Лабораторна робота №4

Виконав: Ваврикович Михайло ПМІ-33

Тема: Шифрування з відкритим ключем на основі задачі рюкзак

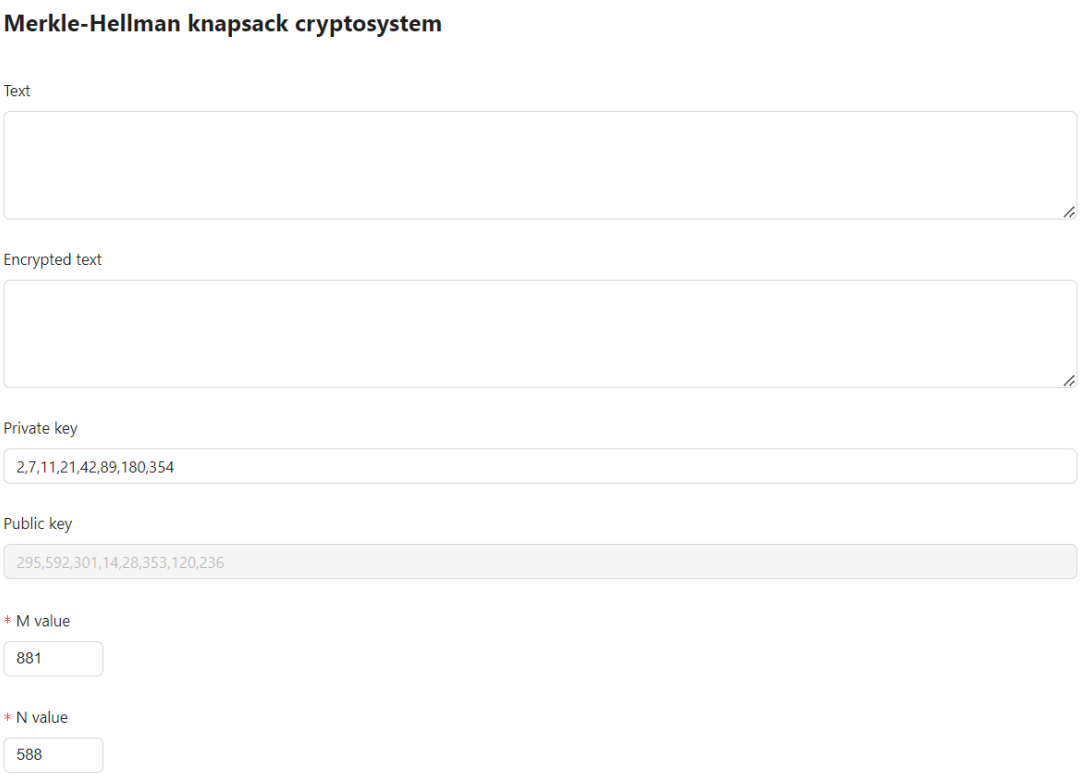
Мета: Ознайомитись з принципами побудови асиметричних криптосистемБазові відомості

Хід роботи

1. Відшукав в Інтернет-ресурсах чисельний приклад з використання алгоритму рюкзака та опрацював його.

   Посилання на ресурс

2. Розробив інтерфейс криптографічної системи для шифрування з використанням задачі рюкзака, передбачивши окремий діалог для формування відкритого ключа.

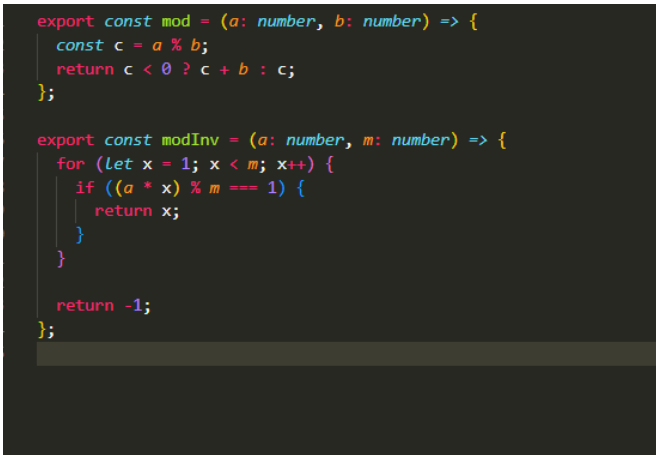


3. Розробив методи, які б забезпечували:
    a. Генерацію пари “Відкритий-закритий” ключі.
    b. Шифрування з використання відкритого ключа.
    c. Розшифрування з використанням закритого ключа.

```
export default {
  encode: (byteCode: string, publicKey: number[]) => {
    const byteCodeChunks = chunk<string>(byteCode.split(''), publicKey.length);

    return byteCodeChunks.map((item) =>
      item.reduce((sum, num, i) => sum + +num * publicKey[mod(i, publicKey.length)], 0),
    );
  },

  decode: (sums: number[], mValue: number, nValue: number, privateKey: number[]) => {
    const sValue = modInv(nValue, mValue);

    const start = Date.now();

    return sums.map((sum) => {
      let divValue = mod(sum * sValue, mValue);
      const values = [];

      while (divValue > 0) {
        if (Date.now() > start + 1000 * 2 || values.length > 100) {
          break;
        }

        for (let i = privateKey.length - 1; i >= 0; i--) {
          if (privateKey[i] > divValue) {
            values.unshift(0);
            continue;
          }

          values.unshift(1);
          divValue -= privateKey[i];
        }
      }

      return values.join('');
    });
  },
};
```

4. Перевірив правильність роботи системи на основі використання даних з чисельного прикладу.
5. Виконав додаткові завдання
    a. Ознайомився з можливостями он-лайн калькулятора для знаходження взаємно обернених чисел, використав його оберненого t за відомим t і перевірив правильність функціонування системи в загальному випадку.
    b. Ознайомився з розширеним алгоритмом Евкліда для знаходження взаємно обернених чисел і модифікував створений програмний код,

додавши метод з реалізацією цього алгоритму і використання його для знаходження оберненого t за відомим t і m.



```
export const mod = (a: number, b: number) => {
  const c = a % b;
  return c < 0 ? c + b : c;
};

export const modInv = (a: number, m: number) => {
  for (let x = 1; x < m; x++) {
    if ((a * x) % m === 1) {
      return x;
    }
  }

  return -1;
};
```

Висновок: я розробив криптосистему на основі задачі про рюкзак.