повторити правила техніки безпеки при роботі за ПК

II. Теоретична частина

1 Шифр перестановки " Скитала "

У V столітті до нашої ери правителі Спарти мали добре відпрацьовану систему секретного військового зв'язку і шифрували свої послання за допомогою *скитала*, першого найпростішого криптографічного пристрою, що реалізує метод простої перестановки.

Шифрування виконувалося в такий спосіб. На стрижень циліндричної форми, що називався *скитала*, намотували спіраллю (виток до витка) смужку пергаменту й писали на ній уздовж стрижня кілька рядків тексту повідомлення (рис. 1). Потім знімали зі стрижня смужку пергаменту з написаним текстом. Букви на цій смужці виявлялися розташованими хаотично. Такий самий результат можна одержати, якщо букви повідомлення писати по кільцю не підряд, а через певне число позицій доти, поки не буде вичерпаний весь текст.

	Н	Е	Д	О	П
	У	С	Т	И	М
	І	_	З	Н	А
	Ч	Е	Н	Н	Я

Рисунок 1 – Шифр "Скитала"

Повідомлення «НЕДОПУСТИМІ ЗНАЧЕННЯ» при розміщенні його по окружності стрижня по п'ять букв дає шифротекст

НУІЧЕ С_ЕДТ ЗНОИН НПМАЯ.

Для розшифрування такого шифротексту потрібно не тільки знати правило шифрування, але й мати ключ у вигляді стрижня певного діаметра. Знаючи тільки вид шифру, але, не маючи ключа, розшифрувати повідомлення було непросто. Шифр "Скитала" багаторазово вдосконалювався в наступні часи.

2 Таблиці для шифрування

У розроблених шифрах перестановки епохи Відродження (кінець XIV сторіччя) застосовуються таблиці, що шифрують, які, по суті, задають правила перестановки букв у повідомленні.

У ролі ключа таблиці для шифрування використовують:

- розмір таблиці;
- слово або фразу, що задають перестановку;
- особливості структури таблиці.

2.1 Таблиці для шифрування. Проста перестановка

Одним із самих примітивних табличних шифрів перестановки є проста перестановка, для якої ключем є розмір таблиці. Цей метод шифрування подібний із шифром скитала.

Наприклад, повідомлення «ЗАГРОЗА ІСНУЄ ЗАВЖИ І ВСЮДИ» записується в таблицю по стовпцях. Результат заповнення таблиці з 4 рядків і 6 стовпців показаний на рис. 2.

З	А	Г	Р	О	З
А	І	С	Н	У	Є
З	А	В	Ж	Д	И
І	В	С	Ю	Д	И

Рисунок 2 – Заповнення таблиці з 4 рядків і 6 стовпців

Після заповнення таблиці текстом повідомлення по стовпцях для формування шифротексту зчитують вміст таблиці по рядках.

Якщо шифротекст записувати групами по чотири букви, виходить таке шифроване повідомлення:

ЗАЗІ АІАВ ГСВС РНЖЮ ОУДД ЗЄИИ

Природно, відправник і одержувач повідомлення повинні заздалегідь домовитися про загальний ключ – розмір таблиці.

2.2 Таблиці для шифрування. Одиночна перестановка по ключу

Трохи більшою стійкістю до розкриття володіє метод шифрування, який називають одиночною перестановкою по ключу. Цей метод відрізняється від попередніх тим, що стовпці таблиці переставляються за ключовим словом, фразою або набором чисел. Довжина ключового слова задає кількість стовпців таблиці.

Візьмемо як ключ, наприклад, слово “ЗАХИСТ”, а текст повідомлення візьмемо з попереднього прикладу. На рис. 3 показані дві таблиці, заповнені текстом повідомлення та ключовим словом при цьому ліва таблиця відповідає заповненню до перестановки, а права таблиця – заповненню після перестановки.

З	А	Х	И	С	Т
2	1	6	3	4	5
З	А	Г	Р	О	З
А	І	С	Н	У	Є
З	А	В	Ж	Д	И
І	В	С	Ю	Д	И

До перестановки

А	З	И	С	Т	Х
1	2	3	4	5	6
А	З	Р	О	З	Г
І	А	Н	У	Є	С
А	З	Ж	Д	И	В
В	І	Ю	Д	И	С

Після перестановки

Рисунок 3 – Таблиці, заповнені ключовим словом і текстом повідомлення

У верхньому рядку лівої таблиці записаний ключ, а номери під буквами ключа визначені відповідно до природного порядку відповідних букв ключа в алфавіті. Якби в ключі трапилися однакові букви, вони б були понумеровані зліва на право. У правій таблиці стовпці переставлені відповідно до порядкових номерів букв ключа.

При зчитуванні вмісту правої таблиці по стовпцях і запису шифротексту групами по п’ять букв одержимо шифроване повідомлення:

АІАВЗ АЗІРН ЖЮОУД ДЗЄИИ ГСВС

2.3 Таблиці для шифрування. Подвійна перестановка

Для забезпечення додаткової секретності можна повторно зашифрувати повідомлення, що вже пройшло шифрування. Такий метод шифрування називається подвійною перестановкою. У випадку подвійної перестановки стовпців і рядків таблиці перестановки визначаються окремо для стовпців і окремо для рядків. Спочатку в таблицю записується текст повідомлення, а потім по черзі переставляються стовпці, а потім рядки. При розшифруванні порядок перестановок повинен бути зворотним.

Наприклад, виконаємо методом подвійної перестановки шифрування тексту «ЗАГРОЗА ІСНУЄ ЗАВЖИ І ВСЮДИ» із ключем 416325 (стовпці) 2431 (рядки).

Шифрування тексту методом подвійної перестановки показано на рис. 4.

Якщо зчитувати шифротекст із правої таблиці порядково блоками по п’ять літер, то вийде таке:

ВДЮІИ САОРЗ ЗГАДЖ ЗИВІУ НАЄС.

	4	**1**	**6**	**3**	**2**	**5**
2	З	А	Г	Р	О	З
4	А	І	С	Н	У	Є
3	З	А	В	Ж	Д	И
1	І	В	С	Ю	Д	И

	1	**2**	**3**	**4**	**5**	**6**
2	А	О	Р	З	З	Г
4	І	У	Н	А	Є	С
3	А	Д	Ж	З	И	В
1	В	Д	Ю	І	И	С

	1	**2**	**3**	**4**	**5**	**6**
1	В	Д	Ю	І	И	С
2	А	О	Р	З	З	Г
3	А	Д	Ж	З	И	В
4	І	У	Н	А	Є	С

Рисунок 4 – Приклад виконання шифрування методом подвійної перестановки

Число варіантів подвійної перестановки швидко зростає при збільшенні розміру таблиці.

Розмір таблиці	Кількість варіантів перестановки
3×3	36
4×4	576
5×5	14400

Однак подвійна перестановка не відрізняється високою стійкістю та порівняно просто «зламується» при будь-якому розмірі таблиці шифрування.

2.4 Застосування магічних квадратів

Магічними квадратами називають квадратні таблиці, в кожну клітинку яких вписано послідовні натуральні числа починаючи з 1, які дають у сумі по кожному стовпцю, кожному рядку і кожній діагоналі те саме число.

Текст, що шифрується, вписується в магічні квадрати відповідно до нумерації їх клітинок. Якщо потім виписати вміст такої таблиці по рядках, то вийде шифротекст, сформований завдяки перестановці букв вихідного повідомлення.

Наприклад, методом магічного квадрата виконати шифрування тексту «ВІРТУАЛЬНИЙ КАНАЛ» .

Шифрування тексту зробимо з використанням магічного квадрата розміром 4×4 (рис. 5) .

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Л	Р	І	А
У	И	Й	Ь
Н	А	Л	К
Т	А	Н	В

Рисунок 5 – Приклад магічного квадрата 4×4
і його заповнення повідомленням

Шифротекст, який одержали при зчитуванні вмісту правої таблиці по рядках групами по чотири букви, має такий вигляд:

ЛРІА УИЙЬ НАЛК ТАНВ.

Число магічних квадратів швидко зростає зі збільшенням розміру квадрата. Існує тільки один магічний квадрат розміром 3×3 (якщо не враховувати його повороти). Кількість магічних квадратів 4×4 становить уже 880, а кількість магічних квадратів 5×5 – близько 250000.

III. Хід виконання роботи

1. Постановка задачі.

Виконати завдання з додатку 1 та 2 на оцінку 3, на оцінку 4-5 додаток 1+2+3. Наступні пункти завдання необхідні для 3 додатку.

2. Побудова математичної моделі

Потрібно скористатись або вивести математичні формули для розв’язання завдання.

3. Побудова алгоритму

Розробити блок-схему в якій відобразити порядок виконання обчислювальних операцій на основі математичної моделі.

4. Складання сценарію діалогу ПК з користувачем

Визначити правила роботи людини з ПК, правила введення даних, форму подання інформації користувачу.

5. Складання програми

Описуємо лістинг програми

6. Відлагодження

Виправляємо помилки при компіляції.

7. Тестування програми.

Перевіряємо роботу програми. Дані потрібно вводити такі, щоб результат роботи програми був відомий вам на перед. Дані можна взяти з математичної моделі.

8. Оформити звіт.

IV. Зміст звіту

1. Тема
2. Мета
3. Хід робити(з пунктами 1-7)
4. Висновок

V. Контрольні питання

1. Дайте визначення таких понять: алфавіт, текст, шифр, ключ, зашифрування, розшифрування, криптосистема, розкриття шифру, стійкість крипто алгоритму.
2. У чому полягає відмінність процесів розшифрування та розкриття шифрів?
3. Сформулюйте алгоритм шифрування тексту одиночною перестановкою по ключу.
4. Сформулюйте алгоритм шифрування тексту подвійною перестановкою.
5. Що використовують у ролі ключа таблиці для шифрування?
6. До якого типу відносять шифри перестановки?
7. Яка шифр називають симетричним?
8. Що називають ключем шифрування?
9. Поясніть алгоритм роботи шифру "Звичайна перестановка"
10. Поясніть алгоритм роботи шифру "Звичайні рядково-стовпчикові табличні перестановки"
11. Поясніть алгоритм роботи шифру "Рядково-стовпчикові табличні перестановки із застосуванням ключа рядків"
12. Поясніть алгоритм роботи шифру "Рядково-стовпчикові табличні перестановки з двома ключами"
13. Поясніть алгоритм роботи шифру "Табличні перестановки з використанням трафарету"

VI. Список літератури

1 Усатенко Т.М. Криптологія: Навчальний посібник. – Суми: Вид-во СумДУ, 2008. – 164 с.
2 Шнайдер Брюс. Прикладная криптология. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002
3 Столлингс Вильям. Криптография и защита сетей: принципы и практика /Пер. с англ – М.: Издательский дом «Вильямс», 2001.
4 Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001.
5 Брассар Ж. Современная криптология / Пер с англ. – М.: Полимед, 1999.
6 Жельников В. Криптография от папируса до компьютера. –М.: ABF, 1996.
7 Введение в криптографию /Под общей ред. В.В. Ященко. – СПб.: Питер, 2001.

Додаток 1.

Виконайте шифрування тексту одиночною перестановкою по ключу.

Варіант	Відкритий текст	Ключ
1	THERE LIVED IN A VILLAGE A MAN WHOSE NAME WAS PETER. HIS NICKNAME, HOWEVER, WAS NUMBSKULL	COPYBOOK
2	BUT EVERY TWO STEPS HE WOULD STOP AND CHECK ARE THOSE THREE RUBLES STILL THERE IN HIS POCKET	EMPIRE
3	ALONG THROUGH THE VILLAGE CAME RUNNING A BOY, WHOSE NAME WAS IGNAT.	INFANTRY
4	OFF WENT IGNAT, AND SOON HE FOUND THE THREE RUBLES, LYING UNDER A BURDOCK PLANT.	OUTSIDER
5	IGNAT RAN TO VISIT EVERY DAY, BUT INSTEAD OF BEING ON THE CART, THE WHEELS LAY IN THE SHED	NOTATION
6	ОДНИМ ИЗ САМЫХ ПРИМИТИВНЫХ ТАБЛИЧНЫХ ШИФРОВ ПЕРЕСТАНОВКИ ЯВЛЯЕТСЯ ПРОСТАЯ ПЕРЕСТАНОВКА	МИСТИФИКАЦИЯ
7	НЕСКОЛЬКО БОЛЬШЕЙ СТОЙКОСТЬЮ К РАСКРЫТИЮ ОБЛАДАЕТ МЕТОД ОДИНОЧНОЙ ПЕРЕСТАНОВКОЙ ПО КЛЮЧУ	ДЕЛЕНИЕ
8	ДВОЙНАЯ ПЕРЕСТАНОВКА НЕ ОТЛИЧАЕТСЯ ВЫСОКОЙ СТОЙКОСТЬЮ И СРАВНИТЕЛЬНО ПРОСТО ВЗЛАМЫВАЕТСЯ ПРИ ЛЮБОМ РАЗМЕРЕ ТАБЛИЦЫ ШИФРОВАНИЯ	РЕГРЕССИЯ
9	ШИФРУЕМЫЙ ТЕКСТ ВПИСЫВАЕТСЯ В МАГИЧЕСКИЕ КВАДРАТЫ В СООТВЕТСТВИИ С НУМЕРАЦИЕЙ ИХ КЛЕТОК.	ПРОГРЕССИЯ
10	ПРИ ШИФРОВАНИИ ПОДСТАНОВКОЙ СИМВОЛЫ ШИФРУЕМОГО ТЕКСТА ЗАМЕНЯЮТСЯ СИМВОЛАМИ ТОГО ЖЕ С ЗАРАНЕЕ УСТАНОВЛЕННЫМ ПРАВИЛОМ ЗАМЕНЫ	ИДЕНТИФИКАЦИЯ
11	ТАКОЙ ШИФР ЗАМЕНЫ МОЖНО ЗАДАТЬ ТАБЛИЦЕЙ ПОДСТАНОВОК, СОДЕРЖАЩЕЙ СООТВЕТСТВУЮЩИЕ ПАРЫ БУКВ ОТКРЫТОГО ТЕКСТА И ШИФРТЕКСТА.	ЗАКОН
12	УСТАНОВИМ ВЗАИМНО ОДНОЗНАЧНОЕ СООТВЕТСТВИЕ МЕЖДУ АЛФАВИТОМ И МНОЖЕСТВОМ ЦЕЛЫХ ЧИСЕЛ	СПРАВОЧНИК

Додаток 2.

Виконайте шифрування тексту подвійною перестановкою.

Варіант	**Відкритий текст**	**Ключ (стовбці-рядки)**
1.	AND PETER THE NUMBSKULL WAS LEFT STANDING ON THE TABLE, WITH CHALK TRICKLING OFF HIS UGLY MUG, AND GRASS FLYING OUT OF HIS POCKET.	4 6 2 8 5 3 7 1 9 – 5 13 8 6 11 7 9 12 4 10 1 3 2
2.	IGNAT RAN TO VISIT EVERY DAY, BUT INSTEAD OF BEING ON THE CART, THE WHEELS LAY IN THE SHED	9 10 8 3 6 4 2 5 7 1 – 5 7 3 6 1 2 4
3.	УСТАНОВИМ ВЗАИМНО ОДНОЗНАЧНОЕ СООТВЕТСТВИЕ МЕЖДУ АЛФАВИТОМ И МНОЖЕСТВОМ ЦЕЛЫХ ЧИСЕЛ	1 15 13 2 6 11 9 10 14 3 12 8 5 4 7 – 5 2 3 4 1
4.	HE GRABBED THOSE THREE RUBLES AND HID THEM DEEP DOWN IN HIS POCKET.	6 3 2 5 4 1 – 1 9 3 7 5 6 4 8 2
5.	OFF WENT IGNAT, AND SOON HE FOUND THE THREE RUBLES, LYING UNDER A BURDOCK PLANT.	8 2 6 4 5 3 1 7 – 1 3 5 2 6 4 8 7
6.	ALONG THROUGH THE VILLAGE CAME RUNNING A BOY, WHOSE NAME WAS IGNAT.	7 5 4 8 9 6 3 1 2 – 4 3 5 2 6 1
7.	ШИФРУЕМЫЙ ТЕКСТ ВПИСЫВАЕТСЯ В МАГИЧЕСКИЕ КВАДРАТЫ В СООТВЕТСТВИИ С НУМЕРАЦИЕЙ ИХ КЛЕТОК	6 2 5 1 3 4 7 – 11 2 5 1 3 10 8 4 6 7 9
8.	PETER THE NUMBSKULL SAT DOWN ON A LOG AND BURST INTO TEARS	6 2 5 3 1 4 8 7 – 5 3 1 6 2 4
9.	ДВОЙНАЯ ПЕРЕСТАНОВКА НЕ ОТЛИЧАЕТСЯ ВЫСОКОЙ СТОЙКОСТЬЮ И СРАВНИТЕЛЬНО ПРОСТО ВЗЛАМЫВАЕТСЯ	1 5 3 6 4 8 9 11 2 7 10 - 7 1 6 2 5 3 4 8
10.	ПРИ СЧИТЫВАНИИ СОДЕРЖИМОГО ПРАВОЙ ТАБЛИЦЫ ПО СТРОКАМ ПОЛУЧИМ ШИФРОВАННОЕ СООБЩЕНИЕ	1 15 13 2 6 11 9 10 14 3 12 8 5 4 7 – 1 5 2 4 3
11.	BUT EVERY TWO STEPS HE WOULD STOP AND CHECK – ARE THOSE THREE RUBLES STILL THERE IN HIS POCKET?	5 3 1 4 2 – 10 2 15 4 6 11 8 12 9 1 7 3 5 13 14
12.	ONE DAY PETER THE NUMBSKULL HAD THREE RUBLES. HE SHOVED THEM INTO HIS POCKET AND WENT OFF FOR A WALK	2 5 3 6 7 4 8 1 – 9 2 10 5 3 6 7 4 8 1
13.	НЕСКОЛЬКО БОЛЬШЕЙ СТОЙКОСТЬЮ К РАСКРЫТИЮ ОБЛАДАЕТ МЕТОД ОДИНОЧНОЙ ПЕРЕСТАНОВКОЙ ПО КЛЮЧУ	7 1 6 2 5 3 4 – 1 5 3 6 4 8 9 11 2 7 10
14.	THERE LIVED IN A VILLAGE A MAN WHOSE NAME WAS PETER. HIS NICKNAME, HOWEVER, WAS NUMBSKULL	9 1 8 2 3 7 6 4 5 – 1 6 3 5 8 2 4 7
15.	ОДНИМ ИЗ САМЫХ ПРИМИТИВНЫХ ТАБЛИЧНЫХ ШИФРОВ ПЕРЕСТАНОВКИ ЯВЛЯЕТСЯ ПРОСТАЯ ПЕРЕСТАНОВКА	1 5 3 6 4 8 9 11 2 7 10 – 7 1 6 2 5 3 4

Додаток 3.

Реалізувати шифр перестановки на C++ або PHP. Користувач вводить текстове повідомлення, ключ(при необхідності, можна рандомом). Результат роботи програми це криптограма.

Варіанти

1. Звичайна перестановка
2. Звичайні рядково-стовпчикові табличні перестановки
3. Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків
4. Рядково-стовпчикові табличні перестановки із застосуванням ключа рядків
5. Рядково-стовпчикові табличні перестановки з двома ключами
6. Табличні перестановки з використанням квадратного трафарету.
7. Табличні перестановки з використанням прямокутного трафарету.
8. Звичайна перестановка
9. Звичайні рядково-стовпчикові табличні перестановки
10. Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків
11. Рядково-стовпчикові табличні перестановки із застосуванням ключа рядків
12. Рядково-стовпчикові табличні перестановки з двома ключами
13. Табличні перестановки з використанням квадратного трафарету.
14. Табличні перестановки з використанням прямокутного трафарету.
15. Звичайна перестановка
16. Звичайні рядково-стовпчикові табличні перестановки
17. Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків
18. Рядково-стовпчикові табличні перестановки із застосуванням ключа рядків
19. Рядково-стовпчикові табличні перестановки з двома ключами
20. Табличні перестановки з використанням квадратного трафарету.
21. Табличні перестановки з використанням прямокутного трафарету.
22. Звичайна перестановка
23. Звичайні рядково-стовпчикові табличні перестановки
24. Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків
25. Рядково-стовпчикові табличні перестановки із застосуванням ключа рядків