

Лабораторна робота 2

Симетричне шифрування. Алгоритм AES

Мета

Дослідити принципи роботи симетричного шифрування на прикладі алгоритму AES.

Завдання

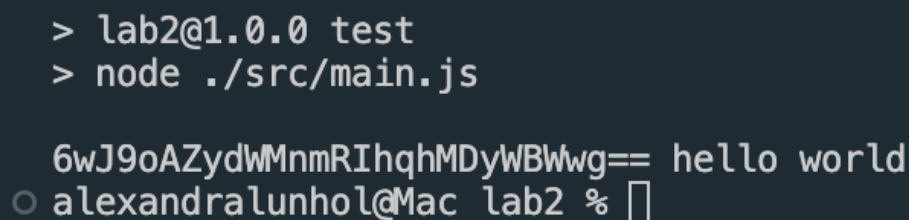
Реалізувати алгоритм симетричного шифрування AES (будь-якої версії - 128 або 256).

Довести коректність роботи реалізованого алгоритму шляхом порівняння результатів з існуючими реалізаціями (напр. сайтом-утилітою <https://cryptii.com>).

Так як коду дуже багато покажу тільки виклик

```
import AesCtr from './aesCtr.js';  
  
const password = 'qwertyuiopasdfghjklzxcvbnmqwerty';  
const plaintext = 'hello world';  
const ciphertext = AesCtr.encrypt(plaintext, password, 256);  
const origtext = AesCtr.decrypt(ciphertext, password, 256);  
console.log(ciphertext, origtext);
```

В результаті маємо



```
> lab2@1.0.0 test  
> node ./src/main.js  
  
6wJ9oAZydWMnmRIhqmDyWBWwg== hello world  
alexandralunhol@Mac lab2 %
```

Висновок

На жаль мій результат роботи програми не співпав з результатом онлайн AES , але працює)