Белорусский государственный университет информатики и радиоэлектроники

Кафедра информатики

Лабораторная работа № 6

Цифровая подпись

Выполнила студент гр. 653502: Серебренников В. А.

Проверил ассистент КИ: Артемьев В. С.

Минск, 2019

Введение

Электронно-цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронно-цифровая подпись - это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

Преимущества использования электронно-цифровой подписи:

- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;
- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;
- гарантировать достоверность документации;
- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;
- построить корпоративную систему обмена документами.

В рамках лабораторной работы необходимо реализовать программные средства проверки ЭЦП на базе алгоритма ГОСТ 3410.

Блок-схема алгоритма

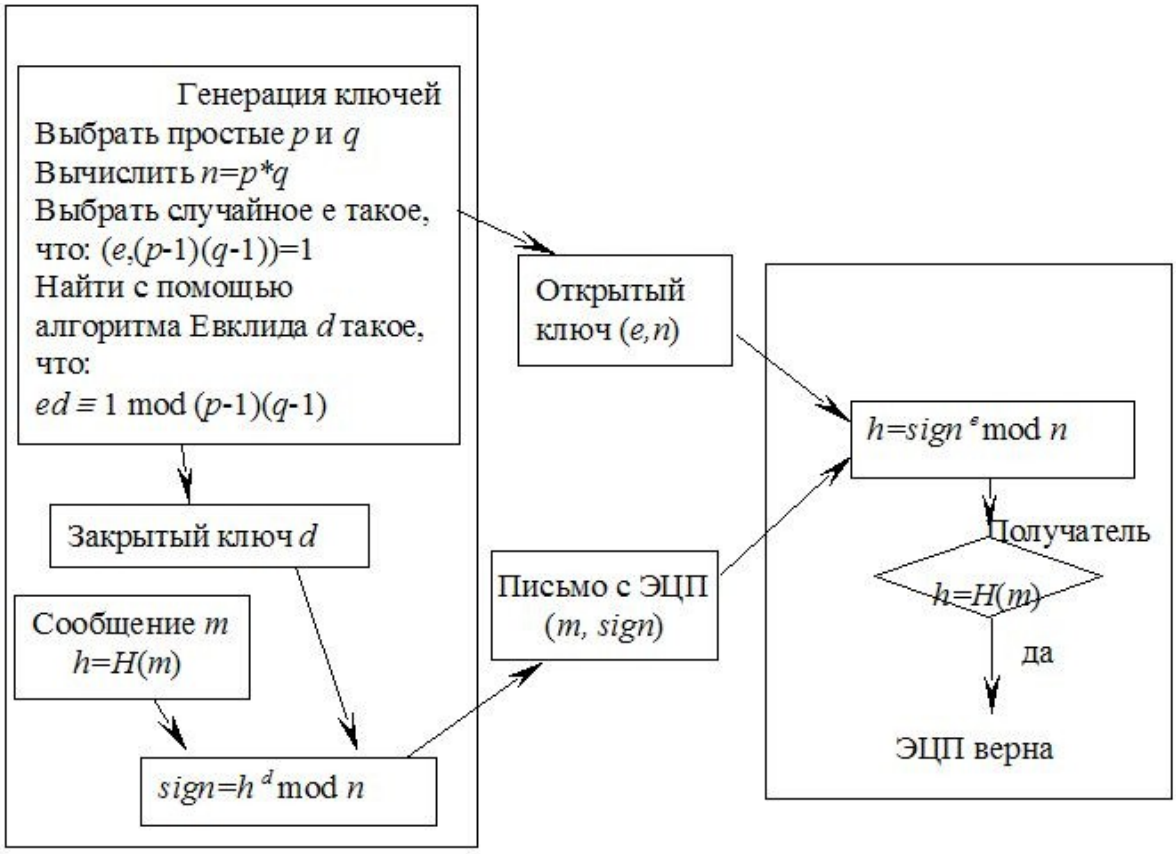

Рис.4.1. Схема ЭЦП на основе алгоритма RSA

Пример работы программы

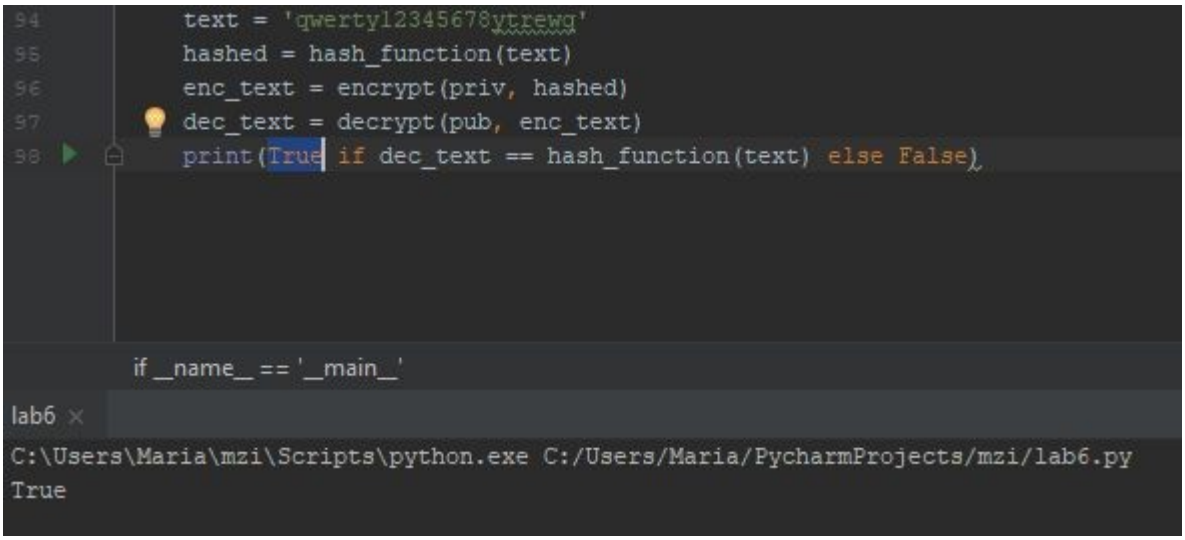

Рис.2. Пример работы

Код программы

```
import random
from hashlib import sha256


def make_key_pair(length):
    start = 1 << (length // 2 - 1)
    stop = 1 << (length // 2 + 1)

    if start >= stop:
        return []
    primes = [2]
    for n in range(3, stop + 1, 2):
        for p in primes:
            if n % p == 0:
                break
        else:
            primes.append(n)

    while primes and primes[0] < start:
        del primes[0]

    n_min = 1 << (length - 1)
    n_max = (1 << length) - 1
    while primes:
        p = random.choice(primes)
        primes.remove(p)
        q_candidates = [q for q in primes
                        if n_min <= p * q <= n_max]
        if q_candidates:
            q = random.choice(q_candidates)
            break
    return p, q


def co_prime(a, b):
    while b != 0:
        a, b = b, a % b
    return a


def mod_inv(aa, bb):
    remainder0, remainder = abs(aa), abs(bb)
    x, lastx = 0, 1
    while remainder:
        remainder0, (quotient, remainder) = remainder, divmod(remainder0, remainder)
        x, lastx = lastx - quotient * x, x
    return lastx * (-1 if aa < 0 else 1) % bb


def is_prime(num):
    if num == 2:
        return True
```

```
    if num < 2 or num % 2 == 0:
        return False
    for n in range(3, int(num ** 0.5) + 2, 2):
        if num % n == 0:
            return False
    return True


def generate_key_pair(p, q):
    n = p * q
    phi = (p - 1) * (q - 1)
    e = random.randrange(1, phi)
    g = co_prime(e, phi)

    while g != 1:
        e = random.randrange(1, phi)
        g = co_prime(e, phi)

    d = mod_inv(e, phi)
    return (e, n), (d, n)


def encrypt(private_key, plain_text):
    key, n = private_key
    return [pow(ord(char), key, n) for char in plain_text]


def decrypt(public_key, cipher_text):
    key, n = public_key
    plain = [chr(pow(char, key, n)) for char in cipher_text]
    return ''.join(plain)


def hash_function(message):
    return sha256(message.encode("UTF-8")).hexdigest()


if __name__ == '__main__':
    pub, priv = make_key_pair(10)
    pub, priv = generate_key_pair(pub, priv)

    text = 'qwerty12345678ytrewq'
    hashed = hash_function(text)
    enc_text = encrypt(priv, hashed)
    dec_text = decrypt(pub, enc_text)
    answer = True if dec_text == hash_function(text) else False
    print(answer)
```

Вывод

Свойства электронной цифровой подписи позволяют использовать её в следующих основных целях электронной экономики и электронного документального и денежного обращения:

- Использование в банковских платежных системах.
- Электронная коммерция (торговля).
- Электронная регистрация сделок по объектам недвижимости.
- Применение ЭЦП в различных расчетных и трейдинговых системах, а также Forex.
- Управление акционерным капиталом и долевым участием.
- ЭП является одним из ключевых компонентов сделок в криптовалютах.

В ходе написания лабораторной работы были изучен алгоритм ГОСТ 3410, а также написана программная реализация проверки ЭЦП с его помощью.