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 №7

З дисципліни

«Алгоритми та математичні методи захисту інформації»

Підготував:

Студент групи ІК-02

Талько Ярослав

Перевірив:

Нестерук А.

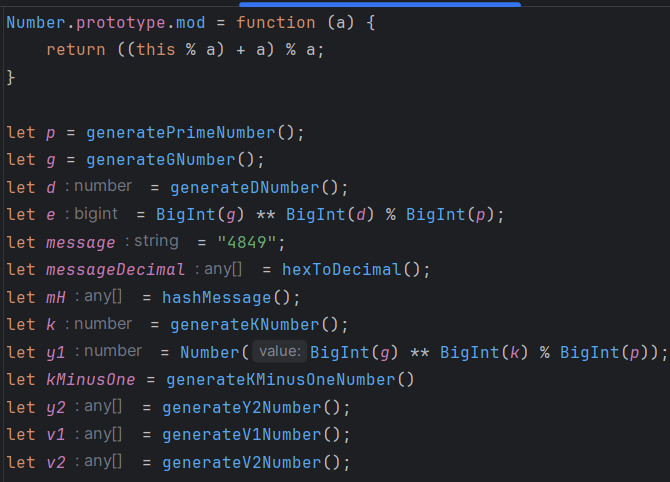
Київ 2024

**Тема:** Електронні цифрові підписи.

**Мета:** Вивчити застосування криптосистем з відкритим ключем до схем електронного цифрового підпису.

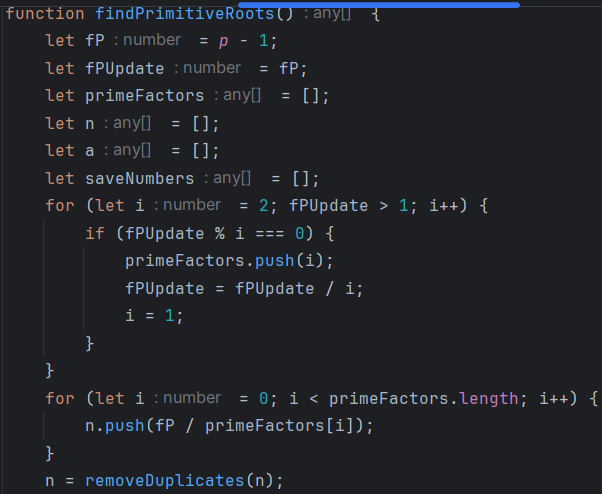
**Хід роботи першого завдання**

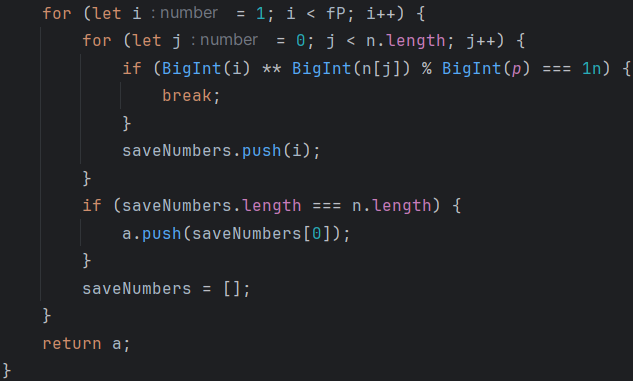
Код програми написаний мовою JS. Спочатку розглянемо основну роботу програми в 1 завданні (у мене 41 варіант, тому я виконував завдання №1 – ЕЦП Ель-Ґамаля):



* Number.prototype.mod – це функція, що дозволяє перевести число по модулю, аби вона було лише додатнім;
* p – велике просте число;
* g – первісний корінь за модулем p;
* d – навмання обране число з інтервалу [2; p-2];
* e – один з елементів відкритого ключа;
* message – повідомлення в 16-му форматі;
* messageDecimal – повідомлення, переведене у 10-ий формат;
* mH – загешоване повідомлення за методом гешування (m^3+9)mod(p-1);
* k – довільне число з інтервалу [1, p-1], де НСД(k, p-1) = 1;
* kMinusOne – обернене за модулем p-1 до k число;
* y1 та y2 – є підписом повідомлення;
* v1 та v2 – перевірка підпису повідомлення. Вони повинні бути рівними.

Далі перейдемо до функцій:

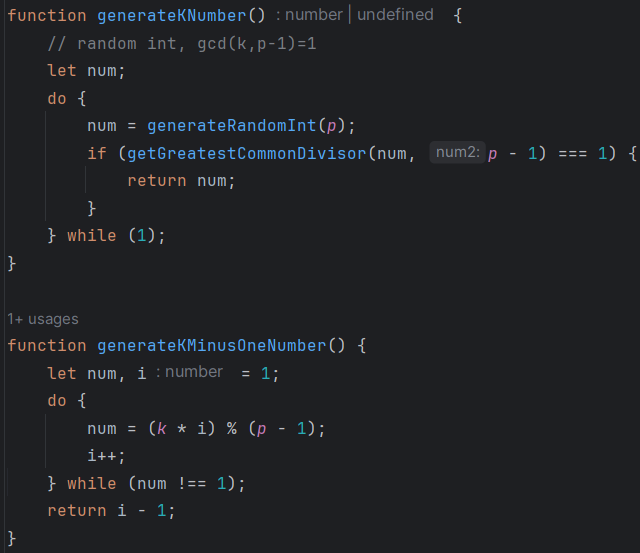




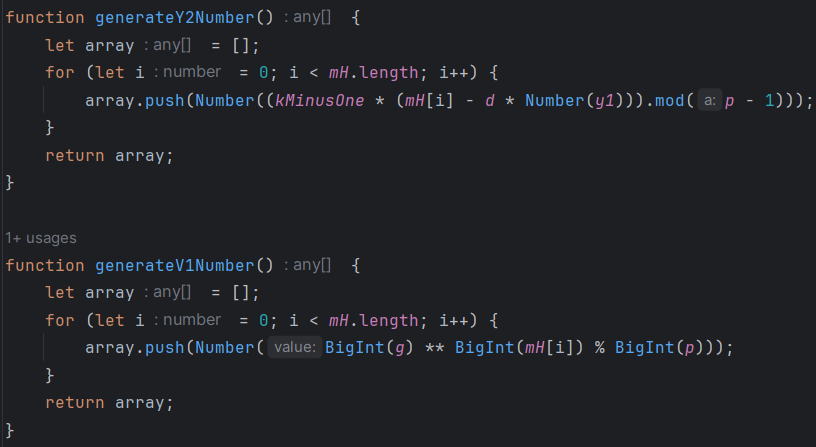
Дана функція забезпечує знаходження первісного кореня g за умовами завдання та власними налаштуваннями алгоритму.



Дані дві функції забезпечують створення чисел g та d згідно з умовами алгоритму. Як бачимо при генерації числа g використовуються додаткові умови, окрім знаходження самого первісного кореня.



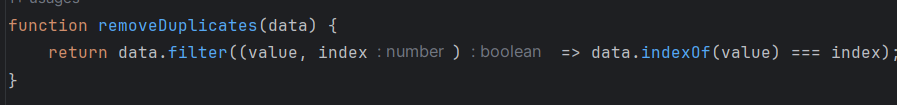
Дані функції забезпечують створення чисел k та оберненого до нього числа по модулю (p-1).



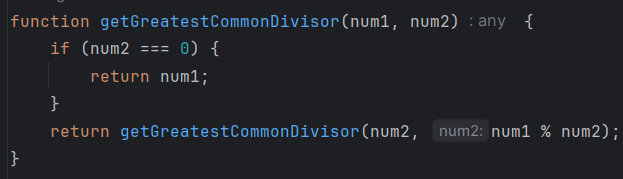
Дані функції займаються створенням чисел y1 та y2 для створення підпису.



Дані функції використовуються для створення чисел v1 та v2, з допомогою яких і буде перевірятися підпис.

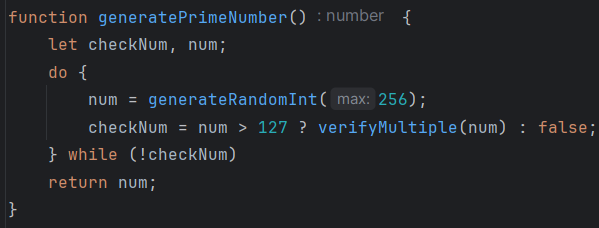


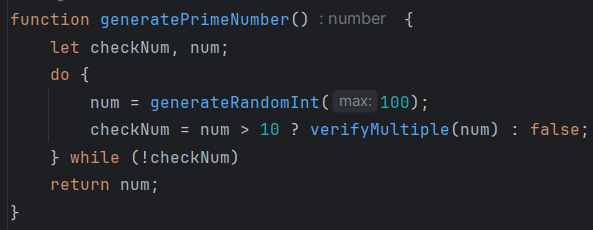
Дана функція є допоміжною і використовується для видалення повторених елементів масиву.



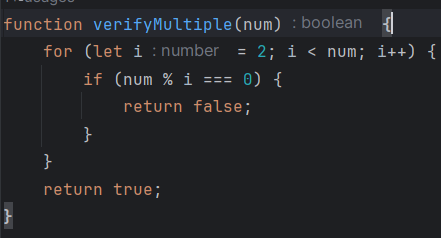
Дана функція також є допоміжною і повертає НСД двох чисел.

Додатково розберемо функції, які зустрічають в обох завданнях:

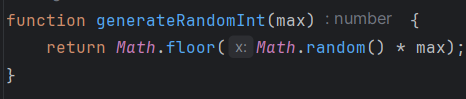




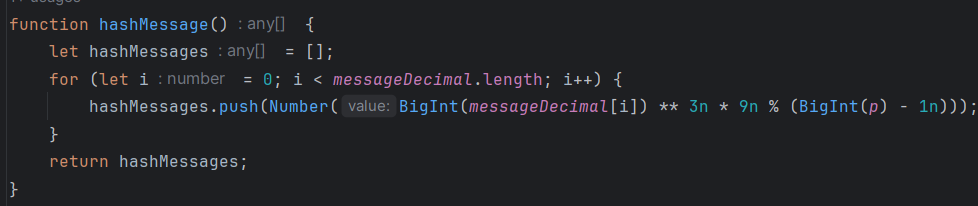
Одна й та ж функція з налаштуваннями для різних алгоритмів використовується для генерації простого числа.



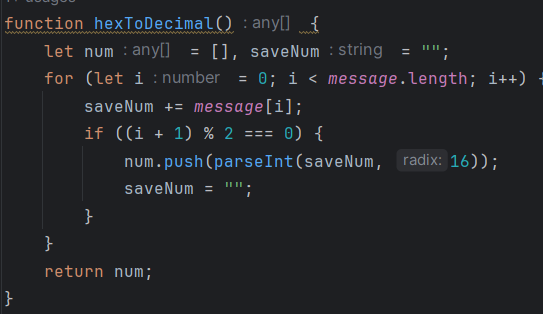
Дана функція додатково перевіряє чи число є простим.



Дана функція виконує генерацію числа в межах [1;max-1].

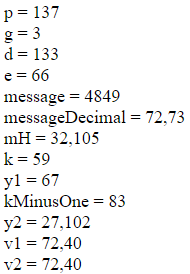
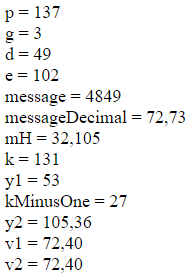
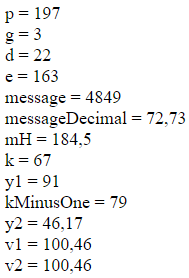


Дана функція виконує процес гешування відповідно до умов задачі.



Дана функція переводить число зі 16-го формату в 10-ий.

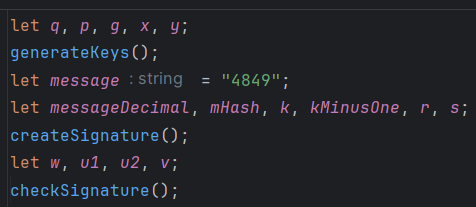
**Результати роботи першої програми:**

****

Одразу представляю кілька скриншотів, аби запевнити, що при різних випадкових значеннях підпис повідомлення успішно підтверджується.

**Хід роботи другого завдання**

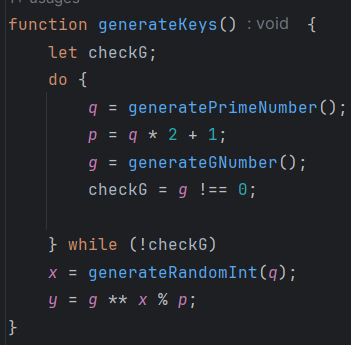
Код програми написаний мовою JS. Розглянемо основну роботу програми в третьому завданні (для мене воно друге – ЕЦП DSA):



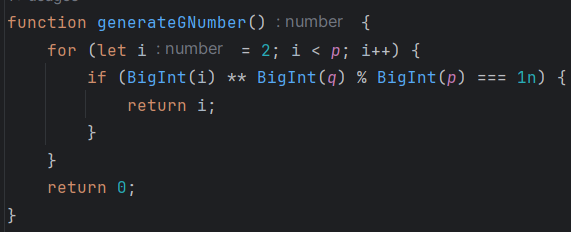
Розглянемо змінні:

* q та p – прості числа, з умовою, що q – дільник p – 1;
* g – первісний корінь за модулем p;
* x – довільне число в інтервалі 0<x<q;
* y – один з елементів відкритого ключа;
* message – повідомлення в 16-му форматі;
* messageDecimal – повідомлення, переведене у 10-ий формат;
* mHash – загешоване повідомлення;
* k та kMinusOne – обернені за модулем повідомлення;
* r та s – підпис повідомлення;
* w, u1, u2 та v – змінні, необхідні для перевірки підпису. Якщо v та r рівні, то підпис вважається дійсним.

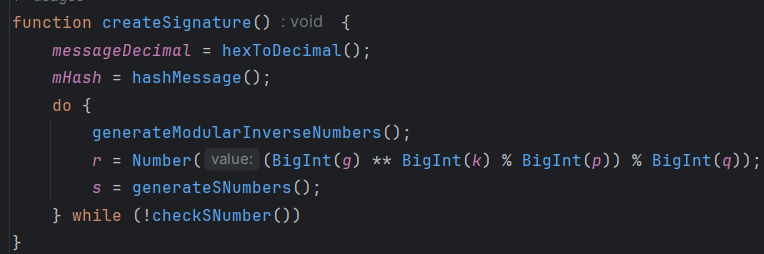
Тепер розглянемо детальніше функції програми:



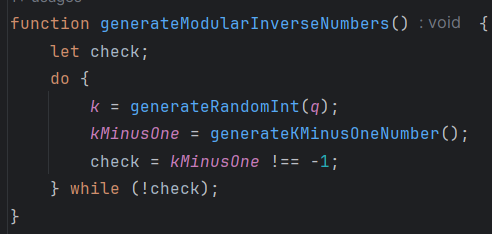
Дана функція забезпечує генерацію ключів із заданими умовами, при яких g не повинен дорівнювати нулю.



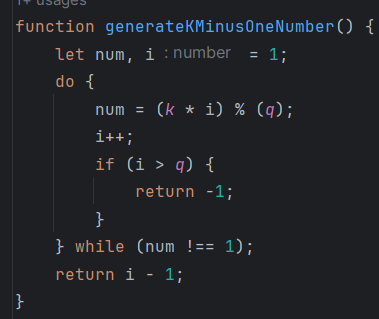
Дана функція генерує первісний корінь g.



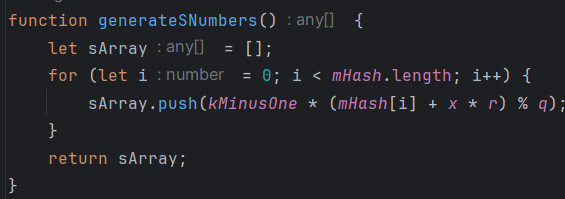
Дана функція займається створенням підпису.



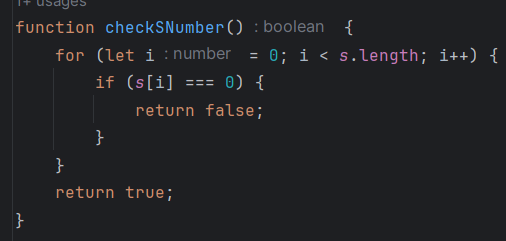
Дана функція генерує обернені по модулю числа.



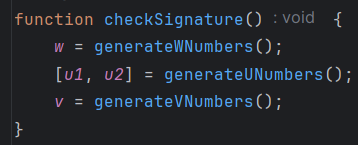
Дана функція спрямована на створення конкретно числа kMinusOne.



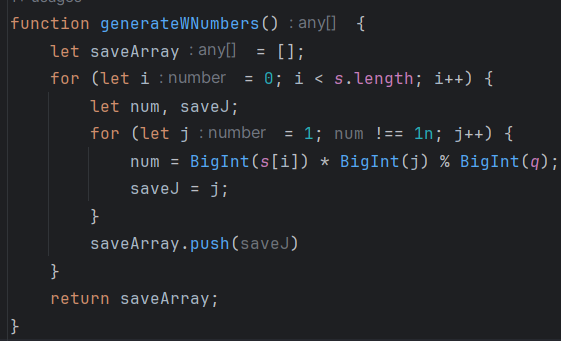
Дана функція займається генерування чисел s.



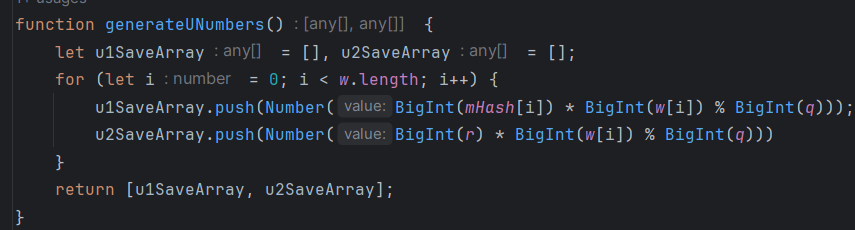
Дана функція перевіряє чи є хоч один із елементів масиву s рівним нулю.



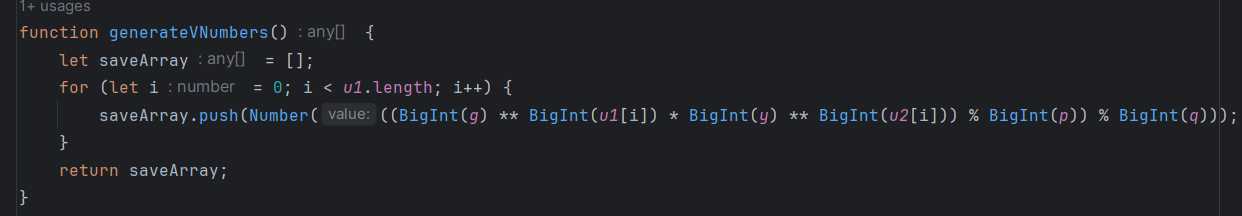
Дана функція перевіряє, чи є підпис валідним.



Дана функція створює числа w.

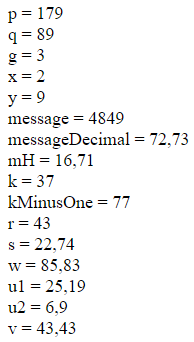
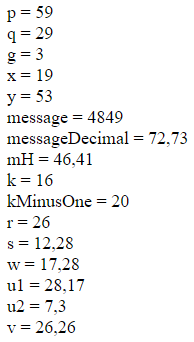
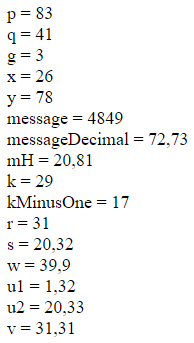


Дана функція створює числа u1 та u2.



Дана функція створює числа v, які необхідні для перевірки підпису.

**Результати роботи першої програми:**

****

Одразу представляю кілька скриншотів, аби запевнити, що при різних випадкових значеннях підпис повідомлення успішно підтверджується (r=v).

**Висновок:** На цій лабораторній роботі я вивчив застосування криптосистем з відкритим ключем до схем електронного цифрового підпису.