**Министерство науки и высшего образования РФ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»**

**(ВлГУ)**

УДК 004.8

Срок хранения 2 года

ВЛГУ.10.05.04.04.05.00 ПЗ

**ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ**

«**ЛР №2 - ПРОТОКОЛЫ СТРОГОЙ АУТЕНТИФИКАЦИИ С СИММЕТРИЧНЫМ АЛГОРИТМОМ ШИФРОВАНИЯ ИЛИ ХЭШ-ФУНКЦИЕЙ, ПРОТОКОЛ SKID 3**»

Специальность 10.05.04 – «Информационно-аналитические системы безопасности»

|  |  |  |
| --- | --- | --- |
| Руководитель |  | к.т.н. доцент кафедры ИЗИ Д. В. Мишин |
|  |
| Исполнитель |  | студент группы ИСБ-119 Д. А. Журавлёв |
|  |  |  |  |

Владимир 2023 г.

**ЛР №2 - Протоколы строгой аутентификации с симметричным алгоритмом шифрования или хэш-функцией, протокол SKID 3**

Изучить и реализовать протоколы строгой аутентификации с симметричным алгоритмом шифрования или хэш-функцией:

- Однонаправленная аутентификация по временной метке или случайном значении;

- Взаимная аутентификация с использованием двух случайно сгенерированных последовательностей;

**Алгоритм:**

SKID2 и SKID3 - это симметричные криптографические протоколы аутентификации, разработанные для проекта RACE RIPE. Они используют MAC[1] для обеспечения безопасности и предполагают, что Алиса и Боб используют общий секретный ключ, К. SKID2 позволяет Бобу доказать свою подлинность Алисе. Вот этот протокол:

(1)Алиса выбирает случайное число, RA. (Документами RIPE определяется 64-битовое число). Она посылает это число Бобу и своё имя А.

(2)Боб выбирает случайное число, RB. (Документами RIPE определяется 64-битовое число). Он посылает Алисе Rb, Hk(Ra, Rb, В) НK ‑ это MAC. (В документах RIPE предлагается функция RIPE-MAC). В - это имя Боба.

(3)Алиса рассчитывает HK(RA, RB, В) и сравнивает результат со значением, полученным от Боба. Если результаты совпадают, Алиса убеждается в том, что она соединилась именно с Бобом.

SKID3 обеспечивает совместную проверку подлинности Алисой и Бобом. Этапы (1) - (3) совпадают с протоколом SKID2, а затем выполняются следующие действия.

(4)Алиса посылает Бобу:

Hk(Rb, A) А - это имя Алисы.

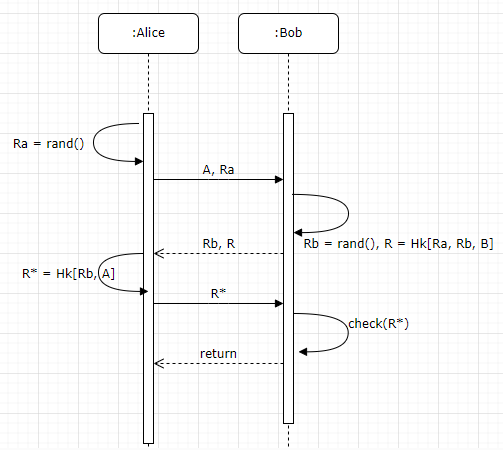
(5)Боб рассчитывает HK(RB, А) и сравнивает результат со значением, полученным от Алисы. Если результаты совпадают, Боб убеждается в том, что он соединился именно с Алисой.

Этот протокол неустойчив к вскрытию "человек-в-середине". В общем случае, вскрытие "человек-в-середине" может угрожать любому протоколу, в который не входит какой-нибудь секрет.

Когда Боб получает сообщение от Алисы, как ему узнать, что это сообщение подлинно? Если Алиса подписала свое сообщение, то все просто. Цифровая подпись Алисы достаточна, чтобы подтвердить кому угодно подлинность ее сообщения.

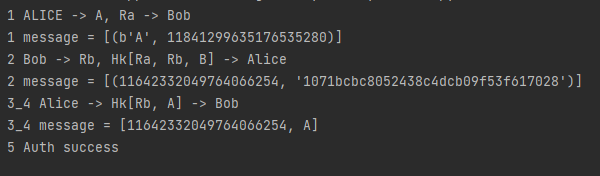
Некоторую проверку подлинности предоставляют и симметричные алгоритмы. Когда Боб получает сообщение от Алисы, шифрованное их общим ключом, он знает, что это сообщение от Алисы. Никто больше не знает их ключа. Однако, у Боба нет возможности убедить в этом кого-то еще. Боб не может показать сообщение Тренту и убедить его, что оно отправлено Алисой. Трент может сделать вывод, что сообщение отправлено или Алисой, или Бобом (так как их секретный ключ никому больше не принадлежит), но у него нет способа определить, кто же конкретно автор сообщения.

**Диаграмма последовательности:**

****

**Программа:**

Программа представляет из себя эмуляцию действий Alice и Bob при использовании протокола SKID 3.

****

**Вывод:**

В процессе работы был изучен протокол SKID 3, реализована программа эмулирующая работу данного протокола.

**Приложение:**

# (1)Алиса выбирает случайное число, RA. (Документами RIPE определяется 64-битовое число). Она посылает это число Бобу и своё имя А.

# (2)Боб выбирает случайное число, RB. (Документами RIPE определяется 64-битовое число). Он посылает Алисе

# Rb, Hk(Ra, Rb, В)

# НK ‑ это MAC. (В документах RIPE предлагается функция RIPE-MAC).

# (3)Алиса рассчитывает HK(RA, RB, В) и сравнивает результат со значением, полученным от Боба.

# (4)Алиса посылает Бобу: Hk(Rb, A)

# (5)Боб рассчитывает HK(RB, А) и сравнивает результат со значением, полученным от Алисы.

import hashlib

import uuid

AliceBD = {'key':b'XH2buFNIPF9VEZ17eqqTX95a\_fPn\_4BFYZTIqJYGpYI='}

BobBD = {'key':b'zzo52-ZqRWH8gyJe\_1KSiQKwOwxwp1d57L0N9zlt7cw='}

def f1():

nameA = b'A'

key\_Ra = uuid.uuid4().int & (1<<64)-1

AliceBD['Ra'] = key\_Ra

print(f'1 ALICE -> A, Ra -> Bob')

print(f'1 message = [{nameA, key\_Ra}]')

return nameA, key\_Ra

def f2(nameA, key\_Ra):

key\_Rb = uuid.uuid4().int & (1<<64)-1

BobBD['Rb'] = key\_Rb

hash\_ = hashlib.md5((key\_Ra).to\_bytes(64, 'big')+b'B'+(key\_Rb).to\_bytes(64, 'big'))

hash\_B = hash\_.hexdigest()

print(f'2 Bob -> Rb, Hk[Ra, Rb, B] -> Alice')

print(f'2 message = [{key\_Rb, hash\_B}]')

return key\_Rb, hash\_B

def f3\_4(key\_Rb, hash\_B):

hash\_ = hashlib.md5((AliceBD['Ra']).to\_bytes(64, 'big') + b'B' + (key\_Rb).to\_bytes(64, 'big'))

hash\_A = hash\_.hexdigest()

if hash\_B == hash\_A:

print(f'3\_4 Alice -> Hk[Rb, A] -> Bob')

print(f'3\_4 message = [{key\_Rb}, A]')

hash\_ = hashlib.md5(key\_Rb.to\_bytes(64, 'big')+b'A')

hash\_A = hash\_.hexdigest()

return hash\_A

def f5(hash\_A):

hash\_ = hashlib.md5((BobBD['Rb']).to\_bytes(64, 'big') + b'A')

hash\_B = hash\_.hexdigest()

if hash\_B == hash\_A:

print(f'5 Auth success')

# https://studopedia.su/3\_28205\_udostoverenie-podlinnosti-soobshcheniy.html

nameA, key\_Ra = f1()

key\_Rb, hash\_B = f2(nameA, key\_Ra)

hash\_A = f3\_4(key\_Rb, hash\_B)

f5(hash\_A)