**Група ІПС-41, Шатохін Максим Сергійович**

**Тема: Алгебра Варіант 16**

**Текст для шифрування:**

you read too loud read much more slowly and with expression

**Ключове слово:**

excellent

**Завдання:**

Зашифрувати і розшифрувати заданий текст, використавши властивості таких алгебр:

1. Групи підстановок;

2. Скінченні кільця;

3. Скінченні поля.

Описати хід виконання завдання.

***Розв’язання***

***Завдання №1.***

Як алгоритм шифрування використаємо блоковий спосіб шифрування.

***Опис*** алгоритму шифрування:

1. Розбиваємо на блоки довжини слова ключ
2. Кожний символ в блоці перетворюється за допомогою підстановок , кожна з яких має вигляд:

де *k* – номер літери у алфавіті *X*, a – її відповідник у алфавіті *X* при підстановці , *i = 1, 2, 3, … t.*

Вважаємо, що всі маленькі літери англійського алфавіту нумеруються з 0 до 25, а всі великі транслюються в маленькі. (Тобто ‘a’ – 0, ‘b’ – 1, …, ‘z’ = 25).

***Псевдо-код*** для шифрування:

# SIZE – кількість різних букв у алфавіті

SIZE = 26

#letter – текст для шифрування, key – слово ключ

блочне\_шифрування(letter, key):

letter := позбавляємось\_від\_пробільних\_символів\_у letter

# лічильник для проходу по слову ключ

k := 0

letter\_num := переводимо букви у числа для letter

key\_num := переводимо букви у числа для key

answer := “”

для i від 1 до довжини letter\_num:

value := (letter\_num[i] + key\_num[k]) % SIZE

# операція += це конкатинація рядка з символом.

answer += переводимо число до букви для value

# лічильник для k змінюється за модулем довжини слова ключ

k := (k + 1) % length(key\_num)

повернути answer

***Шифруємо текст:*** s = “you read too loud read much more slowly and with expression”.

***Слово ключ:*** key = “excellent”.

***Зашифрований текст:*** (запускаємо функцію блочного шифрування)

ciphered = блочне\_шифрування(s, key) =>

ciphered = “clwvplhghsiqyocinwqrelxzvrlplypjlrqpmqjiiavrlwfqr”.

***Дешифрування*** виконується таким чином:

***Псевдо-код*** для дешифрування:

# SIZE – кількість різних букв у алфавіті

SIZE = 26

#ciphered – текст для розшифрування, key – слово ключ

блочне\_розшифрування(ciphered, key):

ciphered:= позбавляємось\_від\_пробільних\_символів\_у ciphered

# лічильник для проходу по слову ключ

k := 0

ciphered\_num := переводимо букви у числа для ciphered

key\_num := переводимо букви у числа для key

answer := “”

для i від 1 до довжини ciphered\_num:

# додаємо SIZE щоб позбутися негативних значень

value := (ciphered\_num[i] - key\_num[k] + SIZE) % SIZE

# операція += це конкатинація рядка з символом.

answer += переводимо число до букви для value

# лічильник для k змінюється за модулем довжини слова ключ

k := (k + 1) % length(key\_num)

повернути answer

***Зашифрований текст:*** s = “clwvplhghsiqyocinwqrelxzvrlplypjlrqpmqjiiavrlwfqr”.

***Слово ключ:*** key = “excellent”.

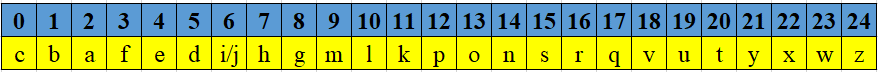
***Розшифрований текст:*** (запускаємо функцію блочного розшифрування)

deciphered = блочне\_розшифрування(s, key) =>

deciphered = “youreadtooloudreadmuchmoreslowlyandwithexpression”.

***Завдання №2***

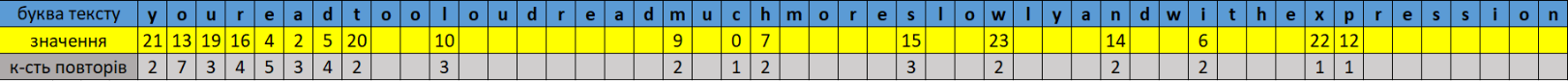
Для кільця візьмемо таку таблицю відповідності чисел до алфавіту англійської мови.



*Таблиця відповідності символів алфавіту до числа*

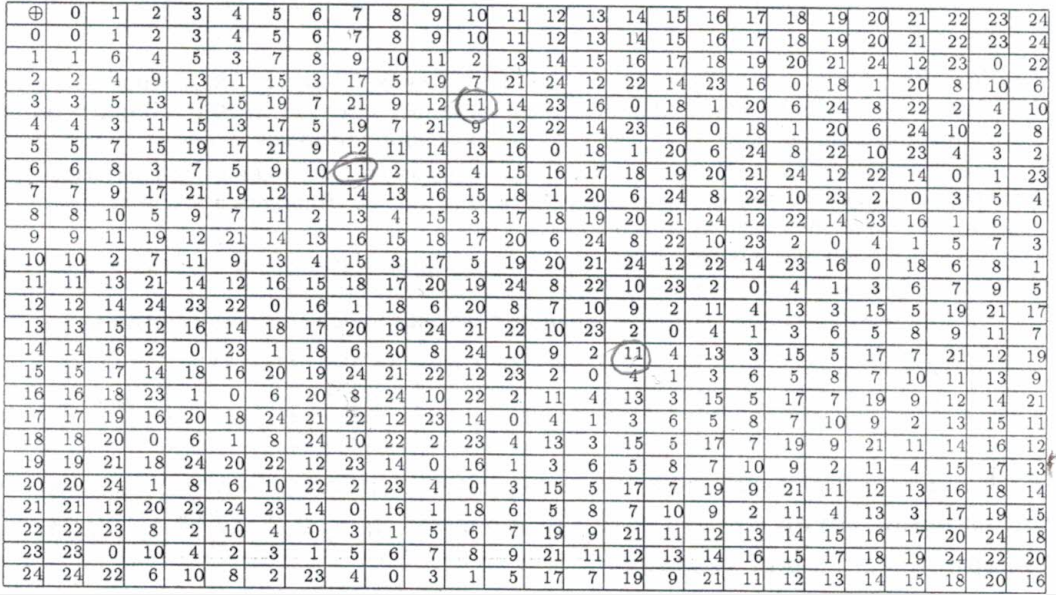
Для тексту “if you have any question you can safely interrupt me” застосуємо алгоритм ***гомофонічного*** шифрування. Для шифрування будемо використовувати таблицю додавання кільця .

Для початку складемо таблицю гомофонів. Для цього спершу підрахуємо кількість повторів для кожної букви:



*Таблиця відповідності символів алфавіту до кількісті повторів*

*(при повторі не показуємо значення)*



*Таблиця додавання кільця .*

Оскільки ми маємо всі значення символів і скільки разів вони повторюються, то можна побудувати саму таблицю гомофонів використовуючи таблицю додавання кільця .

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Символ*** | ***Гомофони*** | | | | | | |
| y | 0505 | 0904 |  |  |  |  |  |
| o | 0203 | 0906 | 1101 | 1005 | 1722 | 2021 | 1416 |
| u | 0704 | 1110 | 0615 |  |  |  |  |
| r | 0612 | 1105 | 0907 | 1402 |  |  |  |
| e | 0323 | 0401 | 2407 | 1921 | 1514 |  |  |
| a | 0918 | 2304 | 0322 |  |  |  |  |
| d | 0103 | 0723 | 0802 | 1716 |  |  |  |
| t | 1801 | 2102 |  |  |  |  |  |
| l | 0801 | 2204 | 0916 |  |  |  |  |
| m | 1004 | 1123 |  |  |  |  |  |
| c | 1909 |  |  |  |  |  |  |
| h | 0804 | 0210 |  |  |  |  |  |
| s | 1301 | 0403 | 1418 |  |  |  |  |
| w | 1203 | 2008 |  |  |  |  |  |
| n | 1201 | 2420 |  |  |  |  |  |
| i | 0101 | 1319 |  |  |  |  |  |
| x | 1808 |  |  |  |  |  |  |
| p | 0213 |  |  |  |  |  |  |

*Таблиця гомофонів*

Заміняємо усі літери тексту на відповідні значення гомофонів і отримаємо шифрограму.



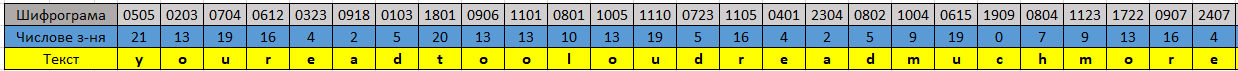
*Початок таблиці відповідності тексту до шифрограми*



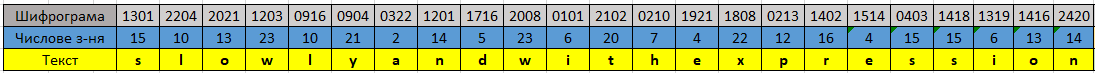
*Кінець таблиці відповідності тексту до шифрограми*

Для того щоб ***розшифрувати*** шифрограму, отримувачу потрібно, ще додатково мати таблицю відповідності чисел до символів та таблицю додавання кільця .

Підрахуємо результат розшифрування:



*Початок таблиці відповідності шифрограми до тексту*



*Кінець таблиці відповідності шифрограми до тексту*

Результат розшифрування співпадає з початковим значення тексту.

***Завдання №3***

Нехай літери алфавіту *Х = {a, b, s, d, … , x, y, z}* англійської мови лінійно упорядковані такий чином:

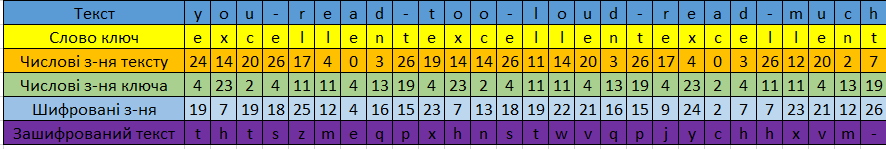


До 26 літер англійського алфавіту, ще додамо 27-ий символ “-” і побудуємо поле за допомогою незвідного полінома , що надасть нам таблицю додавання (див. наступну сторінку).

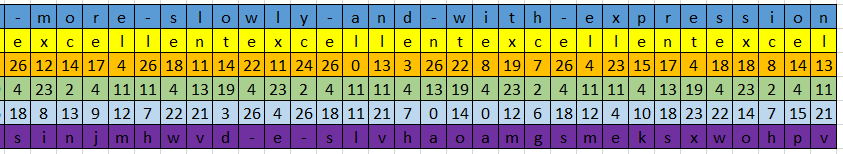
***Зашифруємо*** текст “you read too loud read much more slowly and with expression” за ***ключем*** “excellent

”.

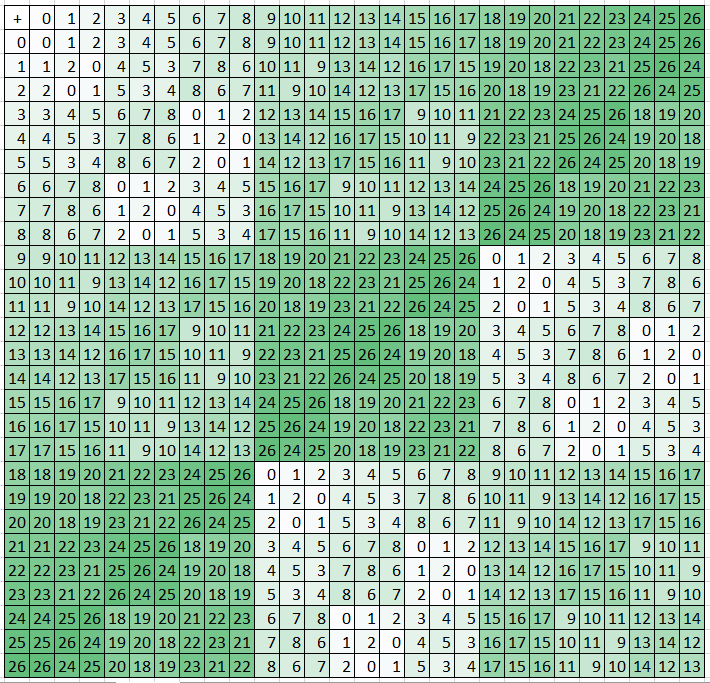
Під час шифрування будемо заповнювати таблицю, де для кожної пари літер будемо знаходити їх числові значення, брати їх як номери рядка та стовбця у адитивній таблиці групи поля та вписувати значення, що знаходяться на перетині рядка зі стовпчиком.



*Початок таблиці шифрування тексту по ключу*



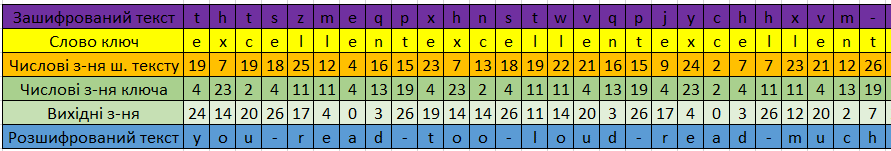
*Кінець таблиці шифрування тексту по ключу*



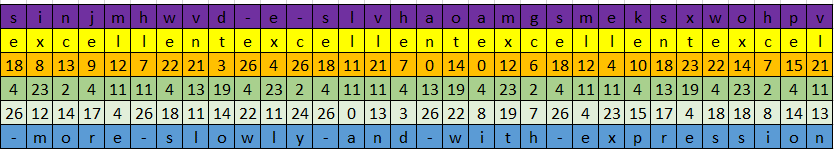
*Таблиця адитивної групи поля .*

***Розшифровуємо*** шифрограму:

1. Виписуємо числові значення для літер шифрограми та ключового слова
2. Після цього кожне значення ключа представляємо як рядок
3. Шукаємо у рядку числове значення літери шифрограми
4. Стовпик заданого значення і є вихідним значенням тексту



*Початок таблиці розшифрування тексту по ключу*



*Кінець таблиці розшифрування тексту по ключу*

Розшифрований текст співпадає з початковим.