Міністерство освіти і науки України

Національний університет «Львівська політехніка»

Інститут комп'ютених наук та інформаційних технологій

Кафедра «Системи штучного інтелекту»

Лабораторна робота №4

з курсу "Технології захисту інформації"

Виконала:

студентка групи КН-308

Ріжко Марія

Перевірив:

Яковина В.С.

Львів 2020 р.

Тема роботи

Створення програмної реалізації алгоритму шифрування з відкритим ключем RSA з використанням Microsoft CryptoAPI

Завдання

З використання функцій CryptoAPI створити програмну реалізацію алгоритму шифрування RSA. Оцінити швидкість шифрування алгоритму RSA та порівняти її зі швидкістю шифрування алгоритму RC5, реалізованого в роботі № 3, зробити відповідні висновки та відобразити їх у звіті до лабораторної роботи.

Програмна реалізація

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
from time import time
from lab3.code import RC5

path = 'lab4//'


# create keys
def create_keys():
    print('Create keys')
    private_key = RSA.generate(4096)
    public_key = private_key.publickey()
    print('Your pair of keys:')
    print(private_key.exportKey(format='PEM'))
    print(public_key.exportKey(format='PEM'))
    return private_key, public_key


# save keys
def save_keys(private_key, public_key, username):
    with open(path + username + '_private' + '.pem', 'wb') as f:
        f.write(private_key.exportKey('PEM'))
    with open(path + username + '_public' + '.pem', 'wb') as f:
        f.write(public_key.exportKey('PEM'))
    print(f'Keys for {username} are saved!\n')


# encrypt message
def encrypt_message(message, receiver, file_name):
    with open(path + receiver + '_public.pem', 'rb') as key_file:
        key = RSA.importKey(key_file.read())

    with open(path + file_name + '_' + receiver + '.txt', 'wb') as
message_file:
        cipher = PKCS1_OAEP.new(key)
```

```
                encrypted_message = cipher.encrypt(bytes(message,
encoding='utf-8'))
            message_file.write(encrypted_message)

        print('Message is encrypted!')


    # decrypt message
    def decrypt_message(file_name, username):
        with open(path + file_name + '.txt', 'rb') as f:
            data = f.read()

        with open(path + username + '_private.pem', 'rb') as f:
            key = RSA.importKey(f.read())

        cipher = PKCS1_OAEP.new(key)
        message = cipher.decrypt(data)

        print('Message is decrypted!')
        return message.decode()


    # create and save keys for users: user1 and user2
    private_key, public_key = create_keys()
    save_keys(private_key, public_key, 'user1')
    private_key, public_key = create_keys()
    save_keys(private_key, public_key, 'user2')

    # send message from user1 to user2
    encrypt_message('This is first message from user1 to user2', 'user2',
'msg1')
    encrypt_message('This is second message from user1 to user2', 'user2',
'msg2')

    # send message from user2 to user1
    encrypt_message('This is first message from user2 to user1', 'user1',
'msg1')

    # read messages
    print(decrypt_message('msg1_user2', 'user2'))
    print(decrypt_message('msg2_user2', 'user2'))
    print(decrypt_message('msg1_user1', 'user1'))

    # try ro read with wrong user key
    try:
        print(decrypt_message('msg1_user2', 'user1'))
    except ValueError:
        print('Incorrect decryption.')

    # compare time
    with open(path + 'test.txt', 'r') as f:
        message = f.read()
        start = time()
        encrypt_message(message, 'user1', 'msg2')
        rsa_enc_time = time() - start
        print('Rsa encryption time:', rsa_enc_time)

    key = 'qwerty12'
    start = time()
    cipher = RC5(16, 16, key.encode())
    cipher.encrypt_file(path + 'test.txt', path + 'res.txt')
    rc5_enc_time = time() - start
    print('Rc5 encryption time:', rc5_enc_time)
```

Результати виконання

```
Create keys
Your pair of keys:
b'-----BEGIN RSA PRIVATE KEY-----\nMIIJKAIBAAKCAgEAkiS/uypYUhxPZEB2LpiTNXxqKoe77QxLGENR3hOHG7juVUQy\nMx+RNO08lMWH584ZH/GHYrSzHo7gBWsz5KwAlz/h8daCtFeDXyKjRlEpsJ5IVwkX\nd2TzMRtuQAM
b'-----BEGIN PUBLIC KEY-----\nMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAkiS/uypYUhxPZEB2LpiT\nNXxqKoe77QxLGENR3hOHG7juVUQyMx+RNO08lMWH584ZH/GHYrSzHo7gBWsz5KwA\nlz/h8daCtFeDXyKj
Keys for user1 are saved!

Create keys
Your pair of keys:
b'-----BEGIN RSA PRIVATE KEY-----\nMIIJJwIBAAKCAgEAmGB17rBFbefWqmSsBBz3lx4vMBUtv8VrmCLtyQWVczeBCvkq\ndtAbWpg7oIzpMw1wFw946EYUMwZSd7r76RSrit5Z88qKS0Pg33wvyxsHemgmFGIo\nw0eln6UtIfG
b'-----BEGIN PUBLIC KEY-----\nMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAmGB17rBFbefWqmSsBBz3\nlx4vMBUtv8VrmCLtyQWVczeBCvkqdtAbWpg7oIzpMw1wFw946EYUMwZSd7r76RSr\nit5Z88qKS0Pg33wv
Keys for user2 are saved!

Message is encrypted!
Message is encrypted!
Message is encrypted!
Message is decrypted!
This is first message from user1 to user2
Message is decrypted!
This is second message from user1 to user2
Message is decrypted!
This is first message from user2 to user1
Incorrect decryption.
Message is encrypted!
Rsa encryption time: 0.003949403762817383
Rc5 encryption time: 0.0020040863037109375

Process finished with exit code 0
```

Висновок

На лабораторній роботі я створила програмну реалізацію алгоритму шифрування з відкритим ключем RSA з використанням Microsoft CryptoAPI.

.