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 №6

З дисципліни

«Алгоритми та математичні методи захисту інформації»

Підготував:

Студент групи ІК-02

Талько Ярослав

Перевірив:

Нестерук А.

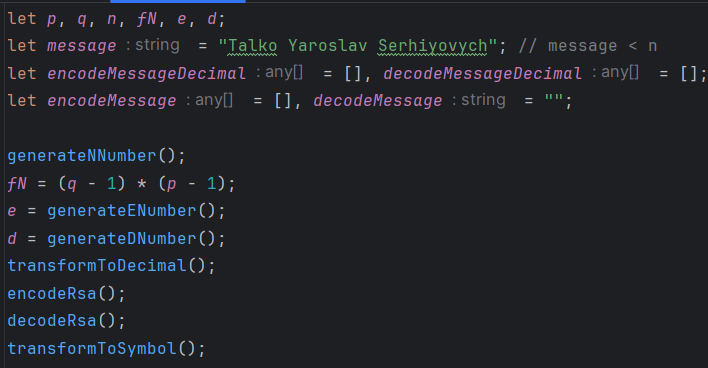
Київ 2024

**Тема:** Криптографічна система RSA.

**Мета:** Вивчити криптографічну систему RSA, на практиці здійснити формування ключа, шифрування і розшифрування фрагмента інформації в даній системі.

**Хід роботи**

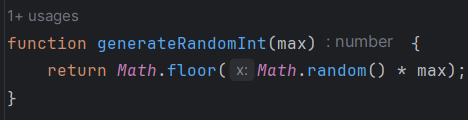
Код програми написаний мовою JS. Спочатку розглянемо основну роботу програми:



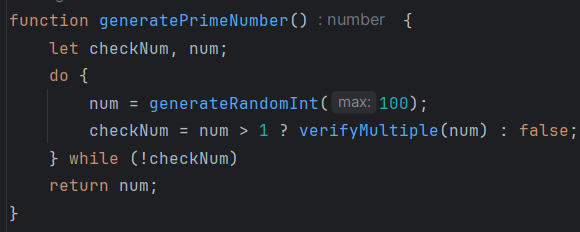
Почнемо зі змінних:

* p, q – два простих числа;
* n – добуток p та q;
* fN – значення функції Ейлера;
* e – випадкове непарне (просте) число, взаємно просте з fN;
* d – обернене число е за модулем fN;
* encodeMessageDecimal та decodeMessageDecimal – змінні, які зберігають повідомлення у вигляді чисел;
* encodeMessage та decodeMessage – відповідно зашифроване та розшифроване повідомлення;

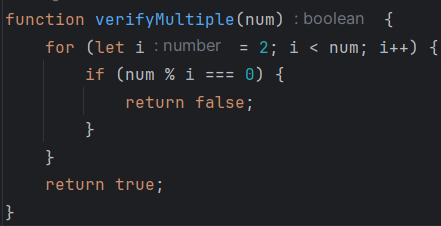
Тепер перейдемо одразу до детального розбору функцій:



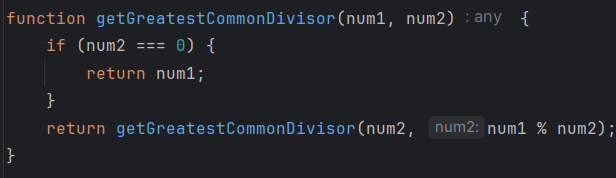
Дана функція займається генерацією простих чисел в інтервалі [1; max).



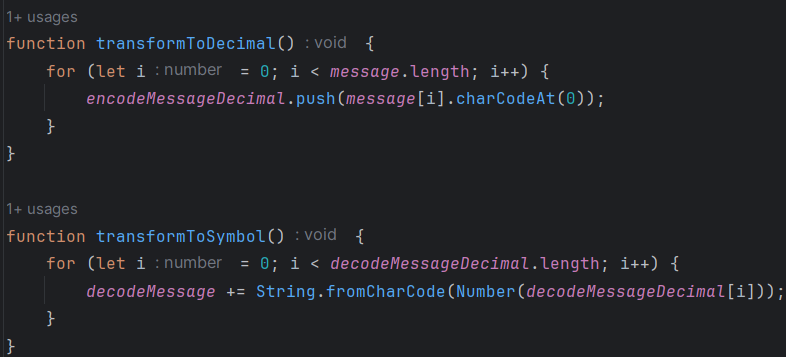
Дана функція генерує випадкове число в інтервалі [2; 99], після чого перевіряє, чи воно просте і лише тоді повертає;



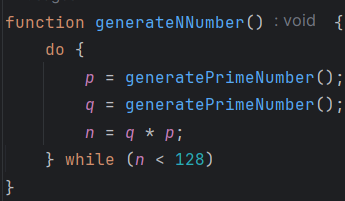
Дана функція перевіряє чи передане їй число справді просте.



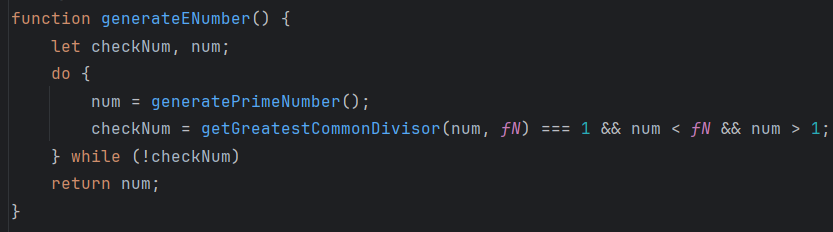
Дана функція повертає найбільший спільний дільник двох чисел.



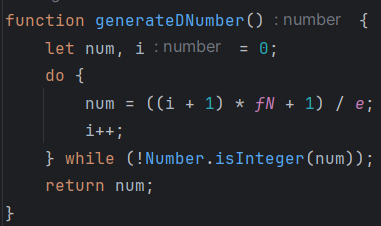
Функції transformToDecimal та transformToSymbol переводять повідомлення в числа та числа в повідомлення відповідно.



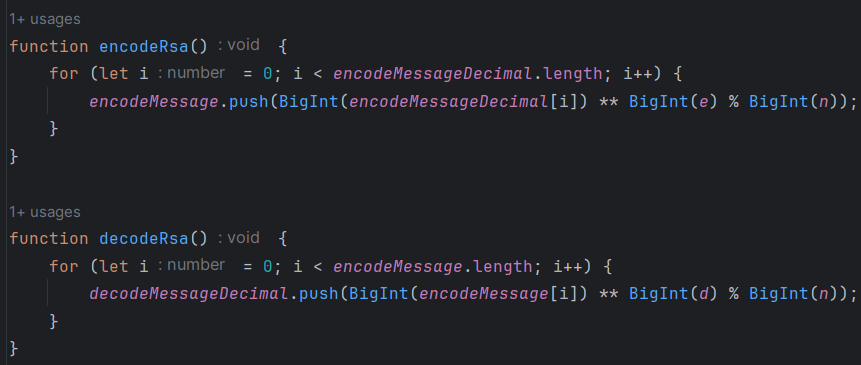
Далі йде функція, яка створює числа p, q та n. Було прийнято рішення обмежити нижній поріг n числом 128 (як у ASCII коді), аби полегшити процес шифрування.



Далі йде функція, яка створює число e. Було прийнято рішення зробити його простим. За замовчуванням число e генерується таким чином, що воно знаходиться в інтервалі (1; fN) і при цьому НСД з числом fN дорівнював одиниці.

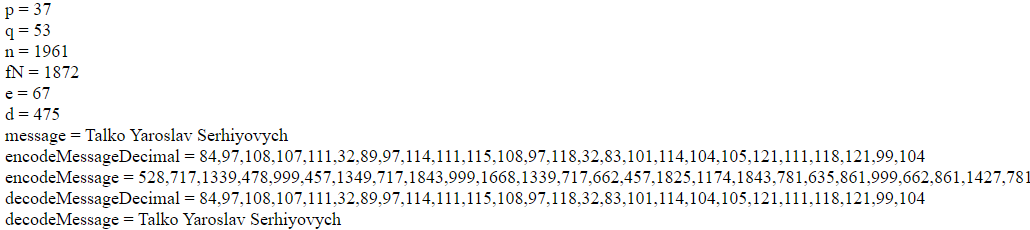


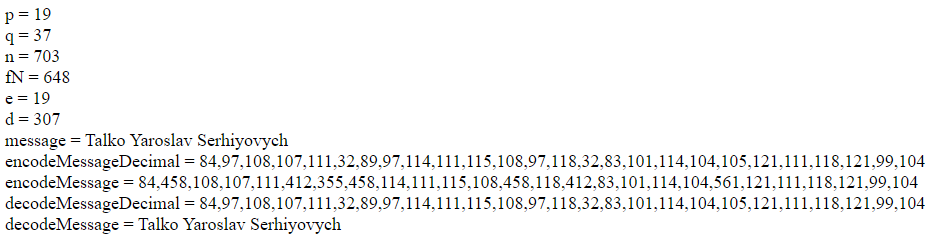
Далі йде функція, яка створює число d. Саме число d дістається за формулою ((i + 1) \* fN + 1) / e. В такому вигляді, збільшуючи ітерацію, відбувається перебирання чисел, поки не знайдеться перше ціле число.

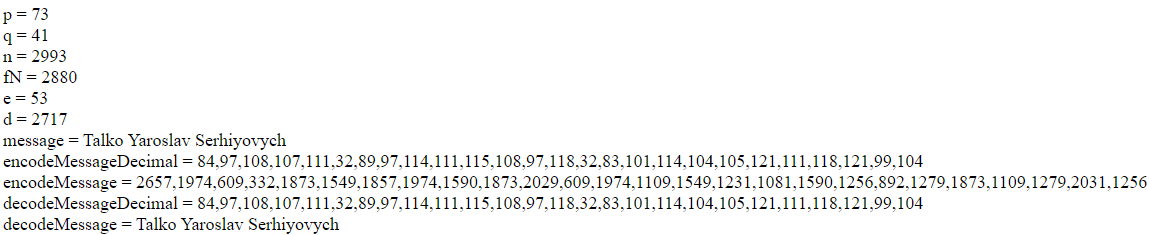


Далі йдуть функції шифрування та дешифрування. В шифруванні повідомлення, переведене в числа, шифрується з допомогою чисел e та n. В розшифруванні зашифроване повідомлення розшифровується з допомогою чисел d та n. На виході з розшифрування отримуються числа, які пізніше будуть переводитися в символи. Важливо зазначити, що повідомлення шифруються та розшифровуються по одному символу за ітерацію.

**Результати роботи програми:**

****

****

****

Одразу представляю кілька скриншотів, аби запевнити, що при різних випадкових значеннях повідомлення успішно шифрується та розшифровується.

**Висновок:** На цій лабораторній роботі я вивчив криптографічну систему RSA, на практиці здійснив формування ключа, шифрування і розшифрування фраґмента інформації в даній системі.