Лабораторна робота №5

Виконав: Вавринович Михайло ПМІ-33

Тема: Шифрування з відкритим ключем

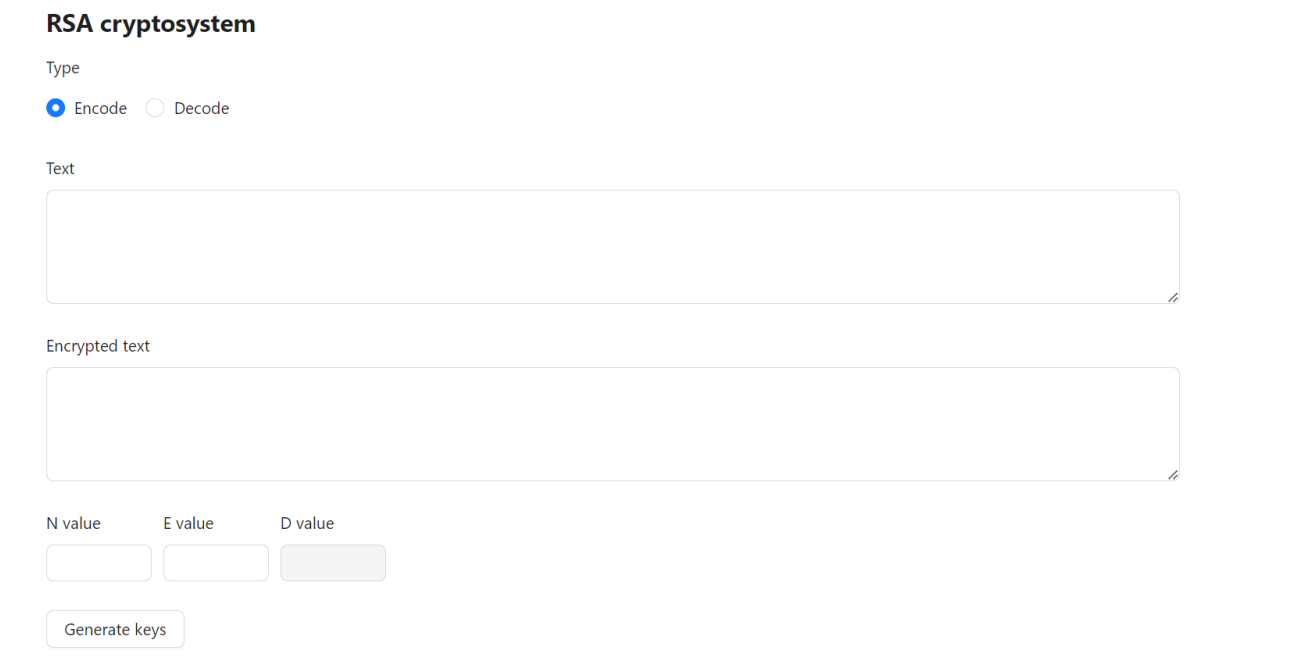
Мета: Реалізувати криптосистему RSA з використанням бінарного алгоритму піднесення до степеня за модулем

Хід роботи

1. Відшукав в Інтернет-ресурсах чисельний приклад з використання бінарного алгоритму піднесення до степеня за модулем та опрацював його.

   Посилання на ресурс

2. Розробив інтерфейс криптографічної системи RSA для шифрування з використанням бінарного алгоритму піднесення до степеня за модулем, передбачивши окремий діалог для формування відкритого ключа.



3. Розробіть методи, які б забезпечували:
    a. Генерацію пари «відкритий –закритий» ключі.
    b. Шифрування з використанням відкритого ключа.
    c. Розшифрування з використанням закритого ключа.

```
const getE = (phiN: number) => {
  let e = getRandomNumber(2, phiN);
  while (!isCoprime(e, phiN)) {
    e = getRandomNumber(2, phiN);
  }
  return e;
};

export default {
  encode: (text: string, n: number, e: number) => {
    const encryptedMessage = [];
    for (let i = 0; i < text.length; i++) {
      const encryptedCharCode = modPow(text.charCodeAt(i), e, n);
      encryptedMessage.push(encryptedCharCode);
    }
    return encryptedMessage;
  },

  decode: (cipher: number[], n: number, d: number) => {
    let decryptedMessage = '';
    for (let i = 0; i < cipher.length; i++) {
      const decryptedCharCode = modPow(cipher[i], d, n);
      decryptedMessage += String.fromCharCode(decryptedCharCode);
    }
    return decryptedMessage;
  },

  getKeys: () => {
    const p = getRandomPrimeNumber();
    const q = getRandomPrimeNumber();
    const n = p * q;
    const phiN = lcm(p - 1, q - 1);
    const e = getE(phiN);
    const d = modInv(e, phiN);

    return {
      publicKey: {
        n,
        e,
      },
      privateKey: {
        n,
        d,
```

4. Перевірив правильність роботи системи на основі використання даних з чисельного прикладу.

Висновок: я реалізував криптосистему RSA з використанням бінарного алгоритму піднесення до степеня за модулем.