МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ФАХОВИЙ КОЛЕДЖ ПРОМИСЛОВОЇ АВТОМАТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ОДЕСЬКОГО НАЦІОНАЛЬНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ»

ЗАТВЕРДЖУЮ

Заступник директора

з НМР ФКПАІТ ОНТУ

_____/Вікторія ОКСАНІЧЕНКО/

“___”_____2022 року

МЕТОДИЧНІ ВКАЗІВКИ
ДЛЯ ВИКОНАННЯ ПРАКТИЧНИХ РОБІТ

з дисципліни

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

для спеціальності 122 «Комп’ютерні науки»

Одеса

2022 рік

Методичні вказівки до виконання практичних робіт розроблено викладачем Бурмакіна Ю. В. згідно з навчальною програмою дисципліни «Технології захисту інформації»

Схвалено цикловою комісією «Комп'ютерних наук та інженерії програмного забезпечення»

Протокол № « _____» від « ___ »_____ 20 _ р.

Голова циклової комісії _____ _____ Тетяна КОСТИРЕНКО
(підпис) (власне ім'я та прізвище)

Практична робота № 1

Тема: Шифри перестановки. Маршрутна перестановка та перестановка по ключу. Метод шифрування подвійною перестановкою.

Мета роботи: Ознайомитися з алгоритмами шифрування та дешифрування у шифрах поодинокої перестановки по ключу та подвійної перестановки.

Теоретичні відомості

При шифруванні перестановкою символи шифрованого тексту переставляються за певним правилом в межах блоку цього тексту.

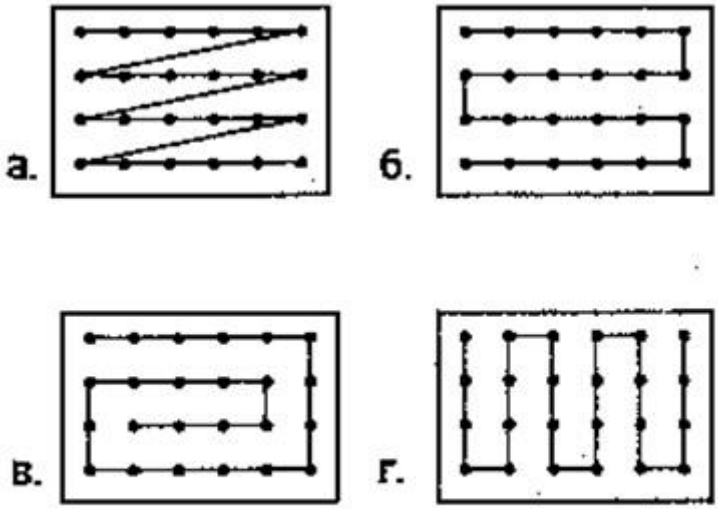


Рисунок 1 – Маршрути запису та читання

Шифруючі таблиці

У шифрах перестановки початку епохи Відродження (кінець XIV століття) часто застосовували шифруючі таблиці, які по суті задають правила перестановки букв в повідомленні.

В якості ключа в шифруючих таблицях використовуються:

- розмір таблиці;
- слово або фраза, задаючі перестановку
- особливості структури таблиці.

Перетворення з цього шифру полягають в тому, що у фігуру вписується по ходу одного "маршруту" початковий текст, а потім по ходу іншого виписується з неї.

Шифр маршрутної перестановки

Шифр перестановки, для якого ключем служить розмір таблиці і маршрут перестановки (особливості структури).

Алгоритм шифрування

Наприклад, зашифруємо повідомлення **ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ**

Використовуємо алфавіт з 32 символів (32 російських букви російського алфавіту).

1) Початкове повідомлення записується в таблицю по горизонталі, починаючи з лівого верхнього кута по черзі, зліва направо і справа наліво (маршрут б на рис 1).

У початковому повідомленні 35 символів, тому вибираємо таблицю з 5 рядків і 7

стовпців (5*7=35 символів). Результат заповнення таблиці показаний на рис.

Т	**Е**	**Р**	**М**	**И**	**Н**	**А**
Б	**И**	**Р**	**П**	**Р**	**О**	**Т**
Ы	**В**	**А**	**Е**	**Т**	**С**	**Е**
В	**О**	**Г**	**О**	**М**	**Ь**	**Д**
П	**О**	**Л**	**Н**	**О**	**Ч**	**Ь**

2) Для формування шифртекста прочитують вміст таблиці по вертикалі, починаючи з верхнього правого кута і рухаючись по черзі зверху вниз і від низу до верху (маршрут г на рис. 3).

Якщо шифртекст записувати групами по п'ять букв, виходить таке шифроване повідомлення: **АТЕДЬ ЧЬСОН ИРТМО НОЕПМ РРАГЛ ООВИЕ ТБЫВП**

Звісно, посилач і одержувач повідомлення повинні заздалегідь умовитися про загальний ключ у вигляді розміру таблиці і маршрут. Об'єднання букв шифртекста в 5-буквені групи не входить в ключ шифру і здійснюється для зручності запису несмислового тексту.

Алгоритм дешифрування

При розшифруванні дії виконують в зворотному порядку.

Дещо більшу стійкість до розкриття має метод шифрування, що називається поодинокою перестановкою по ключу.

Шифр поодинокої перестановки по ключу

Цей метод відрізняється від попереднього тим, що стовпці таблиці переставляються по ключовому слову, фразі або набору чисел завдовжки в рядок таблиці.

Алгоритм шифрування

Зашифруємо повідомлення **ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ**

В якості ключа використаємо слово **ПЕЛИКАН.**

Використовуємо алфавіт з 32 символів(32 російських букви російського алфавіту).

1	2	3	4	5	6	7	8	9	10
А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**

11	12	13	14	15	16	17	18	19	20
К	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**

21	22	23	24	25	26	27	28	29	30
Ф	**Х**	Ц	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**

31	32
Ю	**Я**

1) По ключу і початковому повідомленню формуються таблиця.

Кількість стовпців в таблиці відповідає кількості символів ключового слова.

$$\mathbf{n_{столб}} = \ell_{\mathbf{k}}.$$

В нашому випадку $\mathbf{n_{столб} = 7}$

Кількість рядків в таблиці визначається відношенням кількості символів відкритого повідомлення до довжини ключового слова плюс два рядки (одна на ключове слово, друга для нумерації символів ключа).

$$\mathbf{n_{строк} = \frac{\ell_m}{\ell_k} + 2}$$

$$\mathbf{n_{строк} = \frac{35}{7} + 2 = 5 + 2 = 7}$$

2) Заповнюється ліва таблиця:

а) перший рядок - ключ;

б) другий рядок - записуються номери букв ключового слова, які визначені відповідно до природного порядку їх розташування в алфавіті

в) далі початкове повідомлення записується в таблицю по черзі по стовпцях.

3) В правій таблиці стовпці переставлені відповідно до впорядкованих номерів букв ключа.

На рис 4 показані дві таблиці, заповнені текстом повідомлення і ключовим словом, при цьому ліва таблиця відповідає заповненню до перестановки, а права таблиця - заповненню після перестановки.

ПЕЛИКАН.

П	Е	Л	И	К	А	Н
7	2	5	3	4	1	6
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	0	Н
Р	Т	И	Е	Ь	В	О
М	о	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

До перестановки

А	Е	И	К	Л	Н	П
1	2	3	4	5	6	7
Г	Н	В	Е	П	Л	Т
0	А	А	Д	Р	Н	Е
В	Т	Е	Ь	И	0	Р
П	0	Т	М	Б	Ч	М
О	Р	С	О	Ы	Ь	И

После перестановки

Рисунок 4 – Таблиці заповнені ключовим словом і текстом повідомлення

4) Для формування шифртекста прочитують вміст правої таблиці по рядках (рядки, де знаходилося початкове повідомлення).

При записі шифртекста групами по п'ять букв отримаємо шифроване повідомлення: **ГНВЕП ЛТОАА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ**

Примітка

Якби в ключі зустрілися однакові букви, вони б були пронумеровані зліва направо.

Алгоритм дешифрування

Наприклад:

шифртекст

ЬЛНМФТИТОНААЕНЕГЫЦКХФТИХИ УНО_Й _ОЛОР

ключ: КАФЕДРА

Використовуємо алфавіт з 33 символів (32 російських букви російського алфавіту і пропуск.

1	2	3	4	5	6	7	8	9	10
А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**

11	12	13	14	15	16	17	18	19	20
К	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**

21	22	23	24	25	26	27	28	29	30
Ф	**Х**	Ц	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**

31	32	пробел
Ю	**Я**	_

1) По ключу і шифртексту формуються таблиця.

Кількість стовпців в таблиці відповідає кількості символів ключового слова.

$$\mathbf{n_{столб} = \ell_k}$$

В нашому випадку $\mathbf{n_{столб} = 7}$

Кількість рядків в таблиці визначається відношенням кількості символів шифртекста до довжини ключового слова плюс два рядки(при підрахунку кількості символів, відкидаємо пробіли між групами з п'яти символів).

$$\mathbf{n_{строк} = \frac{\ell_c}{\ell_k} + 2}$$

В нашому випадку $\mathbf{n_{строк} = \frac{35}{7} + 2 = 5 + 2 = 7}$

2) Заповнюється права таблиця:

а) перший рядок - символи ключа по порядку в алфавіті;

б) другий рядок - записуються номери букв ключового слова, які визначені відповідно до природного порядку їх розташування в алфавіті

в) далі шифртекст записується в таблицю по черзі по рядках.

3) В лівій таблиці стовпці переставлені так, щоб у верхньому рядку вийшло ключове слово.

К	**А**	**Ф**	**Е**	**Д**	**Р**	**А**
5	1	7	4	3	6	2
Ф	Ь	И	М	Н	Т	Л
А	Т	Н	А	Н	Е	О
К	Е	Ф	Ц	Ы	Х	Г
У	Т	О	И	Х	Н	И
Л	_	Р	О	_	О	Й
Левая						

А	**А**	**Д**	**Е**	**К**	**Р**	**Ф**
1	2	3	4	5	6	7
Ь	Л	Н	М	Ф	Т	И
Т	О	Н	А	А	Е	Н
Е	Г	Ы	Ц	К	Х	Ф
Т	И	Х	И	У	Н	О
_	Й	_	О	Л	О	Р
правая						

←

4) Для формування початкового повідомлення прочитують вміст лівої таблиці по стовпцях (рядки, де знаходився шифртекст).

Початкове повідомлення:

ФАКУЛЬТЕТ_ИНФОРМАЦИОННЫХ_ТЕХНОЛОГИЙ

Шифр вертикальної перестановки

Алгоритм шифрування

Використовуємо алфавіт з 32 символів (32 російських букви російського алфавіту).

Застосуємо в якості ключа, наприклад, слово **ПЕЛИКАН,** а текст повідомлення **ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ**

1) По ключу і початковому повідомленню формуються таблиця.

Кількість стовпців в таблиці відповідає кількості символів ключового слова.

$$\mathbf{n_{столб} = \ell_k}$$

В нашому випадку $\mathbf{n_{столб} = 7}$

Кількість рядків в таблиці визначається відношенням кількості символів відкритого повідомлення до довжини ключового слова плюс два рядки(одна на ключове слово, друга для нумерації символів ключа)

$$n_{строк} = \frac{\ell_m}{\ell_k} + 2$$

В нашому випадку $\mathbf{n_{строк} = \frac{35}{7} + 2 = 5 + 2 = 7}$

2) Заповнюється ліва таблиця:

а) перший рядок - ключ;

б) другий рядок - записуються номери букв ключового слова, які визначені відповідно до природного порядку їх розташування в алфавіті

в) далі початкове повідомлення записується в таблицю по черзі по рядках.

3) В правій таблиці стовпці переставлені відповідно до впорядкованих номерів букв ключа.

П	**Е**	**Л**	**И**	**К**	**А**	**Н**
7	2	5	3	4	1	6
Т	Е	Р	М	И	Н	А
Т	О	Р	П	Р	И	Б
Ы	В	А	Е	Т	С	Е
Д	Ь	М	О	Г	О	В
П	О	Л	Н	О	Ч	Ь
левая до перестановки						

А	**Е**	**И**	**К**	**Л**	**Н**	**П**
1	2	3	4	5	6	7
Н	Е	М	И	Р	А	Т
И	О	П	Р	Р	Б	Т
С	В	Е	Т	А	Е	Ы
О	Ь	О	Г	М	В	Д
Ч	О	Н	О	Л	Ь	П
правая после перестановки						

——————————————————————————————→

4) Для формування шифртекста прочитують вміст правої таблиці по стовпцях(рядки, де знаходилося початкове повідомлення).

При записі шифртекста групами по п'ять букв отримаємо шифроване повідомлення:

НИСОЧ ЕОВЬО МПЕОН ИРТГО РРАМЛ АБЕВЬ ТТЫДП

Примітка: Якби в ключі зустрілися однакові букви, вони б були пронумеровані зліва направо.

Алгоритм дешифрування

Використовуємо алфавіт з 33 символів(32 російських букви російського алфавіту і пропуск.

Наприклад:

ключ: кафедра

шифртекст:

АТМЫО ТОНХЙ ЛНИТГ УИЦ_О ФЕРНН ЬФОЕИ К_АХЛ

1) По ключу і шифртексту формуються таблиця.

Кількість стовпців в таблиці відповідає кількості символів ключового слова.

$$\mathbf{n_{столб} = \ell_k}$$

В нашому випадку $\mathbf{n_{столб} = 7}$

Кількість рядків в таблиці визначається відношенням кількості символів шифртекста до довжини ключового слова плюс два рядки(при підрахунку кількості символів, відкидаємо пробіли між групами з п'яти символів)

$$n_{строк} = \frac{\ell_c}{\ell_k} + 2$$

В нашому випадку $\mathbf{n_{строк} = \frac{35}{7} + 2 = 5 + 2 = 7}$

2) Заповнюється права таблиця:

а) перший рядок - символи ключа по порядку в алфавіті;

б) другий рядок - записуються номери букв ключового слова, які визначені відповідно до природного порядку їх розташування в алфавіті

в) далі шифртекст записується в таблицю по черзі по стовпцях.

3) В лівій таблиці стовпці переставлені так, щоб у верхньому рядку вийшло ключове слово.

К	А	Ф	Е	Д	Р	А
5	1	7	4	3	6	2
Ф	А	К	У	Л	Ь	Т
Е	Т	_	И	Н	Ф	О
Р	М	А	Ц	И	О	Н
Н	Ы	Х	_	Т	Е	Х
Н	О	Л	О	Г	И	Й
Левая						

А	А	Д	Е	К	Р	Ф
1	2	3	4	5	6	7
А	Т	Л	У	Ф	Ь	К
Т	О	Н	И	Е	Ф	_
М	Н	И	Ц	Р	О	А
Ы	Х	Т	_	Н	Е	Х
О	Й	Г	О	Н	И	Л
правая						

←————————————————

4) Для формування початкового повідомлення прочитують вміст лівої таблиці по рядках(рядки, де знаходився шифртекст).

Початкове повідомлення:

ФАКУЛЬТЕТ_ИНФОРМАЦИОННЫХ_ТЕХНОЛОГИЙ

Для забезпечення додаткової скритності можна повторно зашифрувати повідомлення, яке вже пройшло шифрування. Такий метод шифрування називається подвійною перестановкою. У разі подвійної перестановки стовпців і рядків таблиці перестановки визначаються окремо для стовпців і окремо для рядків.

Алгоритм шифрування

Початкове повідомлення

ПРИЛЕТАЮ ВОСЬМОГО

Ключем до шифру подвійної перестановки служить послідовність номерів стовпців і номерів рядків початкової таблиці (у нашому прикладі послідовності 4132 і 3142 відповідно).

$\mathbf{k_{столб} = 4132}$ $\mathbf{k_{строк} = 3142}$

1) Спочатку в початкову таблицю відрядковий записується текст повідомлення

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

Исходная таблица

	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

Перестановка столбцов

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

Перестановка строк

Рис. 2.3. Пример выполнения шифрования методом двойной перестановки

2) По черзі переставляються стовпці

3) По черзі переставляються рядки

4) Прочитують шифртекст з правої таблиці(таблиця перестановки рядків) відрядковими блоками по чотири букви:

ТЮАЕ ООГМ РЛИП ОЬСВ

При розшифровці порядок перестановок має бути зворотним.

Алгоритм дешифрування

Шифртекст

АЗЮЖ Е_СШ ГТОО ИПЕР

Ключем до шифру подвійної перестановки служить послідовність номерів стовпців і номерів рядків початкової таблиці(у нашому прикладі послідовності 2413 і 4123 відповідно).

$\mathbf{k_{столб} = 2413}$ $\mathbf{k_{строк} = 4123}$

1) Спочатку в праву таблицю перестановок рядків записується текст шифртекста відрядковий

	2	4	1	3
4	П	Р	И	Е
1	З	Ж	А	Ю
2	_	Ш	Е	С
3	Т	О	Г	О

Початкове повідомлення

Ліва таблиця

	1	2	3	4
4	И	П	Е	Р
1	А	З	Ю	Ж
2	Е	_	С	Ш
3	Г	Т	О	О

Перестановка рядків

Права таблиця

	1	2	3	4
1	А	З	Ю	Ж
2	Е	_	С	Ш
3	Г	Т	О	О
4	И	П	Е	Р

2) По черзі переставляються рядки

3) По черзі переставляються стовпці

4) Прочитують початкове повідомлення з лівої таблиці відрядковий:

ПРИЕЗЖАЮ_ШЕСТОГО

Число варіантів подвійної перестановки швидко зростає при збільшенні розміру таблиці :

- для таблиці 3x3 36 варіантів;
- для таблиці 4x4 576 варіантів;
- для таблиці 5x5 14400 варіантів.

Проте подвійна перестановка не відрізняється високою стійкістю і порівняно просто "зламується" при будь-якому розмірі таблиці шифрування.

Постановка задачі

1. Ознайомитися з особливостями шифрів перестановки.
2. Сформулювати алгоритм шифрування.
3. У відповідності з номером студентського квитка з таблиці 1 вибрати вихідні дані до виконання завдання
4. Зашифрувати відкрите повідомлення згідно свого варіанту
5. Обмінятися даними з сусідом по парті та виконати дешифрування
6. Визначити ефективність і криптостійкість шифру

Контрольні питання:

1. Що таке шифри перестановки?
2. Опишіть алгоритм роботи шифрів перестановки.

Практична робота № 2

Тема: Шифри заміни. Шифр Цезаря. Афінна система підстановок Цезаря.

Мета роботи: Ознайомитися з шифрами заміни на прикладі шифру Цезаря.

Теоретичні відомості

При шифруванні заміною (підстановкою) символи шифрованого тексту замінюються символами того ж або іншого алфавіту із заздалегідь встановленим правилом заміни.

Шифри підстановки можуть бути розбиті на дві категорії: моноалфавітні або багатоалфавітні шифри.

МОНОАЛФАВІТНІ (ОДНОАЛФАВІТНІ) ШИФРИ

У моноалфавітній підстановці буква (чи символ) в початковому тексті завжди змінюється на одну і ту ж саму букву (чи символ) в зашифрованому тексті незалежно від його позиції в тексті.

Букви в початковому тексті і зашифрованому тексті знаходяться у відношенні "один до одного".

Приклад 1

Початковий текст: H E L L O

Зашифрований текст: K H O O R

Приклад 2

Початковий текст: H E L L O
Зашифрований текст: A B N Z F

Шифр "Атбаш"

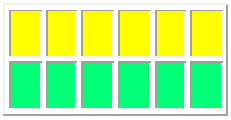
Правило шифрування полягало в заміні 1-ої букви алфавіту буквою з номером $\mathbf{n-i+1}$, де n - число букв алфавіту.

Це слово складене з букв Алеф, Тае, Бет і Шин, тобто першою і останньою, другою і передостанньою буквою давньосемітського алфавіту.

Приклад

У алфавіті A, B, C, кома, точка, плюс.

Таблиця заміни :



Зашифруємо текст: A+ B

Криптограма: +A.

Якщо шифр атбаш використовуваний для алфавіту з непарним числом символів, символ, який посередині алфавіту, не замінюється.

Шифр атбаш є шифром без ключа, тобто веде заміну символів завжди однаково при заданому алфавіті.

Це означає, що вимагається виключити знання супротивником, що використовується саме цей шифр, інакше навіть вручну зашифрований текст швидко прочитується.

Шифр атбаш є шифром простої заміни.

ШИФРИ ПРОСТОЇ ЗАМІНИ

У шифрі простої заміни кожен символ початкового тексту замінюється на один і той же символ з того ж алфавіту незалежно від його позиції в тексті.

Шифр простої заміни є моноалфавітним шифром.

СИСТЕМА ШИФРУВАННЯ ЦЕЗАРЯ

Шифр Цезаря є часткою випадком шифру простої заміни.

Цезарь замінював букви відповідно до підстановки, нижній рядок якої є алфавітом відкритого тексту, зрушеним циклічно на три букви вліво.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
X	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**

K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
H	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**

U	**V**	**W**	**X**	**Y**	**Z**
R	**S**	**T**	**U**	**V**	**W**

Таким чином при шифруванні початкового тексту кожна буква замінювалася на іншу букву того ж алфавіту шляхом зміщення за абеткою від початкової букви на три.

Після закінчення алфавіту здійснювався циклічний перехід до його початку. Тобто Цезарь використав шифр заміни з ключем зміщення K=3.

У системі шифрування Цезаря кожен символ початкового тексту замінюється символом того ж алфавіту, віддаленим від початкового на певне число позицій в алфавіті залежно від значення ключа.

Алгоритм шифрування

1. Задамо алфавіт з 26 символів (букви англійського алфавіту, m=26)

2. №	0	1	2	3	4	5	6	7	8	9
символ	A	B	C	D	E	F	G	H	I	J

№	10	11	12	13	14	15	16	17	18	19
символ	K	L	M	N	O	P	Q	R	S	T

№	20	21	22	23	24	25
символ	U	V	W	X	Y	Z

і значення ключа k . $\mathbf{k = \overline{1,m-1}}$

2. Для кожного символу відкритого тексту $\mathbf{PT = \{p_i\}}$, $\mathbf{i = \overline{1,n}}$:

а) визначаємо порядковий номер символу відкритого повідомлення в алфавіті $\mathbf{j(p_i)}$;

б) визначаємо порядковий номер символу шифртекста по рівнянню шифрування $\mathbf{j(c_i) = j(p_i) + k}$;

в) по відомому порядковому номеру $\mathbf{j(c_i)}$ визначаємо символ криптограми $\mathbf{CT = \{c_i\}}$, $\mathbf{i = \overline{1,n}}$.

Примітка:

Досягши кінця алфавіту виконувався циклічний перехід до його початку. Якщо номер символу шифртекста перевищує довжину алфавіту (m), то отримане значення зменшують на довжину алфавіту.

Приклад 1

Зашифруємо послання Цезаря

VENI VIDI VICI

Ключ k=3

V	E	N	I	V	I	D	I	V	I	C	I
21	4	13	8	21	8	3	9	21	8	2	8

21+3 =24	7	16	11	24	11	6	11	24	11	5	11
Y	**H**	**Q**	**L**	**Y**	**L**	**G**	**L**	**Y**	**L**	**F**	**L**

Криптограма: **Y H Q L Y L G L Y L F L**

Алгоритм дешифрування

1. Задамо алфавіт з 26 символів (букви англійського алфавіту, **m**=26)

№	0	1	2	3	4	5	6	7	8	9
символ	A	B	C	D	E	F	G	H	I	J

№	10	11	12	13	14	15	16	17	18	19
символ	K	L	M	N	O	P	Q	R	S	T

№	20	21	22	23	24	25
символ	U	V	W	X	Y	Z

і значення ключа k . $\mathbf{k = \overline{1,m-1}}$

2. Для кожного символу шифртекста $\mathbf{CT = \{c_i\}}$, $\mathbf{i = \overline{1,n}}$:

а) визначимо порядковий номер символу шифртекста в алфавіті $\mathbf{j(c_i)}$;

б) визначимо порядковий номер символу відкритого повідомлення по рівнянню дешифрування $\mathbf{j(p_i) = j(c_i) - k}$;

в) по відомому порядковому номеру $\mathbf{j(p_i)}$ визначаємо символ відкритого повідомлення $\mathbf{PT = \{p_i\}}$.

Примітка:

Якщо порядковий номер символу відкритого повідомлення менше нуля, то отримане значення збільшують на довжину алфавіту (m).

Приклад 2

Розшифруємо криптограму - I X E V Z U M X G V N E

Ключ дорівнює 6

I	**X**	**E**	**V**	**Z**	**U**	**M**	**X**	**G**	**V**	**N**	**E**
8	23	4	21	25	20	12	23	6	21	13	4
8-6 =2	23-6 =17	4-6 =-2 26-2=24	21-6 =15	25-6 =19	20-6 =14	12-6 =6	23-6 =17	6-6 =0	21-6 =15	13-6 =7	3-6 =-3 26-3 =23
C	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**Y**

Початкове повідомлення: **C R Y P T O G R A P H Y**

Шифр Цезаря називають адитивним шифром. Термін адитивний шифр показує його математичний сенс. Кожному символу зіставлено ціле число $\mathbf{Z_{26}}$. Засекречений ключ - також ціле число в $\mathbf{Z_{26}}$. Алгоритм кодування додає ключ до символу початкового тексту; алгоритм дешифрування віднімає ключ з символу зашифрованого тексту. Усі операції проводяться в $\mathbf{Z_{26}}$.

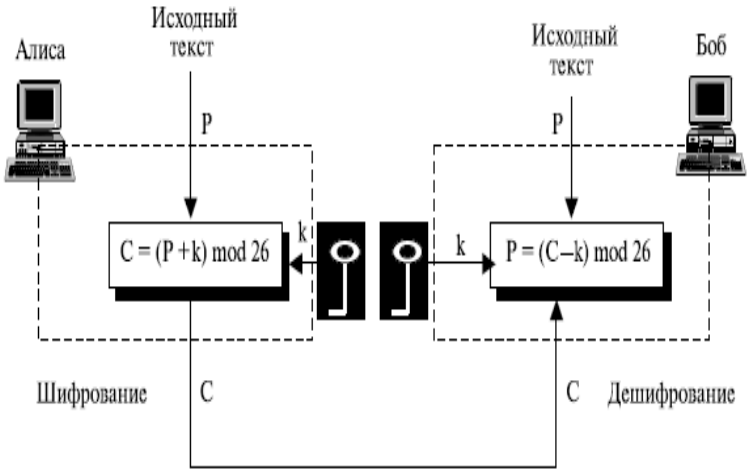
Використовуючи поняття модулярної арифметики можна алгоритм шифрування для шифру Цезаря описати наступним рівнянням криптоперетворення $\mathbf{E_K}$: $\mathbf{j \to (j+k) (mod\ m),\ 1 \le k < m-1}$

де K - значення ключа;

m - кількість букв у використовуваному алфавіті;

j - числовий код букви відкритого тексту;

j +k - числовий код відповідної букви шифр тексту "по модулю m".



Для нашого першого прикладу рівняння криптоперетворення

$$\mathbf{E}_{з}: \mathbf{j} \to (\mathbf{j}+\mathbf{3})(\mathbf{mod\ 26})$$

Вживаний алгоритм шифрування до початкового тексту, буква за буквою:

Початковий текст: **V** $\Rightarrow$ **21**

Шифрування $(21+3)\mathbf{mod}\ 26 \equiv 24(\mathbf{mod}\ 26)$

Шифртекст: **24** $\Rightarrow$**Y**

Початковий текст: **E** $\Rightarrow$ **4**

Шифрування $(4+3)\mathbf{mod}\ 26 \equiv 7(\mathbf{mod}\ 26)$

Шифртекст: **7** $\Rightarrow$**H**

Початковий текст: **N** $\Rightarrow$ **13**

Шифрування $(13+3)\mathbf{mod}\ 26 \equiv 16(\mathbf{mod}\ 26)$

Шифртекст: **16** $\Rightarrow$**Q**

Початковий текст: **I**$\Rightarrow$ **8**

Шифрування $(8+3)\mathbf{mod}\ 26 \equiv 11(\mathbf{mod}\ 26)$

Шифртекст: **11** $\Rightarrow$**L**

і так далі.

Аналогічно алгоритм дешифрування

$$\mathbf{D}_{\mathbf{K}}: \mathbf{j} \to (\mathbf{j}-\mathbf{k})(\mathbf{mod\ m}),\ \mathbf{1} \le \mathbf{k} < \mathbf{m}-\mathbf{1}$$

де **k** - значення ключа;

m - кількість букв у використовуваному алфавіті;

j - числовий код букви шифртекста;

j - k - числовий код відповідної букви відкритого тексту "по модулю m".

Для другого прикладу рівняння криптоперетворення

$$\mathbf{D}_{6}: \mathbf{j} \to (\mathbf{j}-\mathbf{6})(\mathbf{mod\ 26})$$

Вживаний алгоритм дешифрування до криптограми, буква за буквою:

Криптограма: **I** $\Rightarrow$ **8**

Дешифрування $(8-6)\mathbf{mod}\ 26 \equiv 2(\mathbf{mod}\ 26)$

Відкритий текст: **2** $\Rightarrow$**C**

Криптограма: **X** $\Rightarrow$ **23**

Дешифрування $(23-6)\mathbf{mod}\ 26 \equiv 17(\mathbf{mod}\ 26)$

Відкритий текст: **17⇒R**

Криптограма: **E ⇒ 4**

Дешифрування $(4-6)\bmod 26 \equiv -2(\bmod 26) \equiv 24(\bmod 26)$

Відкритий текст: **24 ⇒Y** і так далі.

Гідністю системи шифрування Цезаря є простота шифрування і дешифрування.

До недоліків системи Цезаря слід віднести наступні:

- підстановки, що виконуються відповідно до системи Цезаря, не маскують частот появи різних букв початкового відкритого тексту;
- зберігається алфавітний порядок в послідовності замінюючих букв;
- при зміні значення k змінюються тільки початкові позиції такої послідовності;
- число можливих ключів k мало;
- шифр Цезаря легко розкривається на основі аналізу частот появи букв в шифртексте.

У системі шифрування Цезаря використовувалися тільки адитивні властивості великої кількості цілих Z_m. Проте символи великої кількості множини Z_m можна також множити по модулю m. Аффінний шифр є комбінацією адитивних і мультиплікативних шифрів.

Визначимо перетворення в такій системі:

$$E_{k_1,k_2}(j): Z_m \to Z_m$$

Де m - кількість букв у використовуваному алфавіті;

j - числовий код букви відкритого тексту;

k_1, k_2 - пара ключів, цілі числа, **0 ≤** k_1, k_2 **<m, НОД (** k_1 **, m) = 1**;

$k_1 \cdot j + k_2$ - числовий код відповідної букви шифртекста "по модулю m".

У цьому перетворенні буква, що відповідає числу j, замінюється на букву, що відповідає числовому значенню $(k_1 \cdot j + k_2)$ по модулю m.

Перший ключ k_1 використовується мультиплікативним шифром, другий ключ k_2 - адитивним шифром. Тобто афінний шифр це два шифри вживаних один за іншим.

Слід зауважити, що перетворення $E_{k_1,k_2}(j)$ є взаємно однозначним відображенням на множині Z_m тільки у тому випадку, якщо **НОД(** k_1 **,m)=1**.

Визначимо криптоперетворення при дешифруванні:

$$D_{k_1,k_2}(j) \to \left((j - k_2) \cdot k_1^{-1}\right) (\mathrm{mod}\, m)$$

де

m - кількість букв у використовуваному алфавіті;

j - числовий код букви шифртекста;

k_1, k_2, - пара ключів, цілі числа, $0 \le k_1, k_2 < m$, НОД (k_1, m) = 1;

$(j - k_2) \cdot k_1^{-1}$ - числовий код відповідної букви відкритого тексту "по модулю m";

k_1^{-1} - мультиплікативна інверсія k_1;

$-k_2$ - аддитивна інверсія k_2 .

У Z_m аддитивна інверсія числу **a** може бути вичислена як $x = m - a$. Наприклад, аддитивна інверсія 4 в Z_{10} рівна 10 - 4 = 6.

У модульній арифметиці кожне ціле число має аддитивну інверсію. Сума цілого числа і його аддитивної інверсії порівняння з 0 по модулю m, тобто $a + x \equiv 0 (\mathrm{mod}\, m)$

У модульній арифметиці ціле число може або не може мати мультиплікативної інверсії. Ціле число і його мультиплікативна інверсія порівнянні з 1 по модулю m, тобто $a \cdot x \equiv 1 (\mathrm{mod}\, m)$.

Ціле число **a** в Z_m має мультиплікативну інверсію тоді і тільки тоді, якщо НОД (m, a) = 1

Наприклад, нехай m = 26, = 3, = 5. Тоді, очевидно, НОД(3,26) =1, і ми отримуємо наступну відповідність між числовими кодами букв:

j	0	1	2	3	4	5	6	7	8	9
$3 \cdot j + 5$	5	8	11	14	17	20	23	0	3	6

j	10	11	12	13	14	15	16	17	18	19
$3 \cdot j + 5$	9	12	15	18	21	24	1	4	7	10

j	20	21	22	23	24	25
$3 \cdot j + 5$	13	16	19	22	25	2

Перетворюючи числа у букви англійської мови, отримуємо наступну відповідність для букв відкритого тексту і шифртексту:

p_i	A	B	C	D	E	F	G	H	I	J
c_i	F	I	L	O	R	U	X	A	D	G

p_i	K	L	M	N	O	P	Q	R	S	T
c_i	J	M	P	S	V	Y	B	E	H	K

p_i	U	V	W	X	Y	Z
c_i	N	Q	T	W	Z	C

Приклад 4

Використовуємо алфавіт з 26 символів (26 англійських букв). Отже m = 26.

Нехай $k_1 = 3$, $k_2 = 5$.

Перевіряємо НОД (m, k_1)=НОД (26,3) = 1.

Початкове повідомлення: **H O P E**

Рівняння шифрування $E_{3,5}(j): \quad j \to (3 \cdot j + 5)(\mathrm{mod}\ 26)$

m_i	код символа сообщения	Шифрование	код символа шифртекста	c_i
H	7	$(3 \cdot 7 + 5)(\mathrm{mod}\ 26) \equiv 0(\mathrm{mod}\ 26)$	0	**A**
O	14	$(3 \cdot 14 + 5)(\mathrm{mod}\ 26) \equiv 47(\mathrm{mod}\ 26)$	21	**V**
P	15	$(3 \cdot 15 + 5)(\mathrm{mod}\ 26) \equiv 50(\mathrm{mod}\ 26)$	24	**Y**
E	4	$(3 \cdot 4 + 5)(\mathrm{mod}\ 26) \equiv 17(\mathrm{mod}\ 26)$	17	**R**

Шифртекст: **A V Y R**

Використовуємо алфавіт з 26 символів (26 англійських букв). Отже m = 26.

Нехай $\mathbf{k_1} = 3$, $\mathbf{k_2} = 5$.

Перевіряємо НОД (m, $\mathbf{k_1}$)=НОД (26,3) = 1,

Шифртекст: **A V Y R**

Щоб знайти символи початкового тексту додамо аддитивну інверсію від $-5 \equiv 21 (\mathbf{mod}\ 26)$ (т.е. $26-5=21$) до отриманого зашифрованого тексту(аддитивна інверсія існує оскільки $5+21 \equiv 0 (\mathbf{mod}\ 26)$).

Потім помножимо на мультиплікативну інверсію від $3^{-1} \equiv 9 (\mathbf{mod}\ 26)$.

№	m	$\mathbf{k_1}$	$\mathbf{m \ mod\ k_1}$	$\mathbf{int}\left(\frac{m}{k_1}\right)$	d	u	v
1	26	3	2	8	1	–1	9
2	3	2	1	1	1	1	–1
3	2	1	0	2	1	0	1
4	1	0	–	–	1	1	0

Рівняння дешифрування:

$$\mathbf{D_{3,5}(j) \rightarrow ((j-5) \cdot 3^{-1}) (mod\ 26)}$$

$\mathbf{c_i}$	код символа шифртекста	Шифрование	код символа сообщения	$\mathbf{m_i}$
A	0	$\mathbf{((0+21) \cdot 9) (mod\ 26) \equiv 189 (mod\ 26)}$	7	**H**
V	21	$\mathbf{((21+21) \cdot 9) (mod\ 26) \equiv (189 (mod\ 26) + 189 (mod\ 26)) (mod\ 26) \equiv 14 (mod\ 26)}$	14	**O**
Y	24	$\mathbf{((24+21) \cdot 9) (mod\ 26) \equiv 15 (mod\ 26)}$	15	**P**
R	17	$\mathbf{((17+21) \cdot 9) (mod\ 26) \equiv 4 (mod\ 26)}$	4	**E**

Гідністю афінної системи є зручне управління ключами - ключі шифрування і розшифрування представляються в компактній формі у вигляді пари чисел(($\mathbf{k_1}$, $\mathbf{k_2}$).

Недоліки афінної системи аналогічні недолікам системи шифрування Цезаря.

Постановка задачі

1. Ознайомитися з особливостями шифрів перестановки.
2. Сформулювати алгоритм шифрування.
3. У відповідності з номером студентського квитка з таблиці 1 вибрати вихідні дані до виконання завдання
4. Зашифрувати відкрите повідомлення згідно свого варіанту
5. Обмінятися даними з сусідом по парті та виконати дешифрування
6. Визначити ефективність і криптостійкість шифру

Контрольні питання:

1. Що таке шифр заміни.
2. Шифр «Атбаш».
3. Алгоритм шифрування та дешифрування у системі Цезаря.
4. Гідності та недоліки шифру Цезаря.
5. Що таке афінна система підстановок Цезаря.
6. Алгоритм шифрування та дешифрування у системі підстановок Цезаря.
7. Гідності та недоліки системи підстановок Цезаря.

Практична робота №3

Тема: Система Цезаря з ключовим словом.

Мета: Ознайомитися з системою Цезаря із ключовим словом.

Теоретичні відомості

Система шифрування Цезаря з ключовим словом є моноалфавітною системою підстановки. Особливістю цієї системи є використання ключового слова для зміщення і зміни порядку символів в алфавіті підстановки.

Алгоритм шифрування

1. Задамо алфавіт з 26 символів(букви англійського алфавіту, m=26)

№	0	1	2	3	4	5	6	7	8	9
символ	A	B	C	D	E	F	G	H	I	J

№	10	11	12	13	14	15	16	17	18	19
символ	K	L	M	N	O	P	Q	R	S	T

№	20	21	22	23	24	25
символ	U	V	W	X	Y	Z

і ключове число **k**, $\mathbf{k = \overline{0, m-1}}$ і ключове слово або фраза.

2. Ключове слово записується під буквами алфавіту, починаючи з букви, числовий код якої співпадає з вибраним числом **k**.

3. Букви алфавіту підстановки, що залишилися, записуються після ключового слова в алфавітному порядку:

4. У відповідності отриманої підстановки шифруємо відкрите повідомлення.

Приклад

Ключове число k=5, ключове слово DIPLOMAT

Відкритий текст: S E N D M O R E M O N E Y

	0	1	2	3	4	5	6	7	8	9
исходный алфавит	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
алфавит подстановки	**V**	**W**	**X**	**Y**	**Z**	**D**	**I**	**P**	**L**	**O**

	10	11	12	13	14	15	16	17	18	19
исходный алфавит	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
алфавит подстановки	**M**	**A**	**T**	**B**	**C**	**E**	**F**	**G**	**H**	**J**

	20	21	22	23	24	25
исходный алфавит	**U**	**V**	**W**	**X**	**Y**	**Z**
алфавит подстановки	**K**	**N**	**Q**	**R**	**S**	**U**

Шифртекст: H Z B Y T C G Z T C B Z S

Примітка:

Якщо в ключовому слові або фразі повторюються букви, то запис ключового слова або фрази проводиться без повторів.

Приклад

якщо у БЛОНДИНКА, то записуватися в таблицю підстановок буде слово БЛОНДИКА

Гідністю системи Цезаря з ключовим словом є те, що кількість можливих ключових слів практично невичерпна.

Недоліком цієї системи є можливість злому шифртекста на основі аналізу частот появи букв.

Постановка задачі

1. Ознайомитися з особливостями шифрів перестановки.
2. Сформулювати алгоритм шифрування.
3. У відповідності з номером студентського квитка з таблиці 1 вибрати вихідні дані до виконання завдання
4. Зашифрувати відкрите повідомлення згідно свого варіанту

5. Обмінятися даними з сусідом по парті та виконати дешифрування
6. Визначити ефективність і криптостійкість шифру

Контрольні питання:

1. Особливості шифру Цезаря з ключовим словом.
2. Алгоритм шифрування.
3. Гідності і недоліки шифру.

Практична робота №4

Тема: Шифр Полібія. Шифруючі таблиці Трисемуса.

Мета: Ознайомитися з алгоритмом шифрування Полібія та шифруючими таблицями Трисемуса.

Теоретичні відомості

Шифрований символ відкритого повідомлення замінюється двома цифровими символами, що означають координати клітинки квадрата, перше число означає рядок, друге – стовпець (шифрування зводиться до заміни букви парою цифр).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

При розшифруванні кожна така пара визначала відповідну букву повідомлення.

Причому заповнювати квадрат можна вибираючи символи у будь-якому порядку.

Тобто ключем такого шифру Полібія є розташування букв в таблиці.

Можуть бути алфавіти, де m "проблемно" для складання таблиці. Припустимо, m= 31 - просте число, його не розкласти на множники; m= 46 розкласти можна, а саме: 46 = 23 * 2, але ось тільки якесь ідіотське відношення розмірів. У таких випадках варто якось розширити алфавіт: додати, скажімо, розділові знаки або арифметичні знаки.

Ідею квадрата Полібія проілюструємо таблицею з російськими буквами. Число букв в російському алфавіті відрізняється від числа букв в грецькому, тому розмір таблиці вибраний іншим(6×6).

i / j	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е Ё
2	Ж	З	И Й	К	Л	М
3	Н	О	П	Р	С	Т
4	У	Ф	Х	Ц	Ч	Ш
5	Щ	Ь	Ъ	Ы	Э	Ю
6	Я	_	.	,	:	;

Зашифруємо повідомлення
ВЕСНА_ПРИШЛА

В	**Е**	**С**	**Н**	**А**	**_**	**П**	**Р**	**И**	**Ш**	**Л**	**А**
13	**16**	**35**	**31**	**11**	**62**	**33**	**34**	**23**	**46**	**25**	**11**

На перший погляд шифр здається дуже нестійким, але для його реальної оцінки слід враховувати два чинники:

- можливість заповнити квадрат Полібія буквами довільно, а не тільки строго за абеткою;

- можливість періодично замінювати квадрати.

Тоді аналіз попередніх повідомлень нічого не дає, оскільки до моменту розкриття шифру він може бути замінений.

Букви можуть вписуватися в таблицю в довільному порядку - заповнення таблиці в цьому випадку і є ключем. Для латинського алфавіту в першу клітину можна вписати одну з 25 букв, в другу - одну з 24, в третю - одну з 23 і так далі. Отримуємо максимальну кількість ключів для шифру на таблиці латинського алфавіту : $N = 25 * 24 * 23 * ... * 2 * 1 = 25!$

Відповідно для дешифрування повідомлення знадобиться не лише знання алфавіту, але і ключа, за допомогою якого складалася таблиця шифрування. Але довільний порядок букв важко запам’ятати, тому користувачеві шифру необхідно постійно мати при собі ключ - квадрат. З'являється небезпека таємного ознайомлення з ключем сторонніх осіб. В якості компромісного рішення був запропонований ключ - пароль.

Пароль виписується без повторів букв в квадрат; у клітини, що залишилися, в алфавітному порядку виписуються букви алфавіту, відсутні в паролі.

Слово-шифр повинно складатися з унікальних символів. Таке слово поміщається спочатку квадрата Полібія. Елементи квадрата, що йдуть за ключем, заповнюються буквами в порядку їх проходження в алфавіті з пропуском тих букв, які вже були використані в ключовому слові. Сам алгоритм криптоперетворень залишається такими ж, як і в шифрі Полібія.

Помітимо, що ефективність шифрування залежить від ключового слова, оскільки саме воно задає якість переміщення символів в квадраті Полібія. Для якіснішого перемішування в ключове слово доцільно включати останні символи базового алфавіту.

Зашифруємо повідомлення, використовуючи ключове слово РЕСПУБЛИКА
Т Е Р П Е Н Ь Е _ В О З Н А Г Р А Ж Д А Е Т С Я

i / j						
1		/Ё				
2		/Й				
3						
4						
5						
6						

4112 1114 1235 5312 6325 3633 3524 2611 3231 2412 4113 62

У шифрі використовується заміна один символ початкового тексту на два символи шифротекста. Це симетричний метод шифрування.

Ключовий простір впливає з довжина слова і максимально можлива кількість ключів.

Максимальна довжина ключа дорівнює довжині алфавіту, максимальна кількість варіантів ключа визначається факторіалом від довжини алфавіту. У нашому випадку 36.

Криптостійкість шифру середня, оскільки простір ключів хоч і великий, але обмежений.

Ефективність шифрування залежить від ключового слова.

Зашифруємо теж повідомлення, використовуючи ключ ОБВАЛ

i / j	1	2	3	4	5	6
1	О	Б	В	А	Л	Г
2	Д	Е/Ё	Ж	З	И/Й	К
3	М	Н	П	Р	С	Т
4	У	Ф	Х	Ц	Ч	Ш
5	Щ	Ь	Ъ	Ы	Э	Ю
6	Я	_	.	,	:	–

Т Е Р П Е Н Ь Е_В О З Н А Г Р А Ж Д А Е Т С Я

3622 3433 2232 5222 6213 1124 3214 1634 1423 2114 2236 3561

Шифруючі таблиці Трисемуса

Для отримання такого шифру заміни зазвичай використовувалися таблиця для запису букв алфавіту і ключове слово (чи фраза).

У таблицю спочатку вписувалося по рядках ключове слово, причому букви, що повторюються, відкидалися.

Потім ця таблиця доповнювалася буквами алфавіту, що не увійшли до неї, по порядку.

Оскільки ключове слово або фразу легко зберігати в пам'яті, то такий підхід

спрощував процеси шифрування і дешифрування.

Приклад

Для російського алфавіту шифруюча таблиця може мати розмір 4*8

Виберемо в якості ключа слово БАНДЕРОЛЬ. Шифруюча таблиця з таким ключем показана на рисунку.

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

Шифрування:

- знаходять в таблиці букву відкритого тексту і записують в шифртекст букву, розташовану нижче її в тому ж стовпці;

- якщо буква тексту опиняється в нижньому рядку таблиці, тоді для шифртекста беруть саму верхню букву з того ж стовпця.

Наприклад, при шифруванні за допомогою цієї таблиці повідомлення

В Ы Л Е Т А Е М П Я Т О Г О

отримуємо шифртекст

П Д К З Ы В З Ч Ш Л Ы Й С Й

Такі табличні шифри називаються монограмними, оскільки шифрування виконується по одній букві.

Трисемус першим помітив, що шифруючі таблиці дозволяють шифрувати відразу по дві букви. Такі шифри називаються біграмними.

Постановка задачі

1. Ознайомитися з особливостями шифрів перестановки.
2. Сформулювати алгоритм шифрування.
3. У відповідності з номером студентського квитка з таблиці 1 вибрати вихідні дані до виконання завдання
4. Зашифрувати відкрите повідомлення згідно свого варіанту
5. Обмінятися даними з сусідом по парті та виконати дешифрування
6. Визначити ефективність і криптостійкість шифру

Контрольні питання:

1. Особливості шифру Полібія.
2. Алгоритм шифрування.
3. Особливості шифру Трисемуса.
4. Алгоритм шифрування.
5. Гідності і недоліки шифру.

Практична робота №5

Тема: Криптосистема Віжинера.

Мета: Ознайомитися з алгоритмом шифрування Віжинера.

Теоретичні відомості

Система Віжинера вперше була опублікована в 1586р. і є однією з найстарших і найбільш відомих багатоалфавітних систем. Свою назву вона одержала по імені

французького дипломата XVI століття Блеза Віжинера, що розвивав і вдосконалював криптографічні системи.

Система Віжинера подібна до такої системи шифрування Цезаря, у якої ключ підстановки міняється від букви до букви. Цей шифр багатоалфавітної заміни можна описати таблицею шифрування, що називається таблицею (квадратом) Віжинера. На мал. 1.1 і 1.2 показані таблиці Віжинера для російського й англійського алфавітів відповідно.

Таблиця Віжинера використовується для шифрування й розшифрування. Таблиця має два входи:

- верхній рядок підкреслених символів, який використовується для зчитування чергової букви вихідного відкритого тексту;.
- крайній лівий стовпець ключа.

Послідовність ключів зазвичай одержують із числових значень букв ключового слова.

При шифруванні вихідного повідомлення його виписують у рядок, а під ним записують ключове слово (або фразу). Якщо ключ виявився коротше повідомлення, то його циклічно повторюють. Буква шифротексту перебуває на перетинанні стовпця, обумовленого буквою, що шифрується, і рядка, обумовленого числовим значенням ключа.

Нехай ключова послідовність має довжину r. тоді ключ r-алфавітної підстановки є r-рядок

$$\bar{\pi} = (\pi_0, \pi_1, ..., \pi_{r-1}).$$

Система шифрування Віжинера перетворить відкритий текст $\bar{x} = (x_0, x_1, ..., x_{n-1})$ у шифротекст $\bar{y} = (y_0, y_1, ..., y_{n-1})$ за допомогою $\bar{\pi} = (\pi_0, \pi_1, ..., \pi_{r-1}).$ відповідно до правила

$$T_\pi : \bar{x} = (x_0, x_1, ..., x_{n-1}) \to \bar{y} = (y_0, y_1, ..., y_{n-1}),$$
$$(y_0, y_1, ..., y_{n-1}) = (\pi_0(x_0), \pi_1(x_1), ..., \pi_{n-1}(x_{n-1})),$$

де $\pi_i = \pi(i \bmod r)$

Розглянемо приклад одержання шифротекста за допомогою таблиці Віжинера. Нехай обране ключове слово АМБРОЗІЯ. Необхідно зашифрувати повідомлення ПРИЛІТАЮ СЬОМОГО.

Випишемо вихідне повідомлення в рядок і запишемо під ним ключове слово з повторенням. У третій рядок будемо виписувати букви шифротекста, обумовлені з таблиці Віжинера

Повідомлення **П Р И Л І Т А Ю С Ь О М О Г О**
Ключ **А М Б Р О З І Я**

А М Б Р О З І Я

Шифротекст ПЬЙЫУЩИЗ ССЕКЬХЛН

Ключ	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	ь	ы	ъ	э	ю	я
0	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	ь	ы	ъ	э	ю	я
1	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	ь	ы	ъ	э	ю	я	а
2	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б
3	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в
4	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г
5	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
6	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е
7	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж
8	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з
9	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и
10	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й
11	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
12	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
13	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
14	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
15	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
16	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
17	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
18	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
19	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
20	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
21	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
22	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
23	ч	ш	щ	ь	ы	ъ	э	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
24	ш	щ	ь	ы	ъ	э	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
25	щ	ь	ы	ъ	э	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
26	ь	ы	ъ	э	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
27	ы	ъ	э	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	ь
28	ъ	э	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	ь	ы
29	э	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	ь	ы	ъ
30	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	ь	ы	ъ	э
31	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	ь	ы	ъ	э	ю

Рис. 1.2. Таблиця Віжинера для російського алфавита

Зруйнувати статистичні залежності в закодованих повідомленнях і тим самим підвищити надійність кодування можна за допомогою методу Віжинера. Алгоритм застосування цього методу наведений нижче:

1) Символи вихідного алфавіту нумеруються, починаючи з нуля, наприклад:

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

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Одержують таблицю відповідності;

2) задаються ключем кодування - словом у вихідному алфавіті, наприклад, АСУ;

3) виписують повідомлення, підмет кодуванню, наприклад, нехай це буде повідомлення ІНФОРМАТИКА, і виконують наступні кроки:

а) під кожним його символом записують порядковий номер з таблиці відповідності:

И Н Ф О Р М А Т И К А

8 12 19 13 15 11 0 17 8 9 0

б) під повідомленням виписують ключове слово, а під символами ключа виписують їхні порядкові номери з таблиці відповідності:

А С У А С У А С У А С

0 16 18 0 16 18 0 16 18 0 16

в) порядкові номери символів складаються по модулю, рівному числу символів вихідного алфавіту (у нашім випадку - 31):

8 28 6 13 0 29 0 2 26 9 16

Нагадаємо, що додавання по модулю (позначається ⊕) виконується без переносу одиниці переносу в старший розряд. Так ми одержали при додаванні по модулі 31, наприклад, чисел 17 і 16 (сума дорівнює 33, що на 2 перевищує модуль 31) значення 2;

4) отриманий числовий ряд перетвориться в символи вихідного алфавіту по таблиці відповідності. Так маємо:

И Ь Ж О А Ь А В Ю К С .

Очевидно, що статистика не допоможе декодувати це повідомлення, оскільки повторюються зовсім не ті символи, що у вихідному повідомленні.

Для декодування подібних повідомлень потрібна таблиця відповідності й ключ. Тоді виконують описані вище процедури кодування у зворотному порядку. Складність може представляти тільки операція вирахування з урахуванням модуля. При цьому варто пам'ятати, що не повинні виходити негативні значення. Якщо таке відбувається, потрібно зайняти число, що відповідає модулю.

Приклад 1. Декодувати повідомлення И Ь Ж О А Ь А В Ю К С , задавшись ключем АСУ й знаючи таблицю відповідності.

Рішення:

а) виписуємо під закодованим повідомленням порядкові номери символів з таблиці відповідності (див. вище):

И Ь Ж О А Ь А В Ю К С

8 28 6 13 0 29 0 2 26 9 16

б) виписуємо під повідомленням ключ із порядковими номерами символів:

А С У А С У А С У А С

0 16 18 0 16 18 0 16 18 0 16

в) віднімаємо з урахуванням модуля 31 із чисел у закодованому повідомленні числа для ключа:

8 12 19 13 15 11 0 17 8 9 0

г) перетворимо числа в символи по таблиці відповідності:

И Н Ф О Р М А Т И К А

При декодуванні виникла складність в одержанні кодів символів Т, Ф, Р. Справді, при вирахуванні з 2 числа 16 виходило -14. Тоді до 2 додали модуль 31, одержали 33 і вже з 33 відняли 16. Одержали 17 - порядковий номер символу Т. Аналогічно чинимо й із символами Ф и Р.

Цей вид кодування використовується для зменшення обсягів інформації на носії - сигналі.

Для кодування символів вихідного алфавіту використають двійкові коди змінної довжини: чим більше частота символу, тим коротше його код. **Ефективність коду** визначається середнім числом двійкових розрядів для кодування одного символу - $I_{ср}$ по формулі

$$I_{ср} = \sum_{i=1}^{k} f_s, n_s ,$$

Де k - число символів вихідного алфавіту;

n_s - число двійкових розрядів для кодування символу s;

f_s - частота символу s; причому

$$\sum_{i=1}^{k} f_s = 1$$

При ефективному кодуванні існує межа стиску, нижче якого не «спускається» жоден метод ефективного кодування - інакше буде загублена інформація. Цей параметр визначається **граничним значенням двійкових розрядів** можливого ефективного коду - $I_{пр}$.

$$I_{пр} = -\sum_{i=1}^{n} f_i \log_2 f_i ,$$

де n - потужність кодируемого алфавіту, що кодується;

F_I - частота і-го символу алфавіту, що кодується.

Існують два класичних методи ефективного кодування: метод Шеннона-Фано й метод Хаффмена. Вхідними даними для обох методів є задана безліч вихідних символів для кодування з їхніми частотами; результат - ефективні коди.

Постановка задачі

1. Ознайомитися з особливостями шифрів перестановки.
2. Сформулювати алгоритм шифрування.
3. У відповідності з номером студентського квитка з таблиці 1 вибрати вихідні дані до виконання завдання
4. Зашифрувати відкрите повідомлення згідно свого варіанту
5. Обмінятися даними з сусідом по парті та виконати дешифрування
6. Визначити ефективність і криптостійкість шифру

Контрольні питання:

1. Описати принцип методу шифрування криптосистеми Віжинера.
2. Визначити тип даної криптосистеми й на основі типу дати характеристику
3. Описати типи залежності в шифруванні криптосистемою Віжинера.
4. Алгебраїчно описати систему.
5. Використовуючи таблицю для російського алфавіту зашифрувати наступне вихідне повідомлення: «Головна умова існування вірусів універсальна інтерпретація інформації в обчислювальних системах». К=ЕФІОП.

Практична робота №6

Тема: Алгоритм RSA.

Мета: Ознайомитися з алгоритмом шифрування RSA.

Теоретичні відомості

Ефективними системами криптографічного захисту даних є асиметричні криптосистеми, звані також криптосистемами (КС) з відкритим ключем.

Криптографія з симетричними ключами базується на спільному використанні ключів; асиметрично-ключова криптографія базується на персональному ключі. Є деякі інші аспекти безпеки крім шифрування, які притаманні асиметрично-ключовій криптографії. Вони включають встановлення автентичності та цифрові підписи.

Криптографія з симетричними ключами базується (в основному) на підстановці і перестановці символів (символів або біт), а асиметрично-ключова криптографія - на застосуванні математичних функцій до чисел.

Повідомлення має перед шифруванням кодуватися як ціле число (або безліч цілих чисел). Після дешифрування воно має бути розшифровано як ціле число (або безліч цілих чисел). В асиметричних системах для шифрування даних використовується один ключ, а для дешифрування - інший ключ (звідси і назва - асиметричні).

Для шифрування даних використовується перший ключ, який є відкритим і може бути опублікований для використання всіма користувачами системи.

Дешифрування даних за допомогою відкритого ключа неможливо. Для дешифрування даних одержувач зашифрованої інформації використовує другий ключ, який є секретним. Ключ дешифрування не може бути визначений з ключа шифрування.

У цій криптосистемі застосовують два різних ключа: КВ1 - відкритий ключ відправника А; КВ2 - секретний ключ одержувача В. Генератор ключів доцільно розташовувати на стороні одержувача В (щоб не пересилати секретний ключ К2 по незахищеному каналу). Значення ключів КВ1 і КВ2 залежать від початкового стану генератора ключів.

Розкриття секретного ключа КВ2 по відомому відкритому ключу КВ1 має бути нерозв'язним завданням.

Характерні особливості асиметричних криптосистем:

1. Відкритий ключ КВ1 і криптограма СТ можуть бути відправлені по незахищених каналах, тобто супротивникові відомі КВ1 і СТ.

2. Алгоритм шифрування Е В: РТ -> СТ є відкритим.

Захист інформації в асиметричній криптосистемі заснована на таємності ключа КВ2.

У. Діффі і М. Хеллман сформулювали вимоги, виконання яких забезпечує безпеку асиметричної криптосистеми:

1. Обчислення пари ключів (КВ1, КВ2) отримувачем В на основі початкової умови повинно бути простим.

2. Відправник А, знаючи відкритий ключ КВ1 і повідомлення РТ, може легко обчислити криптограму $\mathbf{CT = E_{K_{B1}}(PT) = E_B(PT)}$(1)

3. Одержувач В, використовуючи секретний ключ КВ2 і криптограму СТ, може легко відновити вихідне повідомлення

$$\mathbf{PT = D_{K_{B2}}(CT) = D_B(CT) = D_B(E_B(PT))} \quad (2)$$

4. Противник, знаючи відкритий ключ КВ1, при спробі обчислити секретний ключ КВ2 наштовхується на непереборну обчислювальну проблему.

5. Противник, знаючи пару (КВ1, СТ), при спробі обчислити вихідне повідомлення pt наштовхується на непереборну обчислювальну проблему.

Криптосистема шифрування даних RSA

Алгоритм RSA запропонований в 1978 р. Автори: Р. Райвест (Rivest), А. Шамір (Shamir) і А. Адлеман (Adleman). Алгоритм отримав свою назву за першими літерами прізвищ його авторів. Алгоритм RSA став першим повноцінним алгоритмом з відкритим ключем, який може працювати як в режимі шифрування даних, так і в режимі електронного цифрового підпису.

Надійність алгоритму грунтується на складності факторизації великих чисел і складності обчислення дискретних логарифмів.

У криптосистемі RSA відкритий ключ КВ1, секретний ключ КВ2, повідомлення РТ і криптограма СТ належать безлічі цілих чисел.

Послідовність дій:

І. Дії користувача В

1) Вибирає два довільних великих простих числа P і Q.

2) Обчислює значення модуля N = P * Q.

3) Обчислює функцію Ейлера

$$\varphi(N)=(P-1)(Q-1)$$

Вибирає випадковим чином значення відкритого ключа КВ1 з урахуванням виконання умов: $1<K_{B1}\le\varphi(N)$, $ÍÑÄ\ (K_{B1},\varphi(N))=1$.

4) Обчислює значення секретного ключа КВ2, використовуючи властивості арифметики за модулем (наприклад, розширений алгоритм Евкліда) при вирішенні порівняння $K_{B2}\equiv K_{B1}^{-1}(\mathrm{mod}\ \varphi(N))$

5) Пересилає користувачеві А пару чисел (N, КВ1) по незахищеному каналу.

II. Дії користувача А

6) Розбиває вихідний відкритий текст РТ на блоки, кожен з яких може бути представлений у вигляді числа $p_i = 0,1, 2, ..., N-1.$

7) зашифровує текст, представлений у вигляді послідовності чисел pi, за формулою

$$c_i = p_i^{K_{B1}}(\mathrm{mod}\ N)$$

і відправляє криптограму

c1, c2, c3, ..., ci, ... користувачеві В.

III. Дії користувача В

8) Розшифровує прийняту криптограму

c1, c2, c3, ..., ci, ...

використовуючи секретний ключ КВ2, за формулою

$$p_i = c_i^{K_{B2}}(\mathrm{mod}\ N)$$

У результаті буде отримана послідовність чисел pi, які представляють собою вихідне повідомлення РТ.

Щоб алгоритм RSA мав практичну цінність, необхідно мати можливість без суттєвих витрат генерувати великі прості числа, вміти оперативно обчислювати значення ключів КВ1 і КВ2.

Завдання 2: Створити відкритий та закритий ключі, при ладанних значення P і Q. В якості відкритого ключа візьміть найбільше просте число, яке менше числа P. Використовуючи алфавіт зашифруйте повідомлення ALGORITHM за допомогою

створеного вами відкритого ключа. Дешифруйте отриману шифрограму за допомогою створеного закритого ключа.

Шифруємо повідомлення ALGORITHM

Заданий англійський алфавіт

№	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
символ	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**

№	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
символ	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**

№	**21**	**22**	**23**	**24**	**25**	**26**
символ	**U**	**V**	**W**	**X**	**Y**	**Z**

Дії користувача B:

1) Вибирає P = 13 і Q = 31.

2) Обчислює модуль N = P * Q = 13 * 31 = 403.

3) Обчислює значення функції Ейлера для N = 403:

$$\varphi(N)=(P-1)(Q-1)=12*30=360$$

4) Вибирає в якості відкритого ключа KB1 довільне число з урахуванням виконання умов:

$1<K_{B1}\le 360$, $ÍÑÄ\ (K_{B1},360)=1$

Нехай KB1 = 11.

5) Обчислює значення секретного ключа KB2, використовуючи розширений алгоритм Евкліда при розв'язанні порівняння $K_{B2}\equiv 11^{-1}(\mathrm{mod}\ 360)$

$\varphi(N)$	**KB1**	$\varphi(N)$ mod **KB1**	int ($\varphi(N)$/ **KB1**)	u	v
360	11	8	32	-4	131
11	8	3	1	3	-4
8	3	2	2	-1	3

3	2	1	1	1	-1
2	1	0	2	0	1
1	0	0	0	1	0

Рішення дає KB2 = 131.

6) Пересилає користувачеві A пару чисел (N = 403. KB1 = 11).

Дії користувача A:

7) Уявляє вихідне повідомлення як послідовність цілих чисел у діапазоні 0 .. 402. (0 .. N-1)

Нехай буква A представляється як число 1, літера L - як число 12 і тд. Тоді повідомлення ALGORITHM можна представити як послідовність чисел 1, 12, 7, 15, 18, 9, 20, 8, 13, тобто p1 = 1, p2 = 12, p3 = 7, p4 = 15, p5 = 18, p6 = 9,
p7 = 20, p8 = 8, p9 = 13.

8) зашифровує текст, представлений у вигляді послідовності чисел p1, p2… p9, використовуючи ключ KB1 = 11 і N = 403, за формулою

$$\tilde{n}_i = p_i^{K_{B1}} (\mathrm{mod}\ N) = p_i^{11} (\mathrm{mod}\ 403)$$

Отримує:

$$\tilde{n}1 = 1^{11} (\mathrm{mod}\ 403) = 1$$

$$\tilde{n}2 = 12^{11} (\mathrm{mod}\ 403) = 12^1 (\mathrm{mod}\ 403) * ((12^2 \mathrm{mod}\ 403)^2)^2 *$$
$$(12^2 \mathrm{mod}\ 403) = 12^1 (\mathrm{mod}\ 403) * (12^2 \mathrm{mod}\ 403) * (183^2 \mathrm{mod}\ 403)$$
$$= 40 * 12 * 144 (\mathrm{mod}\ 403) = 207$$

$$\tilde{n}3 = 7^{11} (\mathrm{mod}\ 403) = 7^1 (\mathrm{mod}\ 403) * ((7^2 \mathrm{mod}\ 403)^2)^2 *$$
$$(7^2 \mathrm{mod}\ 403) = 7^1 (\mathrm{mod}\ 403) * (7^2 \mathrm{mod}\ 403) * (386^2 \mathrm{mod}\ 403)$$
$$= 7 * 49 * 289 (\mathrm{mod}\ 403) = 392$$

$$\tilde{n}4 = 15^{11} (\mathrm{mod}\ 403) = 15^1 (\mathrm{mod}\ 403) * ((15^2 \mathrm{mod}\ 403)^2)^2 *$$
$$(15^2 \mathrm{mod}\ 403) = 15^1 (\mathrm{mod}\ 403) * (15^2 \mathrm{mod}\ 403) * (250^2 \mathrm{mod}\ 403)$$
$$= 15 * 225 * 35 (\mathrm{mod}\ 403) = 46$$

$$\tilde{n}5 = 18^{11} (\mathrm{mod}\ 403) = 18^1 (\mathrm{mod}\ 403) * ((18^2 \mathrm{mod}\ 403)^2)^2 *$$
$$(18^2 \mathrm{mod}\ 403) = 18^1 (\mathrm{mod}\ 403) * (18^2 \mathrm{mod}\ 403) * (196^2 \mathrm{mod}\ 403)$$
$$= 18 * 324 * 131 (\mathrm{mod}\ 403) = 307$$

$$\tilde{n}6 = 9^{11}(\mathrm{mod}\ 403) = 9^{1}(\mathrm{mod}\ 403) * ((9^{2}\ \mathrm{mod}\ 403)^{2})^{2} *$$
$$(9^{2}\ \mathrm{mod}\ 403) = 9^{1}(\mathrm{mod}\ 403) * (9^{2}\ \mathrm{mod}\ 403) * (113^{2}\ \mathrm{mod}\ 403)$$
$$= 9 * 81 * 276(\mathrm{mod}\ 403) = 107$$

$$\tilde{n}7 = 20^{11}(\mathrm{mod}\ 403) = 20^{1}(\mathrm{mod}\ 403) * ((20^{2}\ \mathrm{mod}\ 403)^{2})^{2} *$$
$$(20^{2}\ \mathrm{mod}\ 403) = 20^{1}(\mathrm{mod}\ 403) * (20^{2}\ \mathrm{mod}\ 403) * (9^{2}\ \mathrm{mod}\ 403)$$
$$= 400 * 8(\mathrm{mod}\ 403) = 379$$

$$\tilde{n}8 = 8^{11}(\mathrm{mod}\ 403) = 8^{1}(\mathrm{mod}\ 403) * ((8^{2}\ \mathrm{mod}\ 403)^{2})^{2} *$$
$$(8^{2}\ \mathrm{mod}\ 403) = 8^{1}(\mathrm{mod}\ 403) * (8^{2}\ \mathrm{mod}\ 403) * (66^{2}\ \mathrm{mod}\ 403)$$
$$= 8 * 64 * 326(\mathrm{mod}\ 403) = 70$$

$$\tilde{n}9 = 13^{11}(\mathrm{mod}\ 403) = 13^{1}(\mathrm{mod}\ 403) * ((13^{2}\ \mathrm{mod}\ 403)^{2})^{2} *$$
$$(13^{2}\ \mathrm{mod}\ 403) = 13^{1}(\mathrm{mod}\ 403) * (13^{2}\ \mathrm{mod}\ 403) * (351^{2}\ \mathrm{mod}\ 403)$$
$$= 13 * 169 * 286(\mathrm{mod}\ 403) = 65$$

Відправляє користувачу В криптограму

c1, c2, c3, c4, c5, c6, c7, c8, c9 = 1, 207, 392, 46, 307, 107, 379, 70, 65.

Дії користувача В:

9) Розшифровує прийняту криптограму c1, c2, c3, c4, c5, c6, c7, c8, c9, використовуючи секретний ключ КВ2 = 131. за формулою

$$\mathbf{p_i = c_i^{K_{B2}} (mod\ N)}$$

Отримує:

$$p1 = 1^{131}(\mathrm{mod}\ 403) = 1(\mathrm{mod}\ 403) = 1$$

$$p2 = 207^{131}(\mathrm{mod}\ 403) = 207^{1}(\mathrm{mod}\ 403) * (207^{2}\ \mathrm{mod}\ 403) *$$
$$((((((207^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2})^{2})^{2})^{2} = 207^{1}(\mathrm{mod}\ 403) * (207^{2}\ \mathrm{mod}\ 403) *$$
$$((((((131^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2})^{2})^{2} = 207^{1}(\mathrm{mod}\ 403) * (207^{2}\ \mathrm{mod}\ 403) *$$
$$(((235^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2})^{2} = 207^{1}(\mathrm{mod}\ 403) * (207^{2}\ \mathrm{mod}\ 403) *$$
$$((14^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2} = 207^{1}(\mathrm{mod}\ 403) * (207^{2}\ \mathrm{mod}\ 403) * (131^{2}\ \mathrm{mod}\ 403)^{2} =$$
$$207^{1}(\mathrm{mod}\ 403) * (207^{2}\ \mathrm{mod}\ 403) * (235^{2}\ \mathrm{mod}\ 403) = 207 * 131 * 14(\mathrm{mod}\ 403) =$$
$$207 * 222(\mathrm{mod}\ 403) = 12$$

$$p3 = 392^{131}(\mathrm{mod}\ 403) = 392^{1}(\mathrm{mod}\ 403) * (392^{2} \bmod 403) *$$
$$((((((392^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2})^{2} = 392^{1}(\mathrm{mod}\ 403) * (392^{2} \bmod 403) *$$
$$(((((121^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2} = 392^{1}(\mathrm{mod}\ 403) * (392^{2} \bmod 403) *$$
$$((((133^{2} \bmod 403)^{2})^{2})^{2})^{2} = 392^{1}(\mathrm{mod}\ 403) * (392^{2} \bmod 403) *$$
$$(((360^{2} \bmod 403)^{2})^{2})^{2} = 392^{1}(\mathrm{mod}\ 403) * (392^{2} \bmod 403) *$$
$$((237^{2} \bmod 403)^{2})^{2} = 392^{1}(\mathrm{mod}\ 403) * (392^{2} \bmod 403) * (152^{2} \bmod 403)^{2} =$$
$$392^{1}(\mathrm{mod}\ 403) * (392^{2} \bmod 403) * (133^{2} \bmod 403) = 392 * 121 * 360(\mathrm{mod}\ 403) =$$
$$281 * 360(\mathrm{mod}\ 403) = 7$$

$$p4 = 46^{131}(\mathrm{mod}\ 403) = 46^{1}(\mathrm{mod}\ 403) * (46^{2} \bmod 403) *$$
$$((((((46^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2})^{2} = 46^{1}(\mathrm{mod}\ 403) * (46^{2} \bmod 403) *$$
$$(((((101^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2} = 46^{1}(\mathrm{mod}\ 403) * (46^{2} \bmod 403) *$$
$$((((126^{2} \bmod 403)^{2})^{2})^{2})^{2} = 46^{1}(\mathrm{mod}\ 403) * (46^{2} \bmod 403) *$$
$$(((159^{2} \bmod 403)^{2})^{2})^{2} = 46^{1}(\mathrm{mod}\ 403) * (46^{2} \bmod 403) *$$
$$((295^{2} \bmod 403)^{2})^{2} = 46^{1}(\mathrm{mod}\ 403) * (46^{2} \bmod 403) * (380^{2} \bmod 403)^{2} =$$
$$46^{1}(\mathrm{mod}\ 403) * (46^{2} \bmod 403) * (126^{2} \bmod 403) = 46^{1}(\mathrm{mod}\ 403) *$$
$$(46^{2} \bmod 403) * (159 \bmod 403) = 46 * 101 * 159(\mathrm{mod}\ 403) =$$
$$46 * 342(\mathrm{mod}\ 403) = 15$$

$$p5 = 307^{131}(\mathrm{mod}\ 403) = 307^{1}(\mathrm{mod}\ 403) * (307^{2} \bmod 403) *$$
$$((((((307^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2})^{2} = 307^{1}(\mathrm{mod}\ 403) * (307^{2} \bmod 403) *$$
$$(((((350^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2} = 307^{1}(\mathrm{mod}\ 403) * (307^{2} \bmod 403) *$$
$$((((391^{2} \bmod 403)^{2})^{2})^{2})^{2} = 307^{1}(\mathrm{mod}\ 403) * (307^{2} \bmod 403) *$$
$$(((144^{2} \bmod 403)^{2})^{2})^{2} = 307^{1}(\mathrm{mod}\ 403) * (307^{2} \bmod 403) *$$
$$((183^{2} \bmod 403)^{2})^{2} = 307^{1}(\mathrm{mod}\ 403) * (307^{2} \bmod 403) * (40^{2} \bmod 403)^{2} =$$
$$307^{1}(\mathrm{mod}\ 403) * (307^{2} \bmod 403) * (391^{2} \bmod 403) = 307^{1}(\mathrm{mod}\ 403) *$$
$$(307^{2} \bmod 403) * (144 \bmod 403) = 307 * 350 * 144(\mathrm{mod}\ 403) =$$
$$307 * 25(\mathrm{mod}\ 403) = 18$$

$$p6 = 107^{131}(\mathrm{mod}\ 403) = 107^{1}(\mathrm{mod}\ 403) * (107^{2} \bmod 403) *$$
$$((((((107^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2})^{2} = 107^{1}(\mathrm{mod}\ 403) * (107^{2} \bmod 403) *$$
$$(((((165^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2} = 107^{1}(\mathrm{mod}\ 403) * (107^{2} \bmod 403) *$$
$$((((224^{2} \bmod 403)^{2})^{2})^{2})^{2} = 107^{1}(\mathrm{mod}\ 403) * (107^{2} \bmod 403) *$$
$$(((204^{2} \bmod 403)^{2})^{2})^{2} = 107^{1}(\mathrm{mod}\ 403) * (107^{2} \bmod 403) *$$
$$((107^{2} \bmod 403)^{2})^{2} = 107^{1}(\mathrm{mod}\ 403) * (107^{2} \bmod 403) * (165^{2} \bmod 403)^{2} =$$
$$107^{1}(\mathrm{mod}\ 403) * (107^{2} \bmod 403) * (224^{2} \bmod 403) = 107 * 165 * 204(\mathrm{mod}\ 403)$$
$$= 107 * 211(\mathrm{mod}\ 403) = 9$$

$$p7 = 379^{131}(\mathrm{mod}\ 403) = 379^{1}(\mathrm{mod}\ 403) * (379^{2} \bmod 403) *$$
$$((((((379^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2})^{2} = 379^{1}(\mathrm{mod}\ 403) * (379^{2} \bmod 403) *$$
$$(((((173^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2} = 379^{1}(\mathrm{mod}\ 403) * (379^{2} \bmod 403) *$$
$$((((107^{2} \bmod 403)^{2})^{2})^{2})^{2} = 379^{1}(\mathrm{mod}\ 403) * (379^{2} \bmod 403) *$$
$$(((165^{2} \bmod 403)^{2})^{2})^{2} = 379^{1}(\mathrm{mod}\ 403) * (379^{2} \bmod 403) *$$
$$((224^{2} \bmod 403)^{2})^{2} = 379^{1}(\mathrm{mod}\ 403) * (379^{2} \bmod 403) * (204^{2} \bmod 403)^{2} =$$
$$379^{1}(\mathrm{mod}\ 403) * (379^{2} \bmod 403) * (107^{2} \bmod 403) = 379 * 173 * 165(\mathrm{mod}\ 403) =$$
$$281 * 165(\mathrm{mod}\ 403) = 20$$

$$p8 = 70^{131}(\mathrm{mod}\ 403) = 70^{1}(\mathrm{mod}\ 403) * (70^{2} \bmod 403) *$$
$$((((((70^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2})^{2} = 70^{1}(\mathrm{mod}\ 403) * (70^{2} \bmod 403) *$$
$$(((((64^{2} \bmod 403)^{2})^{2})^{2})^{2})^{2} = 70^{1}(\mathrm{mod}\ 403) * (70^{2} \bmod 403) *$$
$$((((66^{2} \bmod 403)^{2})^{2})^{2})^{2} = 70^{1}(\mathrm{mod}\ 403) * (70^{2} \bmod 403) *$$
$$(((326^{2} \bmod 403)^{2})^{2})^{2} = 70^{1}(\mathrm{mod}\ 403) * (70^{2} \bmod 403) *$$
$$((287^{2} \bmod 403)^{2})^{2} = 70^{1}(\mathrm{mod}\ 403) * (70^{2} \bmod 403) * (157^{2} \bmod 403)^{2} =$$
$$70^{1}(\mathrm{mod}\ 403) * (70^{2} \bmod 403) * (66^{2} \bmod 403) = 70 * 64 * 326(\mathrm{mod}\ 403) =$$
$$70 * 311(\mathrm{mod}\ 403) = 8$$

$$p9 = 65^{131}(\mathrm{mod}\ 403) = 65^{1}(\mathrm{mod}\ 403) * (65^{2}\ \mathrm{mod}\ 403) *$$
$$((((((65^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2})^{2})^{2})^{2} = 65^{1}(\mathrm{mod}\ 403) * (65^{2}\ \mathrm{mod}\ 403) *$$
$$(((((195^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2})^{2})^{2} = 65^{1}(\mathrm{mod}\ 403) * (65^{2}\ \mathrm{mod}\ 403) *$$
$$((((143^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2})^{2} = 65^{1}(\mathrm{mod}\ 403) * (65^{2}\ \mathrm{mod}\ 403) *$$
$$(((299^{2}\ \mathrm{mod}\ 403)^{2})^{2})^{2} = 65^{1}(\mathrm{mod}\ 403) * (65^{2}\ \mathrm{mod}\ 403) *$$
$$((338^{2}\ \mathrm{mod}\ 403)^{2})^{2} = 65^{1}(\mathrm{mod}\ 403) * (65^{2}\ \mathrm{mod}\ 403) * (195^{2}\ \mathrm{mod}\ 403)^{2} =$$
$$65^{1}(\mathrm{mod}\ 403) * (65^{2}\ \mathrm{mod}\ 403) * (143^{2}\ \mathrm{mod}\ 403) = 65 * 195 * 299(\mathrm{mod}\ 403) =$$
$$65 * 273(\mathrm{mod}\ 403) = 13$$

Таким чином, відновлено початкове повідомлення:

A L G O R I T H M

1 12 7 15 18 9 20 8 13

Постановка задачі

1. Ознайомитися з особливостями шифрів перестановки.
2. Сформулювати алгоритм шифрування.
3. У відповідності з номером студентського квитка з таблиці 1 вибрати вихідні дані до виконання завдання
4. Зашифрувати відкрите повідомлення згідно свого варіанту
5. Обмінятися даними з сусідом по парті та виконати дешифрування
6. Визначити ефективність і криптостійкість шифру

Контрольні питання:

1. Криптосистема RSA.
2. Алгоритм шифрування.
3. Алгоритм дешифрування.
4. Гідності та недоліки шифру.

Таблиця 1

1 варіант
Фраза: На верхней галерее терем
Ключове слово: Воронка (Funnel)
2 варіант
Фраза: Старый воин уже спешил к стене
Ключове слово: Радио (Radio)
3 варіант
Фраза: Однако гордая княгиня не возмутилась
Ключове слово: Фура (Truck)
4 варіант
Фраза: Пусть княжичи прячутся
Ключове слово: Метла (Broom)
5 варіант
Фраза: Столпившиеся на верху воины закричали
Ключове слово: Рай (Paradise)
6 варіант
Фраза: Всадница едва не рухнула на руки
Ключове слово: Фоторамка (Frame)
7 варіант
Фраза: Шум вокруг нас усилился
Ключове слово: Ласка (Weasel)
8 варіант
Фраза: Время тянулось все томительнее
Ключове слово: Юла (Whirligig)
9 варіант
Фраза: Наконец они прибыли в богатый город
Ключове слово: Вьюга (Snowstorm)
10 варіант
Фраза: Но вскоре что то произошло
Ключове слово: Оптоволокно (Optical fiber)
11 варіант
Фраза: Они почти миновали длинный переход
Ключове слово: Гемоглобин (Hemoglobin)
12 варіант
Фраза: Они свернули за угол теремка
Ключове слово: Коледж (College)
13 варіант
Фраза: В проходе их заволок сизый дым
Ключове слово: Лямка (Strap)
14 варіант
Фраза: Маленькое бревенчатое помещенице
Ключове слово: Гемодиализ (Hemodialysis)
15 варіант
Фраза: Дальнейшее произошло мгновенно
Ключове слово: Бинокль (Binoculars)
16 варіант
Фраза: Проводник пристально смотрел

Ключове слово: Иа (Berry)
17 варіант
Фраза: За оградой ощутился смрад
Ключове слово: Одиночество (Loneliness)
18 варіант
Фраза: Двигайся в обход градской насыпи
Ключове слово: Товариш (Comrade)
19 варіант
Фраза: Под его головой загудела земля
Ключове слово: Ад (Hell)
20 варіант
Фраза: К вечеру очередного дня
Ключове слово: Одинадцать (Eleven)
21 варіант
Фраза: Вечером у костра
Ключове слово: Оградка (Fence)
22 варіант
Фраза: Солнце жгло немилосердно
Ключове слово: Шестнадцать (Sixteen)
23 варіант
Фраза: Гребец продолжил налегать на весла
Ключове слово: Пятнадцать (Fifteen)
24 варіант
Фраза: Напали на него внезапно
Ключове слово: Город (City)
25 варіант
Фраза: Люди стали нести подношения
Ключове слово: Дружба (Friendship)