Навчально-науковий інститут інформаційних технологій
Харківський національний економічний університет
імені Семена Кузнеця

Звіт
З Виконання лабораторної роботи №6
за дисципліною: “ Безпека банківських систем ”
на тему: “ВИВЧЕННЯ ЗАХИСТУ ПОВІДОМЛЕНЬ В ПРОТОКОЛІ SET”

Виконав: студент кафедри
Кібербезпеки та інформаційних
технологій
4 курсу, спец. Кібербезпека,
групи 6.04.125.010.21.2
Бойко Вадим Віталійович
Перевірив:
Лимаренко Вячеслав Володимирович

ХНЕУ ім. С. Кузнеця
2024

Мета: ознайомитися з принципами роботи протоколу SET (Secure Electronic Transaction).

Завдання:

1. Виконати дослідження методів шифрування, що використані в протоколі SET (DES та RSA).
2. Розробити програму шифрування повідомлень з використанням або симетричного алгоритму DES, або за допомогою несиметричного алгоритму RSA.
3. В якості мови програмування використати будь-яку мову на ваш вибір.
4. Навести вихідний код програми.
5. Разом зі звітом надати скомпільовану програму у архіві.

Контрольні питання:

1. Що таке протокол SET?
2. Для чого використовується протокол SET?
3. Які засоби шифрування в ньому використовуються?
4. Чим гарантується цілісність даних в протоколі SET?
5. За рахунок чого відбувається автентифікація рахунка власника карти в протоколі SET?

Хід роботи:

Виконаю дослідження методів шифрування, що використані в протоколі SET (DES та RSA).

Протокол DES (Data Encryption Standard)

Історія створення та розвитку:

- Розробка: Був розроблений компанією IBM на початку 1970-х років і прийнятий урядом США як офіційний стандарт шифрування у 1977 році.
- Критика та модифікації: З самого початку DES піддавався критиці через відносно невелику довжину ключа (56 біт), що робило його потенційно вразливим до грубої сили. У відповідь на цю критику були розроблені різні модифікації DES, такі як Triple DES, який використовував три послідовні застосування алгоритму DES з різними ключами.
- Застарівання: З розвитком обчислювальної техніки та появою більш потужних комп'ютерів, DES поступово став недостатньо безпечним для захисту конфіденційної інформації.

Принцип роботи:

- Блочний шифр: DES є блоковим шифром, тобто він шифрує дані фіксованими блоками по 64 біти.
- Ключ: Довжина ключа DES становить 56 біт.
- Структура: Алгоритм використовує мережу Фейстеля, яка складається з 16 раундів перетворень.
- Слабкі ключі: У DES існують так звані слабкі ключі, які надають менший рівень безпеки.

Застосування:

- Раніше широко використовувався для захисту даних у різних сферах, включаючи фінанси, уряд і військову справу.
- Сьогодні: Вважається застарілим і рекомендується використовувати більш сучасні алгоритми шифрування.

Протокол RSA (Rivest–Shamir–Adleman)

Історія створення та розвитку:

- Розробка: Був розроблений в 1977 році Рональдом Рівестом, Аді Шаміром і Леном Адлеманом.
- Широке застосування: RSA швидко став одним з найпопулярніших алгоритмів асиметричної криптографії завдяки своїй простоті та ефективності.
- Постійна актуальність: Незважаючи на появу нових алгоритмів, RSA залишається одним з найбільш широко використовуваних алгоритмів для шифрування та створення цифрових підписів.

Принцип роботи:

- Асиметрична криптографія: RSA використовує пару ключів: публічний і приватний. Публічний ключ використовується для шифрування даних, а приватний – для дешифрування.
- Математична основа: Безпека RSA заснована на складності факторизації великих цілих чисел.
- Застосування: RSA використовується для шифрування даних, створення цифрових підписів, а також для обміну ключами в гібридних криптосистемах.

Застосування:

- Широке застосування: RSA використовується в багатьох сферах, включаючи електронну комерцію, електронну пошту, цифрові сертифікати та інші системи, що вимагають високого рівня безпеки.

Порівняння DES та RSA

Характеристика	**DES**	**RSA**
Тип	Симетричний	Асиметричний
Довжина ключа	56 біт (застарілий)	Змінна, зазвичай 2048 біт і більше
Швидкість	Швидкий	Повільніший, ніж симетричні алгоритми
Застосування	Шифрування даних	Шифрування, цифрові підписи, обмін ключами
Безпека	Вважається застарілим	Більш безпечний, але схильний до атак при використанні коротких ключів

Напишу код, перед початком роботи встановлю бібліотеку

```
pip install pycryptodome
```

Код має наступний вигляд

```python
from Crypto.Cipher import DES
from Crypto.Util.Padding import pad, unpad
from Crypto.Random import get_random_bytes

def encrypt_des(key, data):
    cipher = DES.new(key, DES.MODE_ECB)
    padded_data = pad(data, DES.block_size)
    ciphertext = cipher.encrypt(padded_data)
    return ciphertext

def decrypt_des(key, ciphertext):
    cipher = DES.new(key, DES.MODE_ECB)
    decrypted_data = cipher.decrypt(ciphertext)
    return unpad(decrypted_data, DES.block_size)

key = get_random_bytes(8)

data = b"SecretMsg"
print(f"Original data: {data}")

ciphertext = encrypt_des(key, data)
print(f"Encrypted data: {ciphertext}")

decrypted_data = decrypt_des(key, ciphertext)
print(f"Decrypted data: {decrypted_data}")
```

Й перевірю виконання

```
C:\Users\vadim\Desktop\bbs>python des.py
Original data: b'SecretMsg'
Encrypted data: b'>S\xc4d\x04\x07\tA\x03\x18\xcfv\x9f\r :'
Decrypted data: b'SecretMsg'
```

Й як можна побачити програма працює

Відповіді на контрольні запитання:

1. Що таке протокол SET?

   SET (Secure Electronic Transaction) – це стандартизований протокол, розроблений для забезпечення безпечних електронних платежів за допомогою кредитних або дебетових карток. Він був створений консорціумом компаній, включаючи Visa, Mastercard, Microsoft та інші, з метою забезпечення високого рівня безпеки при здійсненні онлайн-платежів.

2. Для чого використовується протокол SET?

   Протокол SET призначений для вирішення проблем безпеки, пов'язаних з електронними платежами, зокрема:

   a. Захист номерів кредитних карт: Завдяки шифруванню та використанню цифрових сертифікатів, номер кредитної картки не передається в чистому вигляді по незахищених мережах.
   b. Аутентифікація сторін: Протокол забезпечує взаємну аутентифікацію між покупцем, продавцем, банком-емітентом та банком-еквайром.
   c. Цілісність даних: Завдяки використанню криптографічних хеш-функцій, гарантується, що дані платежу не були підроблені під час передачі.

3. Які засоби шифрування в ньому використовуються?

   Протокол SET використовує асиметричну криптографію, яка базується на використанні пар ключів: публічного та приватного. Основні криптографічні алгоритми, що застосовуються в SET:

   a. RSA: Використовується для шифрування даних та створення цифрових підписів.
   b. DES: Симетричний алгоритм шифрування, який використовується для шифрування даних перед їх шифруванням алгоритмом RSA.
   c. MD5: Хеш-функція для створення цифрових відбитків даних.

4. Чим гарантується цілісність даних в протоколі SET?

   Цілісність даних в протоколі SET забезпечується за рахунок використання цифрових підписів та хеш-функцій.

   a. Цифрові підписи: Кожен учасник транзакції має свій цифровий сертифікат, який містить його публічний ключ. Перед відправкою повідомлення воно підписується приватним ключем відправника. Одержувач може перевірити підпис, використовуючи публічний ключ відправника. Це дозволяє переконатися в тому, що повідомлення не було підроблено.
   b. Хеш-функції: Перед підписанням повідомлення обчислюється його хеш. Цей хеш також підписується. Одержувач обчислює хеш отриманого повідомлення і порівнює його з хешем, що міститься в підписі. Якщо хеші збігаються, це означає, що повідомлення не було змінено під час передачі.

5. За рахунок чого відбувається автентифікація рахунка власника карти в протоколі SET?

   Автентифікація рахунка власника карти в протоколі SET відбувається за допомогою цифрових сертифікатів та PIN-коду.

   a. Цифрові сертифікати: Кожен учасник транзакції (власник карти, продавець, банк-емітент, банк-еквайр) має свій цифровий сертифікат, який підтверджує його ідентичність.
   b. PIN-код: Власник карти використовує свій PIN-код для підтвердження своєї особистості. Цей PIN-код зашифрований і передається в безпечному вигляді.