**Лабораторна робота №3**

**ШИФРИ ПЕРЕСТАНОВКИ**

**Мета роботи: вивчення шифрів перестановки**

**Теоретичні відомості**

В шифрах перестановки усе символи відкритого тексту переносяться в шифрограму у незмінному виді, але змінюють своє місце розташування.

**При шифруванні перестановкою символи** тексту, який шифрується, переставляються за певним правилом в межах блоку цього тексту.

Шифри перестановки використовувалися з V ст. до н.е. – наприклад, жезл Сцітала, проста маршрутна перестановка, одиночна перестановка по ключу, поворотні решітки, подвійна таблична перестановка і т.д.

Розглянемо два методи шифрування:

1. Шифр одиночної перестановки за ключем.

2. Шифр подвійний перестановки.

У цих методах стовпці таблиці переставляються за ключовим словом, фразою або набором чисел довжиною у рядок таблиці.

В алгоритмах та прикладах використовується алфавіт з 27 символів (26 букв англійського алфавіту та пробіл). Алфавіт наведений у таблиці 3.1.

Таблиця 3.1.

«Англійський алфавіт та пробіл»

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J |

| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|
| K | L | M | N | O | P | Q | R | S | T |

| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|
| U | V | W | X | Y | Z | пробіл |

**Шифр одиночної перестановки за ключем**

Ключем шифру є заздалегідь вибране слово, яке визначає довжину блоку і перестановку символів у кожному блоці, на які розбивається вихідне повідомлення.

***Алгоритм шифрування***

1) По ключу і вихідному повідомленню формується таблиця.

Кількість стовпців у таблиці відповідає кількості символів ключового слова.

$$\mathbf{n_{стовбців}} = \ell_{\mathbf{ключа}}.$$

Кількість рядків у таблиці визначається відношенням кількості символів відкритого повідомлення (**pt**) до довжини ключового слова плюс два рядки (одна для ключового слова, друга для нумерації символів ключа)

$$\mathbf{n_{рядків}} = \lfloor \ell_{\mathbf{pt}} / \ell_{\mathbf{ключа}} \rfloor + \mathbf{2}.$$

Квадратні дужки означають цілу частину від ділення двох чисел, округлену до найближчого більшого цілого

2) Заповнюється ліва таблиця:

а) перший рядок – ключ;

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

у) далі вихідне повідомлення записується у таблицю по черзі по стовпцях.

3) У правій таблиці стовпці переставлені у відповідності до упорядкованих номерів символів ключа.

4) Для формування шифртекста, зчитують вміст правої таблиці по рядках.

***Зауваження:***

- якщо довжина повідомлення виявилася меншою, ніж кількість комірок у таблиці, то останні комірки таблиці можна доповнити довільними символами;
- якщо у ключі зустрілися однакові букви, вони нумеруються зліва направо.

**Приклад 3.1.** Провести шифрування методом одиночної перестановки за ключем. Використовуємо алфавіт з таблиці 3.1.

**Відкритий текст:** for_loop_control_variable_must_be_simple_local_variable

**Ключ:** activate

***Зауваження.*** Надалі, у повідомленнях і шифрограмах знаки пробілів позначені підкресленням.

**Розв'язання**

**1)** Визначаємо кількість стовбців та рядків

$$\mathbf{n_{стовбців}} = \ell_{\text{ключа}} = \mathbf{8}, \qquad \mathbf{n_{рядків}} = \left\lfloor \ell_{\text{pt}} / \ell_{\text{ключа}} \right\rfloor + 2 = \lceil 55/8 \rceil + 2 = \mathbf{9}$$

**2)** Згідно з алгоритмом заповнюємо ліву таблицю

| **a** | **c** | **t** | **i** | **v** | **a** | **t** | **e** |
|---|---|---|---|---|---|---|---|
| **1** | **3** | **6** | **5** | **8** | **2** | **7** | **4** |
| f | p | o | a | s | i | o | r |
| o | _ | l | b | t | m | c | i |
| r | c | _ | l | _ | p | a | a |
| _ | o | v | e | b | l | l | b |
| l | n | a | _ | e | e | _ | l |
| o | t | r | m | _ | _ | v | e |
| o | r | i | u | s | l | a | _ |
| ліва | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| права | | | | | | | |

напрямок процесу шифрування

**3)** У правій таблиці стовпці переставлені у відповідності до упорядкованих номерів символів ключа.

| **a** | **c** | **t** | **i** | **v** | **a** | **t** | **e** |
|---|---|---|---|---|---|---|---|
| **1** | **3** | **6** | **5** | **8** | **2** | **7** | **4** |
| f | p | o | a | s | i | o | r |
| o | _ | l | b | t | m | c | i |
| r | c | _ | l | _ | p | a | a |
| _ | o | v | e | b | l | l | b |
| l | n | a | _ | e | e | _ | l |
| o | t | r | m | _ | _ | v | e |
| o | r | i | u | s | l | a | _ |
| ліва | | | | | | | |

| **a** | **a** | **c** | **e** | **i** | **t** | **t** | **e** |
|---|---|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| f | i | p | r | a | o | o | s |
| o | m | _ | i | b | l | c | t |
| r | p | c | a | l | _ | a | _ |
| _ | l | o | b | e | v | l | b |
| l | e | n | l | _ | a | _ | e |
| o | _ | t | e | m | r | v | _ |
| o | l | r | _ | u | i | a | s |
| права | | | | | | | |

напрямок процесу шифрування

4) Для формування шифртекста, зчитують вміст правої таблиці по рядках.

**Шифртекст:** fipraoosom_iblctrpcal_a_ _lobevlblenl_a_eo_temrv_olr_uias

***Алгоритм дешифрування***

1) По ключу і шифртексту формується таблиця.

Кількість стовпців у таблиці відповідає кількості символів ключового слова.

$$\mathbf{n_{стовбців}} = \ell_{\mathbf{ключа}}.$$

Кількість рядків у таблиці визначається відношенням кількості символів шифртексту (**ct**) до довжини ключового слова плюс два рядки (одна для ключового слова, друга для нумерації символів ключа)

$$\mathbf{n_{рядків}} = \left[\ell_{\mathbf{ct}} / \ell_{\mathbf{ключа}}\right] + \mathbf{2}.$$

Квадратні дужки означають цілу частину від ділення двох чисел, округлену до найближчого більшого цілого

2) Заповнюється права таблиця:

а) перший рядок – символи ключа по порядку у алфавіті;

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

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

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

4) Для формування вихідного повідомлення зчитують вміст лівої таблиці по стовпцях

**Приклад 3.2.** Провести дешифрування методом одиночної перестановки за ключем. Використовуємо алфавіт з таблиці 3.1.

**Шифртекст:** aciaibanlzlni_eentv_soial_taro_ _lic

**Ключ:** mouse

**Розв'язання**

**1)** Визначаємо кількість стовбців та рядків

$$\mathbf{n_{стовбців}} = \ell_{\text{ключа}} = 5,\ \mathbf{n_{рядків}} = \left[\ell_{\text{ст}} / \ell_{\text{ключа}}\right] + 2 = [33/5] + 2 = 9$$

**2)** Згідно з алгоритмом заповнюємо праву таблицю

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| ліва | | | | |

| **e** | **m** | **o** | **s** | **u** |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |
| a | c | i | a | i |
| b | a | n | l | z |
| l | n | i | _ | e |
| e | n | t | v | _ |
| s | o | i | a | l |
| _ | t | a | r | o |
| _ | _ | l | i | c |
| права | | | | |

напрямок процесу дешифрування

←————————————————————

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

| **m** | **o** | **u** | **s** | **e** |
|---|---|---|---|---|
| **2** | **3** | **5** | **4** | **1** |
| c | i | i | a | a |
| a | n | z | l | b |
| n | i | e | _ | l |
| n | t | _ | v | e |
| o | i | l | a | s |
| t | a | o | r | _ |
| _ | l | c | i | _ |
| ліва | | | | |

| **e** | **m** | **o** | **s** | **u** |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |
| a | c | i | a | i |
| b | a | n | l | z |
| l | n | i | _ | e |
| e | n | t | v | _ |
| s | o | i | a | l |
| _ | t | a | r | o |
| _ | _ | l | i | c |
| права | | | | |

напрямок процесу дешифрування

←————————————————————

4) Для формування вихідного повідомлення зчитують вміст лівої таблиці по стовпцях

**Відкритий текст:**

Cannot_initialize_local_variables

**Метод шифрування «Подвійна перестановка»**

Для забезпечення додаткової скритності, при використанні табличних шифрів перестановки проводять повторне шифрування. Такий метод шифрування називається подвійною перестановкою. У випадку подвійної перестановки, перестановки стовпців і рядків таблиці визначаються окремо.

Ключем до шифру подвійної перестановки служить послідовність номерів стовпців і номерів рядків початкової таблиці.

***Алгоритм шифрування***

1) За кількістю символів в обох ключах формуються три таблиці.

$$\mathbf{n_{рядків}} = \ell_{\mathbf{k_{рядків}}} + \mathbf{1}; \qquad \mathbf{n_{стовпців}} = \ell_{\mathbf{k_{стовпців}}} + \mathbf{1}$$

Додатковий рядок і стовпець використовуються для запису ключів:

а) над першим рядком кожної таблиці записується ключ $\mathbf{k_{стовпців}}$;

б) перед першим стовпцем кожної таблиці записується ключ $\mathbf{k_{рядків}}$.

2) Заповнюються ліва таблиця:

а) розставляються значення ключів;

б) вихідне повідомлення записується в таблицю по черзі по рядках, зліва на право.

3) Проводиться переставлення:

а) у середній таблиці стовпці переставляються відповідно до упорядкування цифр ключа $\mathbf{k_{стовпців}}$ за зростанням;

б) в правій таблиці рядки переставляються відповідно до упорядкування цифр ключа $\mathbf{k_{рядків}}$ за зростанням.

4) Для формування шифртекста, зчитують вміст правої таблиці по рядках зліва направо.

***Зауваження:*** якщо довжина повідомлення виявилася меншою, ніж кількість комірок у таблиці, то останні комірки таблиці можна доповнити довільними символами.

**Приклад 3.3.** Провести шифрування методом подвійної перестановки. Використовуємо алфавіт з таблиці 3.1.

**Відкритий текст:** missing_operator; **Ключі:** $\mathbf{k_{стовпців}} = \mathbf{4132}$; $\mathbf{k_{рядків}} = \mathbf{3142}$

**Розв'язання**

**1)** За кількістю символів в обох ключах формуються три таблиці.

$$\mathbf{n_{рядків}} = \ell_{\mathbf{k_{рядків}}} + \mathbf{1} = \mathbf{4} + \mathbf{1} = \mathbf{5}; \qquad \mathbf{n_{стовпців}} = \ell_{\mathbf{k_{стовпців}}} + \mathbf{1} = \mathbf{4} + \mathbf{1} = \mathbf{5}$$

**2)** Спершу в початковій (лівій) таблиці розставляються значення ключів та порядково, зліва направо, записується текст повідомлення

| | **4** | **1** | **3** | **2** |
|---|---|---|---|---|
| **3** | m | i | s | s |
| **1** | i | n | g | _ |
| **4** | o | p | e | r |
| **2** | a | t | o | r |

Оригінал тексту
Ліва таблиця

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

Переставляння стовпців
Середня таблиця

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

Переставляння рядків
Права таблиця

Напрямок процесу шифрування

**3)** Проводиться переставлення:

**а)** в середню таблицю записується результат послідовної перестановки стовпців (ключ $\mathbf{k_{стовпців} = 4132}$ впорядковується за зростанням):

| | **4** | **1** | **3** | **2** |
|---|---|---|---|---|
| **3** | m | i | s | s |
| **1** | i | n | g | _ |
| **4** | o | p | e | r |
| **2** | a | t | o | r |

Оригінал тексту
Ліва таблиця

| | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| 3 | i | s | s | m |
| 1 | n | _ | g | i |
| 4 | p | r | e | o |
| 2 | t | r | o | a |

Переставляння стовпців
Середня таблиця

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Переставляння рядків
Права таблиця

Напрямок процесу шифрування

**б)** в праву таблицю записується результат послідовної перестановки рядків (ключ $\mathbf{k_{рядків} = 3142}$ впорядковується за зростанням):

| | **4** | **1** | **3** | **2** |
|---|---|---|---|---|
| **3** | m | i | s | s |
| **1** | i | n | g | _ |
| **4** | o | p | e | r |
| **2** | a | t | o | r |

Оригінал тексту
Ліва таблиця

| | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| 3 | i | s | s | m |
| 1 | n | _ | g | i |
| 4 | p | r | e | o |
| 2 | t | r | o | a |

Переставляння стовпців
Середня таблиця

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| **1** | n | _ | g | i |
| **2** | t | r | o | a |
| **3** | i | s | s | m |
| **4** | p | r | e | o |

Переставляння рядків
Права таблиця

Напрямок процесу шифрування

**4)** Для формування шифртекста, зчитують вміст правої таблиці по рядках зліва направо.

**Шифртекст:** n_gitroaissmpreo

***Алгоритм дешифрування***

1) За кількістю символів в обох ключах формуються три таблиці.

$$\mathbf{n_{рядків} = \ell_{k_{рядків}} + 1}; \qquad \mathbf{n_{стовпців} = \ell_{k_{стовпців}} + 1}$$

Додатковий рядок і стовпець використовуються для запису ключів:

а) над першим рядком кожної таблиці записується ключ $\mathbf{k_{стовпців}}$;

б) перед першим стовпцем кожної таблиці записується – ключ $\mathbf{k_{рядків}}$.

2) Заповнюється права таблиця:

а) розставляються значення ключів за зростанням значень;

б) криптограма записується в таблицю послідовно по рядках зліва на право.

3) Проводиться переставляння:

а) у середній таблиці рядки переставляються відповідно до заданого порядком цифр ключа $\mathbf{k_{рядків}}$;

б) в лівій таблиці стовпці переставляються відповідно до заданого порядком цифр ключа $\mathbf{k_{стовпців}}$.

4) Для формування відкритого тексту, зчитують вміст лівої таблиці по рядках зліва направо.

**Приклад 3.3.** Провести дешифрування методом подвійної перестановки. Використовуємо алфавіт з таблиці 3.1.

**Шифртекст:** n_gitroaissmpreo

**Ключі:** $\mathbf{k_{стовпців} = 4132}$; $\mathbf{k_{рядків} = 3142}$

**Розв'язання**

**1)** За кількістю символів в обох ключах формуються три таблиці.

$\mathbf{n_{рядків} = \ell_{k_{рядків}} + 1 = 4 + 1 = 5}$; $\mathbf{n_{стовпців} = \ell_{k_{стовпців}} + 1 = 4 + 1 = 5}$

**2)** Спершу в правій таблиці розставляються значення цифр ключів за зростанням та порядково, зліва направо, записується текст криптограми

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| **1** | n | _ | g | i |
| **2** | t | r | o | a |
| **3** | i | s | s | m |
| **4** | p | r | e | o |

Оригінал тексту
Ліва таблиця

Переставляння стовпців
Середня таблиця

Переставляння рядків
Права таблиця

напрямок процесу дешифрування

←

**3)** Проводиться переставляння:

а) у середній таблиці рядки переставляються відповідно до заданого порядком цифр ключа $\mathbf{k_{рядків} = 3142}$;

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| **3** | i | s | s | m |
| **1** | n | _ | g | i |
| **4** | p | r | e | o |
| **2** | t | r | o | a |

| | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| **1** | n | _ | g | i |
| **2** | t | r | o | a |
| **3** | i | s | s | m |
| **4** | p | r | e | o |

Оригінал тексту
Ліва таблиця

Переставляння стовпців
Середня таблиця

Переставляння рядків
Права таблиця

напрямок процесу дешифрування

←

б) в лівій таблиці стовпці переставляються відповідно до заданого порядком цифр ключа $\mathbf{k_{стовпців}}$.

| | **4** | **1** | **3** | **2** |
|---|---|---|---|---|
| 3 | m | i | s | s |
| 1 | i | n | g | _ |
| 4 | o | p | e | r |
| 2 | a | t | o | r |

Оригінал тексту
Ліва таблиця

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| **3** | i | s | s | m |
| **1** | n | _ | g | i |
| **4** | p | r | e | o |
| **2** | t | r | o | a |

Переставляння стовпців
Середня таблиця

| | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| **1** | n | _ | g | i |
| **2** | t | r | o | a |
| **3** | i | s | s | m |
| **4** | p | r | e | o |

Переставляння рядків
Права таблиця

напрямок процесу дешифрування

←

4) Для формування відкритого тексту, зчитують вміст лівої таблиці по рядках зліва направо.

**Відкритий текст:** missing_operator

**Завдання**

**1.** Зашифруйте за допомогою шифру стандартної перестановки за ключем повідомлення, яке вибране з таблиці відповідно до номера варіанта. Алфавіт з таблиці 3.1.

| **№ варіанту** | **1** | **2** |
|---|---|---|
| ключ | line | column |
| повідомлення | array_type_required | constant_expression_expected |
| **№ варіанту** | **3** | **4** |
| ключ | exit | click |
| повідомлення | data_type_too_large | expression_expected |
| **№ варіанту** | **5** | **6** |
| ключ | button | edit |
| повідомлення | expression_too_complicated | file_type_not_allowed_here |
| **№ варіанту** | **7** | **8** |
| ключ | close | drop |
| повідомлення | function_needs_result_type | invalid_function_result_type |
| **№ варіанту** | **9** | **10** |
| ключ | create | menu |
| повідомлення | missing_operator_or_semicolon | missing_parameter_type |
| **№ варіанту** | **11** | **12** |
| ключ | destroy | resize |
| повідомлення | not_enough_actual_parameters | ordinal_type_required |
| **№ варіанту** | **13** | **14** |
| ключ | style | window |
| повідомлення | syntax_error_in_real_number | too_many_actual_parameters |
| **№ варіанту** | **15** | |
| ключ | hide | |
| повідомлення | unterminate_string | |

**2.** Дешифруйте за допомогою шифру стандартної перестановки за

ключем криптограму, обрану з таблиці відповідно до номера варіанта. Алфавіт з таблиці 3.1.

| **№ варіанту** | **1** | **2** |
|---|---|---|
| ключ | destroy | hide |
| шифртекст | ctei_rcoaxoeetnnpnxseste psd | _ia_rrrteeryqdapu_ye |
| **№ варіанту** | **3** | **4** |
| ключ | close | edit |
| шифртекст | eteoxxesnppds_er_iec | tdtayaorptogea_e_ _l |
| **№ варіанту** | **5** | **6** |
| ключ | exit | mouse |
| шифртекст | fa_pilhelle_eorn_weote_tyd | eespodxilo_poi_ _rncc_e_ao_sttm |
| **№ варіанту** | **7** | **8** |
| ключ | menu | click |
| шифртекст | _iolfnntuv_ _nartcleytispidue | fudpoulsennt_ _ _c_r_ntte_eiys_e |
| **№ варіанту** | **9** | **10** |
| ключ | drop | resize |
| шифртекст | mmtgiey_stppseeair_rn_ _a | normesgl_ire_oosamonrstip_ _ioc |
| **№ варіанту** | **11** | **12** |
| ключ | window | column |
| шифртекст | _xo_ser_rnyree_un_arimt_lrnba | n_renaoaaroltcmsu_ _te_gpeut_ha |
| **№ варіанту** | **13** | **14** |
| ключ | create | style |
| шифртекст | _otdnurry_aiedp_lrqie_ _e | rrtnusaoya_mo_l_e_a_ _tmcp_eata |
| **№ варіанту** | **15** | |
| ключ | line | |
| шифртекст | imuenin_gnts_aet_trr | |

3. Зашифруйте за допомогою шифру подвійної перестановки повідомлення, вибране з таблиці відповідно до номера варіанта. Використовувати алфавіт $\mathbf{Z}_{33}$, який наданий в таблиці 3.2.

Таблиця 3.2

Алфавіт $\mathbf{Z}_{33}$

| **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
|---|---|---|---|---|---|---|---|---|---|
| **a** | **b** | **c** | **d** | **e** | **f** | **g** | **h** | **i** | **j** |

| **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** |
|---|---|---|---|---|---|---|---|---|---|
| **k** | **l** | **m** | **n** | **o** | **p** | **q** | **r** | **s** | **t** |

| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
|---|---|---|---|---|---|---|---|---|---|
| u | v | w | x | y | z | . | , | ; | : |

| 30 | 31 | 32 |
|---|---|---|
| ' | { | } |

| **№ варіанта** | 1 | | 2 | |
|---|---|---|---|---|
| ключі | $\mathbf{k}_{\text{стовпців}}=34512$ | $\mathbf{k}_{\text{рядків}}=54132$ | $\mathbf{k}_{\text{стовпців}}=45321$ | $\mathbf{k}_{\text{рядків}}=12453$ |
| повідомлення | ';' expected but ':' found | | 'cha' is not a type identifier | |
| **№ варіанта** | 3 | | 4 | |
| ключі | $\mathbf{k}_{\text{стовпців}}=35412$ | $\mathbf{k}_{\text{рядків}}=13425$ | $\mathbf{k}_{\text{стовпців}}=32145$ | $\mathbf{k}_{\text{рядків}}=13245$ |
| повідомлення | ';' not allowed before 'else' | | expression too complicated | |
| **№ варіанта** | 5 | | 6 | |
| ключі | $\mathbf{k}_{\text{стовпців}}=52431$ | $\mathbf{k}_{\text{рядків}}=13452$ | $\mathbf{k}_{\text{стовпців}}=23541$ | $\mathbf{k}_{\text{рядків}}=12354$ |
| повідомлення | file type not allowed here | | function needs result type | |
| **№ варіанта** | 7 | | 8 | |
| ключі | $\mathbf{k}_{\text{стовпців}}=32154$ | $\mathbf{k}_{\text{рядків}}=13254$ | $\mathbf{k}_{\text{стовпців}}=35412$ | $\mathbf{k}_{\text{рядків}}=54321$ |
| повідомлення | invalid function result type | | low bound exceeds high bound | |
| **№ варіанта** | 9 | | 10 | |
| ключі | $\mathbf{k}_{\text{стовпців}}=53214$ | $\mathbf{k}_{\text{рядків}}=34512$ | $\mathbf{k}_{\text{стовпців}}=53421$ | $\mathbf{k}_{\text{рядків}}=32154$ |
| повідомлення | not enough actual parameters | | syntax error in real number | |
| **№ варіанта** | 11 | | 12 | |
| ключі | $\mathbf{k}_{\text{стовпців}}=41235$ | $\mathbf{k}_{\text{рядків}}=35412$ | $\mathbf{k}_{\text{стовпців}}=23154$ | $\mathbf{k}_{\text{рядків}}=45321$ |
| повідомлення | too many actual parameters | | '.' expected but ';' found | |
| **№ варіанта** | 13 | | 14 | |
| ключі | $\mathbf{k}_{\text{стовпців}}=$ 2 3 1 4 5 | $\mathbf{k}_{\text{рядків}}=53214$ | $\mathbf{k}_{\text{стовпців}}=12354$ | $\mathbf{k}_{\text{рядків}}=23541$ |
| повідомлення | function needs result type | | invalid function result type | |
| **№ варіанта** | 15 | | | |
| ключі | $\mathbf{k}_{\text{стовпців}}=51234$ | $\mathbf{k}_{\text{рядків}}=34512$ | | |
| повідомлення | ‘rea’ is not a type identifier | | | |

**4.** Дешифруйте за допомогою шифру подвійної перестановки криптограму, обрану з таблиці відповідно до номера варіанта. Використовувати алфавіт $\mathbf{Z}_{33}$, який наданий в таблиці 3.2.

| **№ варіанта** | **1** | | **2** | |
|---|---|---|---|---|
| ключі | $\mathbf{k}_{\text{стовпців}}=35412$ | $\mathbf{k}_{\text{рядків}}=34512$ | $\mathbf{k}_{\text{стовпців}}=12354$ | $\mathbf{k}_{\text{рядків}}=34512$ |
| повідомлення | hbhgidzonubolwoexudndscee | | resluttyepinvlaidfnuctino | |
| **№ варіанта** | **3** | | **4** | |
| ключі | $\mathbf{k}_{\text{стовпців}}=23145$ | $\mathbf{k}_{\text{рядків}}=45321$ | $\mathbf{k}_{\text{стовпців}}=23154$ | $\mathbf{k}_{\text{рядків}}=53214$ |
| повідомлення | eypzzlsuttsedrenfuctnione | | f;’uoudb'tcpeetzndzz”.xe | |
| **№ варіанта** | **5** | | **6** | |

| | | | | |
|---|---|---|---|---|
| ключі | $\mathbf{k}_{\text{стовпців}} = 41235$ | $\mathbf{k}_{\text{рядків}} = 32154$ | $\mathbf{k}_{\text{стовпців}} = 53421$ | $\mathbf{k}_{\text{рядків}} = 35412$ |
| повідомлення | alpuayacntoomtarszezamert | | mulnazzerbatynserinrorerx | |
| **№ варіанта** | **7** | | **8** | |
| ключі | $\mathbf{k}_{\text{стовпців}} = 53214$ | $\mathbf{k}_{\text{рядків}} = 54321$ | $\mathbf{k}_{\text{стовпців}} = 51234$ | $\mathbf{k}_{\text{рядків}} = 23541$ |
| повідомлення | retsearampautlchguaoetonn | | terseotennughaoaramptualc | |
| **№ варіанта** | **9** | | **10** | |
| ключі | $\mathbf{k}_{\text{стовпців}} = 13254$ | $\mathbf{k}_{\text{рядків}} = 32154$ | $\mathbf{k}_{\text{стовпців}} = 23541$ | $\mathbf{k}_{\text{рядків}} = 13452$ |
| повідомлення | citnoifdnuivnlatyteprselu | | tfucnzypzeeionneedrstsutl | |
| **№ варіанта** | **11** | | **12** | |
| ключі | $\mathbf{k}_{\text{стовпців}} = 52431$ | $\mathbf{k}_{\text{рядків}} = 12354$ | $\mathbf{k}_{\text{стовпців}} = 32145$ | $\mathbf{k}_{\text{рядків}} = 13425$ |
| повідомлення | tielfopneyoalltzezzreehdw | | pxerelpmicissonootcoetadz | |
| **№ варіанта** | **13** | | **14** | |
| ключі | $\mathbf{k}_{\text{стовпців}} = 35412$ | $\mathbf{k}_{\text{рядків}} = 13245$ | $\mathbf{k}_{\text{стовпців}} = 45321$ | $\mathbf{k}_{\text{рядків}} = 54132$ |
| повідомлення | no";bewdelotlae'froe'esl | | epyatreiiftneidtonis'ah'c | |
| **№ варіанта** | **15** | | | |
| ключі | $\mathbf{k}_{\text{стовпців}} = 34512$ | $\mathbf{k}_{\text{рядків}} = 12453$ | | |
| повідомлення | ex';'tepeczzndzt'dbuou:'f | | | |

**Контрольні запитання**

1. Дайте визначення терміну «шифрування».
2. Дайте визначення терміну «дешифрування».
3. Дайте визначення терміну «розтин шифру».
4. Дайте визначення терміну «шифр».
5. Дайте визначення терміну «відкритий текст».
6. Дайте визначення терміну «шифртекст».
7. Дайте визначення терміну «ключ».
8. Дайте визначення терміну «криптосистема».
9. Які шифри називають блоковими.
10. Які криптосистеми називають симетричними.
11. Які шифри називають «шифрами перестановки».
12. Опишіть алгоритми шифрування і дешифрування одиночної перестановки за ключем.
13. Опишіть алгоритми шифрування і дешифрування подвійної перестановки.