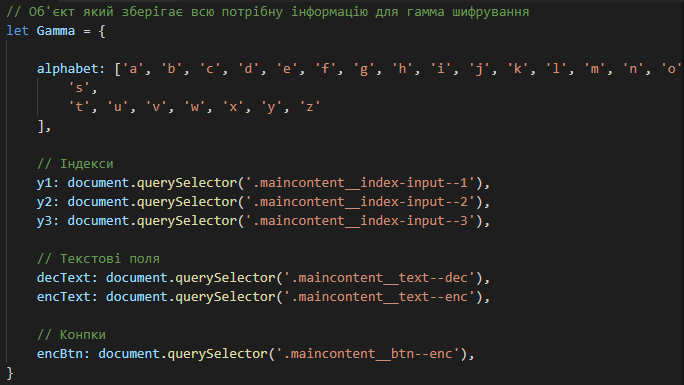
**Лабораторна робота № 3**

**Заремського Артема ( 414 група )**

1. **ЕТАП 1**, написати об’єкт з властивостями, в яких буде міститися інформація про алфавіт та про те, що було введено в поля користувачем:
2. Алфавіт;
3. Зчитувати індекси;
4. Зчитувати слова з textarea;
5. Зчитувати стан кнопкок.

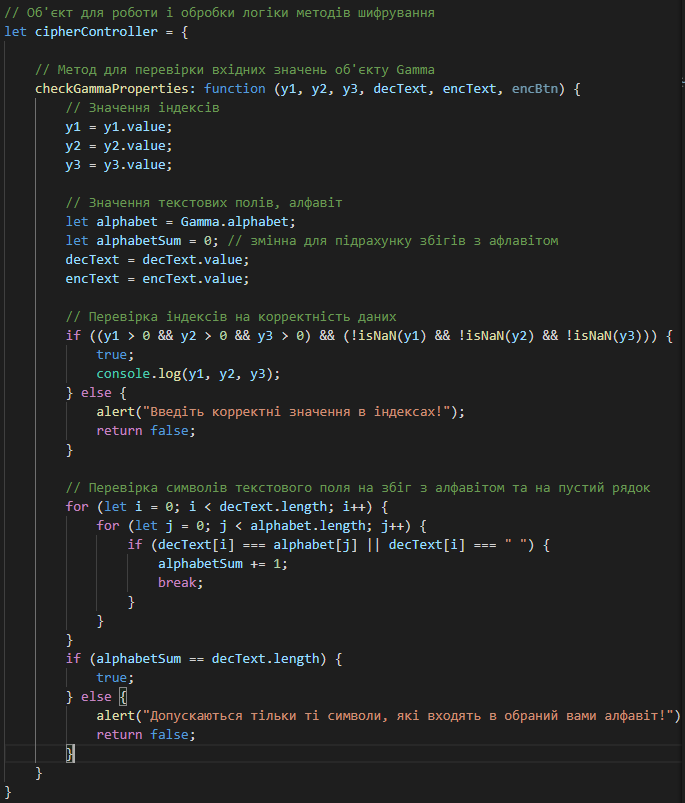


1. **ЕТАП 2**, написати об’єкт, який буде містити методи для роботи з об’єктами шифрування:
2. Перевірка Індексів:

* Повинні бути > 0;
* Повинні бути числовими.

1. Перевірка текстових полів:

* Символи тексту повинні збігатись з символами заданого алфавіту ( реалізуємо через цикл перебору та пошуку елементів массиву ).
* Текстове поле не повинне бути пустим.

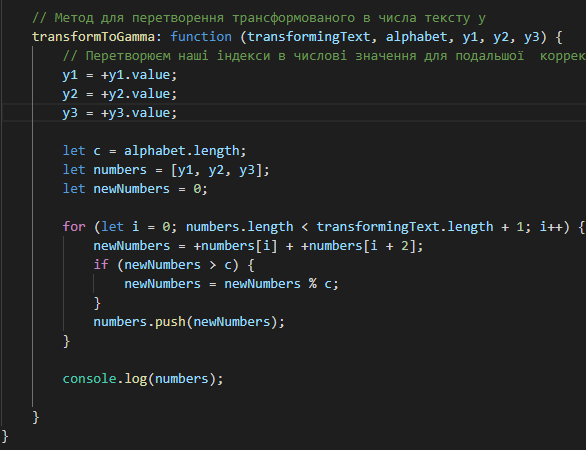


1. **ЕТАП 3**, написати метод для перетворення символів текстового поля в цифрові індекси їх положення у алфавіті.

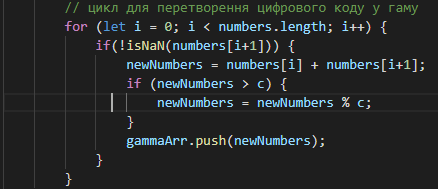


1. **ЕТАП 4,** написати метод для рахування індексів і складання гами для подальшої роботи з нею.

Метод для перетворення ключів в код по формулі.



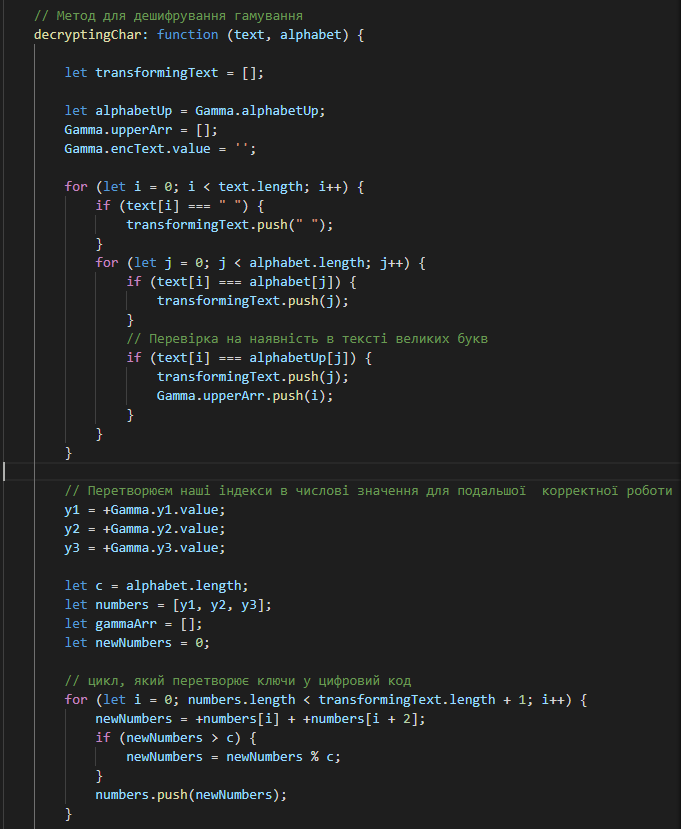
Метод для перетворення цифр у гаму.



1. **ЕТАП 5,**  Написати метод, який додає цифровий код до гами, переводить отримані числа у букви та виводить нам їх на екран у друге текстове поле.



1. **ЕТАП 6,** Написати метод, який дешифрує повідомлення, якщо відомі ключи.



**КОНТРОЛЬНІ ЗАПИТАННЯ**

1. Нехай у нас є відкрите повідомлення *t1,…,tn,* що являє собою послідовність символів. Ключ К являє собою послідовність чисел k1,…,kn з множини M={0,…,32}. Зашифрований текст s1,…,sn обчислюється за такою формулою: **si=(C(ti)+ki) mod 33**, де С – функція, що перетворює символ у його порядковий номер. Запис d=(a+b) mod m означає, що d співпадає із залишком від ділення на m суми чисел a+b, наприклад, 1=(4+7) mod 10. Визначений таким чином шифр називається шифром гаммування з випадковою рівноймовірною гаммою (гаммою прийнято називати послідовність чисел k1,…,kn, що додається за модулем до шифрованого повідомлення).
2. Запис d=(a+b) mod m означає, що d співпадає із залишком від ділення на m суми чисел a+b, наприклад, 1=(4+7) mod 10.
3. За допомогою ключів ми створюємо цифровий код за допомогою якого створуюється гама та шифрується наше повідомлення.
4. Ключ К являє собою послідовність чисел k1,…,kn з множини M={0,…,32}.
5. трудовитрати ручного дешифрування даного повідомлення методом прямого перебору ключів складає 555 годин. Процес можна прискорити, якщо застосувати ЕОМ. У цьому випадку результати генерування всіх ключів та дешифрування всіх варіантів буде отримано практично миттєво, і лише 9 годин знадобиться криптоаналітику для відбору істинного повідомлення серед хибних.
6. Якщо криптоаналітик буде відкидати по одному невірному повідомленню за секунду, то йому потрібно буде на те, щоби продивитися всі повідомлення приблизно 9 годин.
7. Таким чином, ми можемо розділити криптографічні алгоритми на три великих групи. До першої групи відносяться досконалі алгоритми, які не піддаються розкриттю при правильному використанні (наприклад, алгоритм одноразових блокнотів, або шифр гаммування випадковою рівноймовірною гаммою). Другу групу формують шифри, що допускають неоднозначне дешифрування. Наприклад, така ситуація виникає, коли шифрують за допомогою простої заміни коротке повідомлення. До третьої групи належать шифри, криптограми яких можуть бути однозначно розшифровані, однак складність дешифрування забезпечується трудомісткістю алгоритму дешифрування. Тобто в останньому випадку стійкість шифру забезпечується складністю алгоритмів дешифрування.
8. Розшифрувати повідомлення можна за допомогою формули. Відкидати по одному невірному повідомленню за секунду. Якщо ми маємо частину зашифрованого повідомлення, наприклад, знаємо, що воно починається з літер «НАК». У алгоритмі заміни номер Н=16, А=00, К=13. Це означає, що виконуються співвідношення: (16+ Z1) mod 32 =19; (00+ Z2) mod 32 =14 i (13+ Z3) mod 32 =15. Звідси можна знайти перших три знаки гамми: 3; 14; 2. Тепер можна скласти систему з таких трьох рівнянь.
9. Задавати більше ключів.