РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

РЕФЕРАТ

ПО ТЕМЕ “Установление подлинности запрос-ответ”

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Пиняева Анна Андреевна

Группа: НПИмд-01-24

МОСКВА

2025

Актуальность

- Рост киберугроз: фишинг, MITM-атаки, утечки паролей.
- Модель Zero Trust требует строгой проверки подлинности.
- Проблема: Как доказать право на доступ, не раскрывая секрет?

Решение: Метод «Вызов-Ответ» (Challenge-Response).

Понятие аутентификации и её факторы

Аутентификация — подтверждение того, что субъект является тем, за кого себя выдает.

Три фактора аутентификации:

- Фактор знания — “что пользователь знает”
- Фактор владения — “что у пользователя есть”
- Биометрический фактор — “кем является пользователь”

Метод «вызов–ответ». Историческая справка

1970-е – первые идеи

1980-е – стандартизация и первые реализации

1990-е – переход к публичным ключам

2000-е – борьба с фишингом и массовое внедрение

2010-е – рождение современных безпарольных стандартов

2020-е – глобальный переход на Passkeys

Метод «вызов–ответ». Базовый принцип

Рис.1 Общая схема метода “вызов-ответ”

Метод «вызов–ответ». Использование шифра с симметричным ключом

Секретность здесь - открытый ключ засекречивания, известный и претендент у и верификатору. Функция - алгоритм шифрования, с помощью которого обрабатывается вызов перед посылкой ответа.

Подход 1.

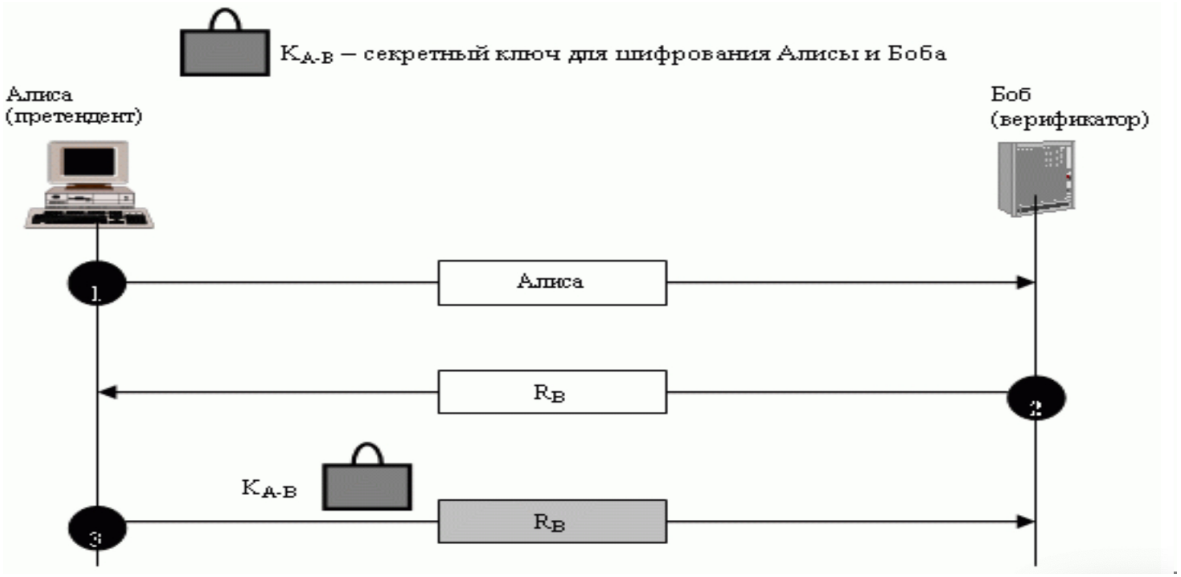

Рис.2 Принцип первого подхода

Подход 2.

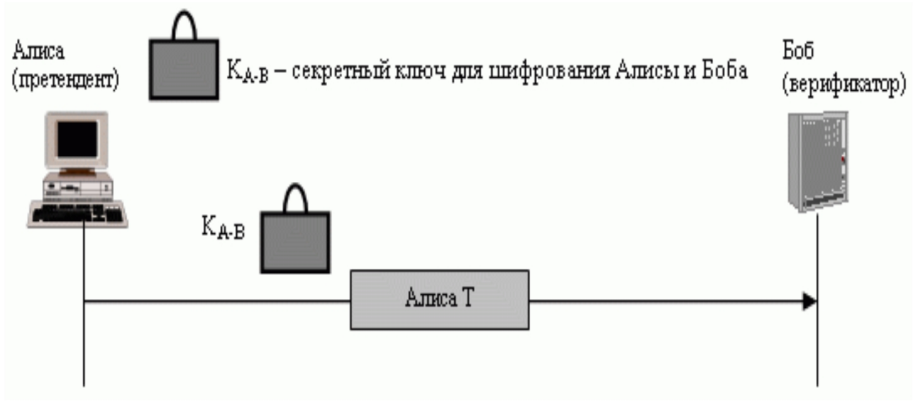

Рис.3 Принцип второго подхода

Подход 3.

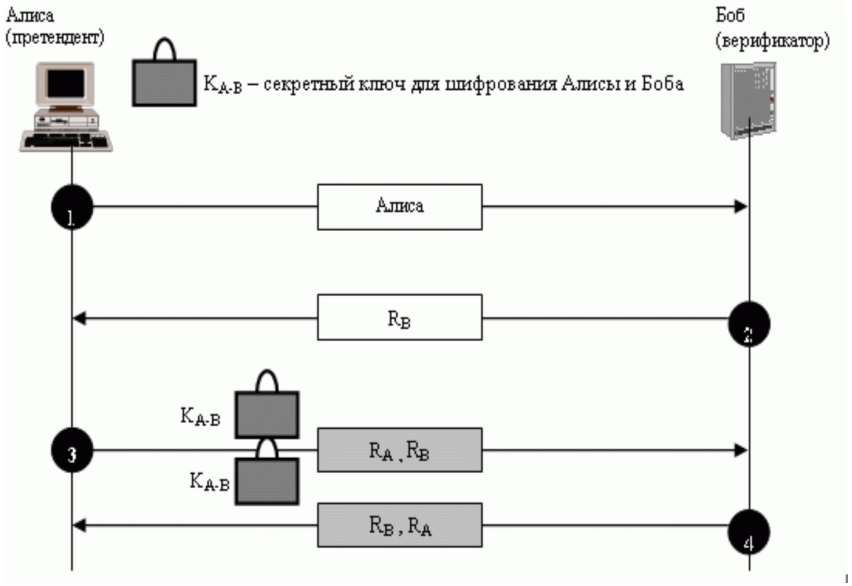

Рис.4 Принцип третьего подхода

Метод «вызов–ответ». Использование функций ключевого хэширования

Такой подход обладает важным преимуществом: он обеспечивает не только проверку подлинности, но и контроль целостности сообщений, поскольку результат вычисления MAC зависит как от данных, так и от секретного ключа.

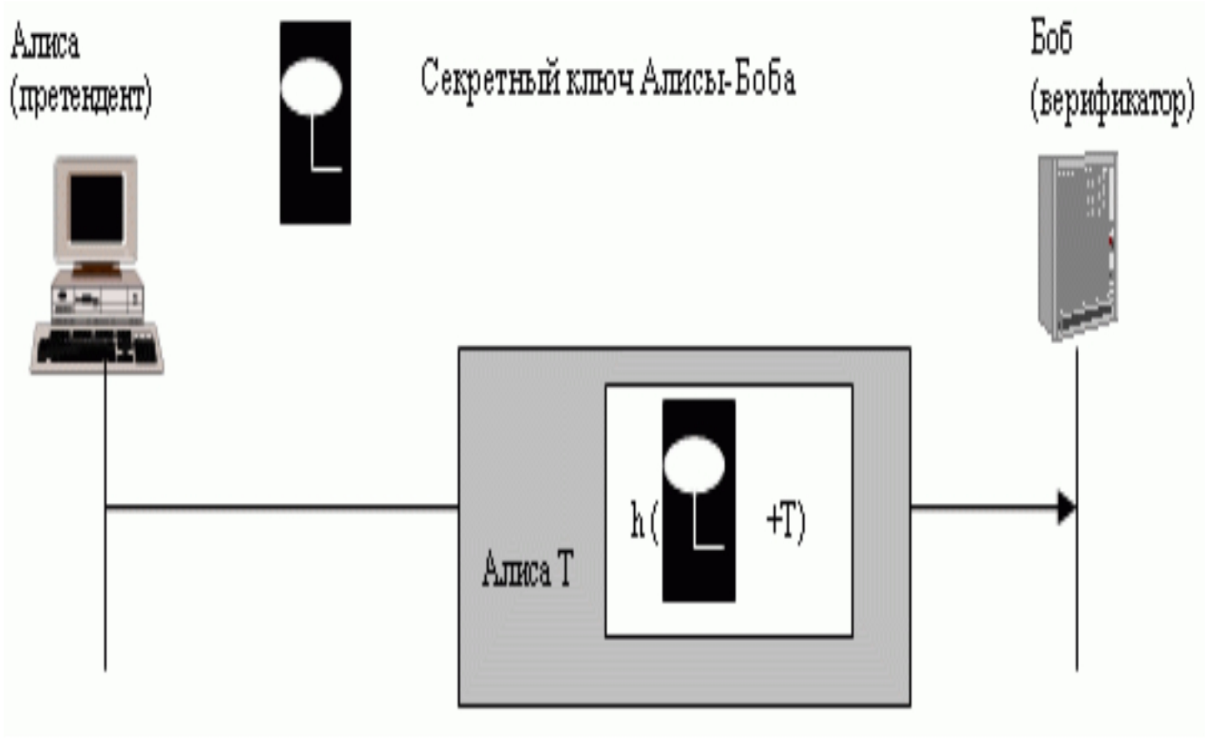

Рис.5 Схема формирования ответа на вызов

Метод «вызов–ответ». Использование цифровой подписи

В этом случае секретом является закрытый ключ претендента, а его открытый ключ доступен верификатору и может быть опубликован. Задача претендента — доказать владение закрытым ключом, соответствующим известному открытому ключу.

Подход 1.

Рис.2.8 Схема первого подхода

Подход 2.

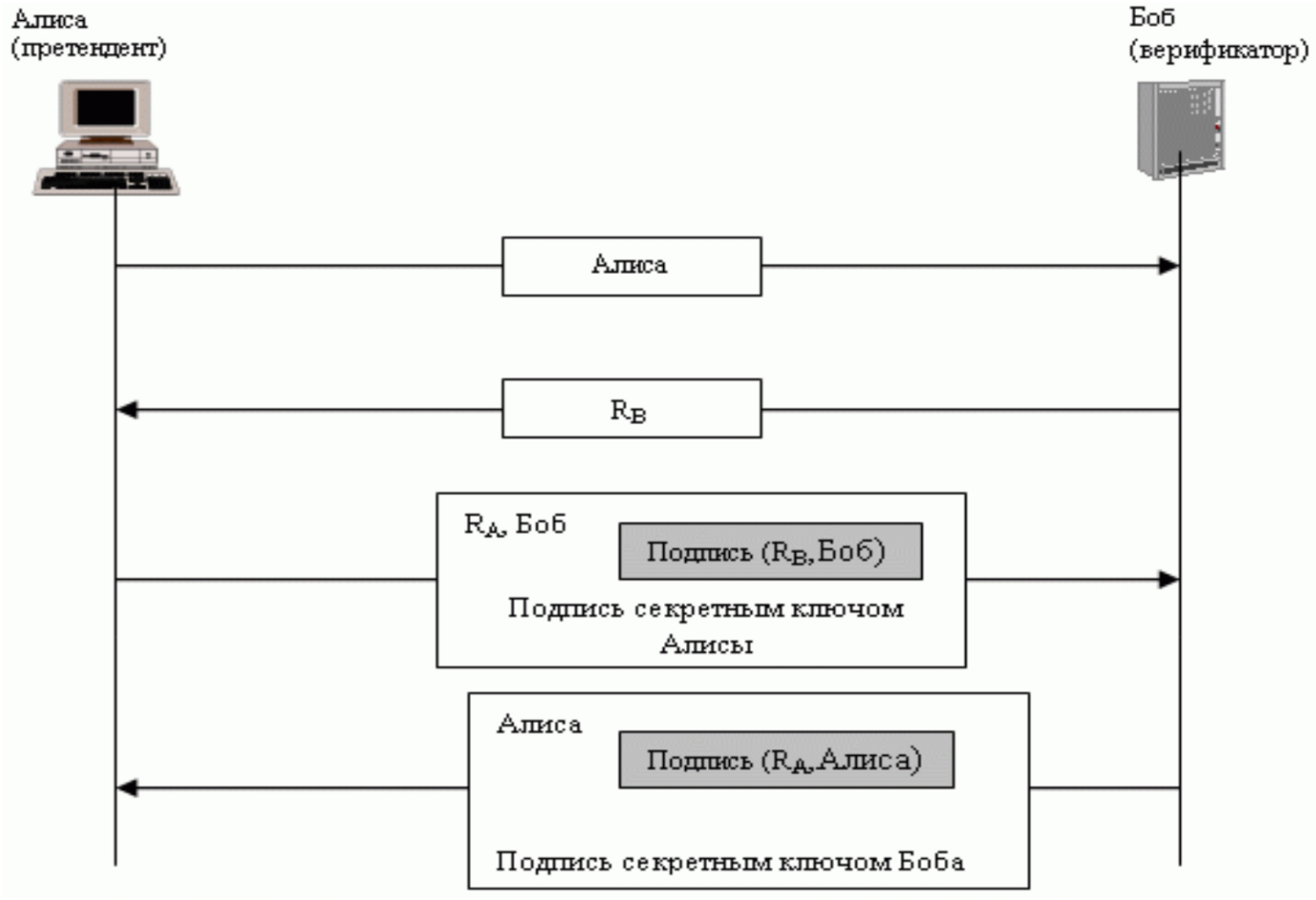

Рис.2.9 Схема второго подхода

Метод «вызов–ответ». Проблемы и ограничения

1. Зависимость от качества генератора случайных чисел
2. Проблема хранения секретов
3. Уязвимость к MITM при отсутствии взаимной аутентификации
4. Требования к синхронизации времени
5. Зависимость от каналов и протоколов передачи
6. Уязвимости реализации (implementation flaws)
7. Проблемы масштабируемости
8. Ограничения производительности
9. Зависимость от криптографической стойкости используемых примитивов
10. Влияние человеческого и организационного фактора

Заключение

Выводы:

- Мощный метод для доказательства владения секретом без его раскрытия.
- Гибкий: реализуем через симметричные/асимметричные схемы, подписи, хеши.
- Защищает от перехвата, повторного использования и фишинга.

Актуальность:

- Основа современных стандартов (FIDO2, WebAuthn, Passkeys).
- Ключевой компонент архитектур Zero Trust.

Список используемых источников

1. Кушниренко, А. Г. Криптографические методы защиты информации: учебное пособие. — Санкт-Петербург: Университет ИТМО, 2018. — 210 с.
2. Объектная аутентификация: лекция 15 // Материалы курса “Математические основы защиты информации”. — mathsec, 2020. (файл: mathsec_lection15-object-authentication_16x9.pdf)
3. Лекция «Установление подлинности объекта» // Учебные материалы по криптографии. — 2019. (файл: Установление подлинности объекта.pdf)
4. Stallings, W. Cryptography and Network Security: Principles and Practice. — 7th ed. — Pearson, 2017. — 752 p.
5. Kaufman, C., Perlman, R., Speciner, M. Network Security: Private Communication in a Public World. — 3rd ed. — Prentice Hall, 2016. — 888 p.
6. Menezes, A., van Oorschot, P., Vanstone, S. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.
7. Wikipedia contributors. Challenge–response authentication // Wikipedia, The Free Encyclopedia. URL: https://en.wikipedia.org/wiki/Challenge–response_authentication
8. NIST Special Publication 800-63-3. Digital Identity Guidelines. — NIST, 2017. URL: https://pages.nist.gov/800-63-3
9. RFC 4226 — OATH HOTP Algorithm: An HMAC-Based One-Time Password Algorithm. — IETF, 2005
10. RFC 6238 — TOTP: Time-Based One-Time Password Algorithm. — IETF, 2011
11. Переводная статья: Challenge–response authentication // Wikipedia (RU). URL: https://translated.turbopages.org/... (дата обращения: 20.01.2025)
12. Studfile. Аутентификация. Методы и протоколы. URL: https://studfile.net/preview/321440/page:4/
13. Лампорта, Л. One-Time Password Authentication. — Bell Labs Technical Report, 1981
14. Dworkin, M. Recommendation for Block Cipher Modes of Operation. — NIST SP 800-38A, 2001
15. ISO/IEC 9798-4. Entity Authentication Mechanisms Using Symmetric Encryption Algorithms. — International Organization for Standardization, 1999