Міністерство освіти і науки України

КПІ ім. Ігоря Сікорського

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій (ІСТ)

Звіт до комп’ютерного практикуму №5

З дисципліни

«Алгоритми та математичні методи захисту інформації»

Підготував:

Студент групи ІК-02

Талько Ярослав

Перевірив:

Нестерук А.

Київ 2024

**Тема:** Криптосистема Ель-Ґамаля.

**Мета:** Навчитися використовувати криптосистему Ель-Гамаля для шифрування повідомлень.

**Хід роботи**

Код програми написаний мовою JS. Спочатку розглянемо основну роботу програми:

****

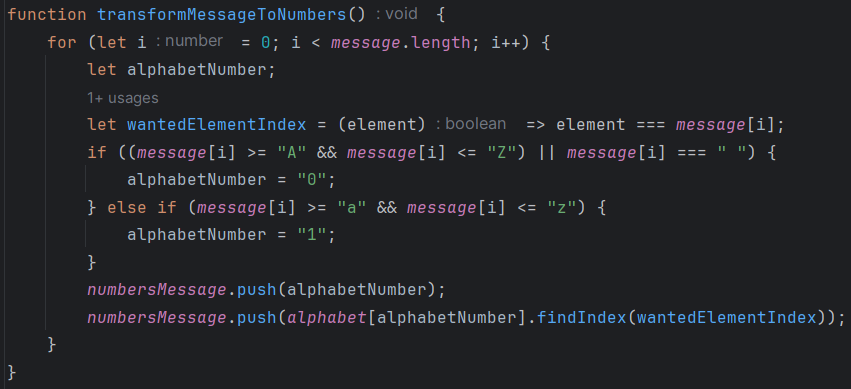
Так, як у мене 41 варіант, то я взяв 11 варіант з 30 доступних. Розглянемо змінні:

* alphabet – змінна, що зберігає всередині себе англійський алфавіт великих та малих букв окремо + пробіл;
* g та p – числа, що дані за умовою. Їхнім найбільшим спільним дільником повинно бути число 1;
* a – випадкове число, яке повинно бути в інтервалі [1; p-2];
* h – первісний корінь g за модулем p;
* r – випадкове число, яке повинно бути в інтервалі [1; p-1];
* c1 – лазівка;
* c2 – шифротекст;
* message – повідомлення, яке необхідно зашифрувати;
* decodeMessage – розшифроване повідомлення;
* numbersMessage – масив, що зберігає повідомлення в числах;
* decodeNumbersMessage – масив, що зберігає розшифроване повідомлення в числах.

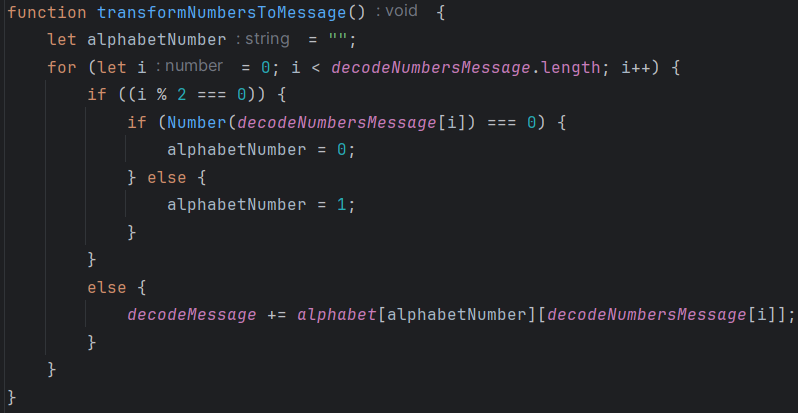
Далі йдуть функції:

* transformMessageToNumbers() – переводить повідомлення в числа;
* transformNumbersToMessage() – переводить числа в повідомлення;
* elGamalKeys() – присвоює змінній h значення;
* elGamalEncrypt() – створює лазівки та шифротекст;
* elGamalDecrypt() – розшифровує повідомлення.
* getRandomInt() – функція, що використовується по ходу програми

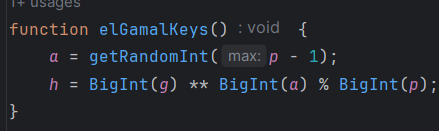
Розберемо функції детальніше:



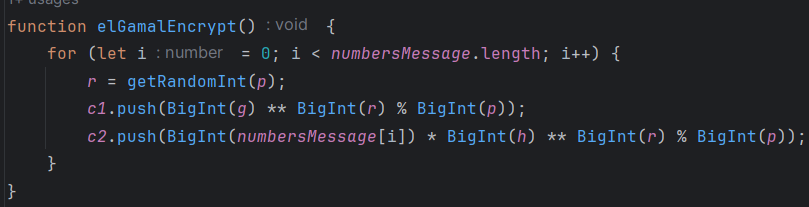
Основна задача функції «перетворення в числа» – це знайти відповідний символ у масиві alphabet і запихнути знайдений індекс у масив numbersMessage. Важливо зазначити, для того, щоб визначити чи літера є частиною верхнього/нижнього реґістру, перед кожним з символів, що перетворюється у число, вставляється у масив 0 або 1, що позначає алфавіт великих та малих літер відповідно.



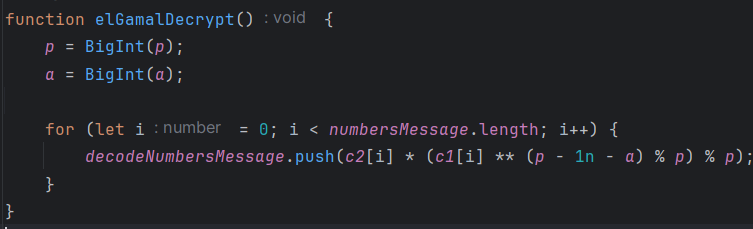
Функція «перетворення чисел в повідомлення» працює в зворотному порядку. Тобто береться кожне парний елемент масиву, в якому записане «позначення» на алфавіт. А потім за цим алфавітом та непарним елементом масиву шукається відповідна літера.



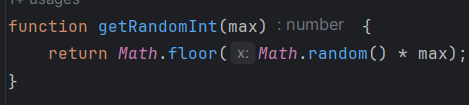
Функція «ключів Ель-Ґамаля» генерує число а в інтервалі [1; p-2] (тут показано p-1, бо функція генерації випадкового числа, генерує число від до максимального елемента не включно). Після чого обчислюємо значення первісного кореня g.



Функція шифрування проходить по всьому масиву і генерує число r в інтервалі [1; p-1]. Після чого створює лазівки та шифротекст.

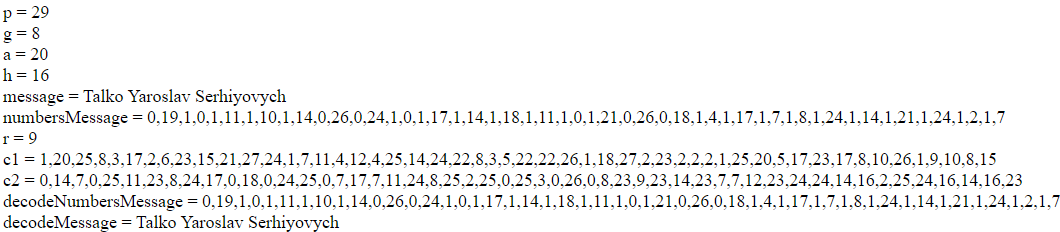


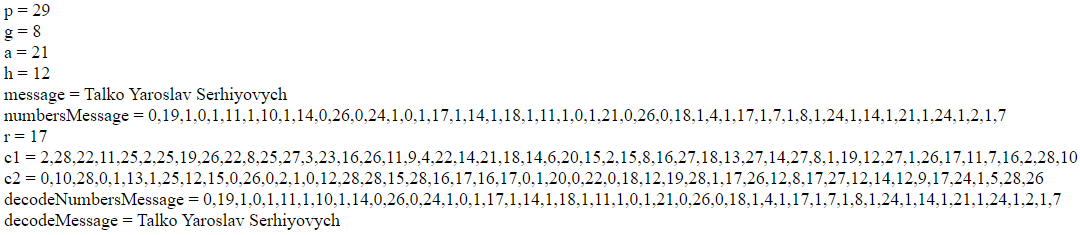
Функція розшифрування проходить по всьому масиву, використовує лазівку та шифротекст для розшифрування повідомлення.

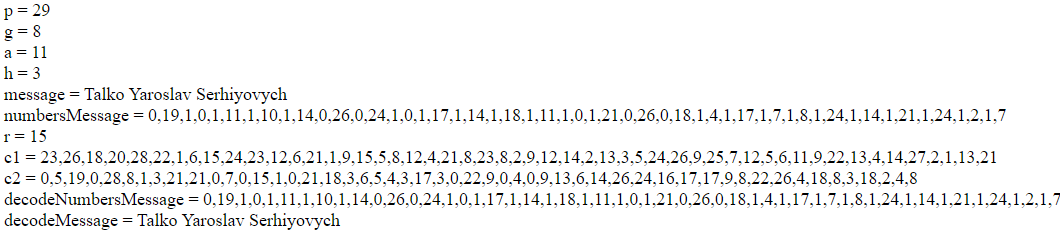


Функція генерації випадково числа генерує його в межах [1; max).

**Результати роботи програми:**







Одразу показую роботу програми при різних випадкових числах, аби запевнити в її роботі.

**Висновок:** На цій лабораторій роботі я навчився використовувати криптосистему Ель-Ґамаля для шифрування повідомлень.