Доклад

Асимметричные криптосистемы: обзор, виды, применение

Беличева Дарья Михайловна

Содержание

# 1 Введение

**Цель работы**

Целью данного доклада является представление основного принципа работы асимметричных криптосистем, их видов и применения в современных информационных системах.

**Задачи**

* Дать определение асимметрическим криптосистемам;
* Рассмотреть историю развития асимметричных криптосистем и их вклад в криптографию;
* Описать основные принципы работы асимметричных криптосистем;
* Представить основные виды асимметричных криптосистем;
* Проанализировать преимущества и недостатки асимметричной криптографии в сравнении с симметричными методами;
* Рассмотреть примеры применения асимметричных криптосистем в различных областях.

## 1.1 Актуальность

В условиях стремительного роста объемов передаваемой и обрабатываемой информации, вопросы безопасности данных становятся крайне важными для защиты личных и корпоративных данных. Асимметричные криптосистемы играют ключевую роль в современных технологиях, обеспечивая безопасную передачу информации, проверку подлинности и целостности данных. Их широкое применение в таких областях, как интернет-коммуникации, электронная коммерция, блокчейн и цифровые подписи, делает эту тему особенно актуальной. С учетом развития квантовых технологий и потенциальных угроз для традиционных криптосистем, изучение асимметричной криптографии и ее устойчивости перед новыми вызовами становится важной задачей для обеспечения информационной безопасности в будущем.

# 2 Теоретическое введение

## 2.1 Определение

Криптография – это наука о способах преобразования информации с целью ее защиты от незаконных пользователей[1]. Современные методы защиты информации зависят от криптографических алгоритмов, обеспечивающих безопасность при передаче и хранении данных. Одним из таких алгоритмов является асимметрическое шифрование.

Асимметричное шифрование – это метод шифрования данных, предполагающий использование двух ключей – открытого и закрытого (рис. 1). Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом[2]. Такой принцип работы делает эти криптосистемы удобными для решения ряда задач в области безопасности, таких как безопасная передача данных и проверка подлинности.

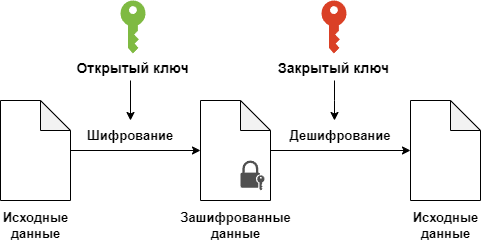


Рис. 1: Ассиметричное шифрование

## 2.2 История и развитие

Исторически первые криптосистемы были симметричными, где обе стороны должны были обладать общим секретным ключом. Однако обмен ключами был проблематичным. В 1976 году Уитфилд Диффи и Мартин Хеллман предложили первую в мире асимметричную криптосистему – протокол для безопасного обмена ключами. Это решение позволило передавать секретные ключи по открытому каналу.

Позднее, в 1977 году, был разработан алгоритм RSA, названный в честь его создателей Рональда Ривеста, Ади Шамира и Леонарда Адлемана. RSA стал первым практическим алгоритмом шифрования с открытым ключом и сегодня широко используется для шифрования данных, цифровых подписей и электронной коммерции.

# 3 Основы асимметричных криптосистем

Асимметричная криптография работает на основе математических задач, решение которых требует значительных вычислительных ресурсов, таких как факторизация больших чисел или вычисление дискретных логарифмов.

Основные принципы:

* **Открытый ключ** используется для шифрования данных. Он может быть свободно передан по открытому каналу.
* **Закрытый ключ** используется для расшифровки зашифрованной информации. Он остается известным только владельцу.

Отправитель использует публичный ключ чтобы зашифровывать (закрыть) сообщение. Зашифрованное сообщение очень сложно расшифровать без приватного ключа, поэтому можно, в целом, без опаски передавать его получателю по открытым каналам связи. Получатель расшифровывает (открывает) сообщение своим секретным, приватным ключом.

## 3.1 Сравнение симметрических и асимметричных криптосистем

Сравнительная характеристика этих систем шифрования приведена в таблице 1.

Таблица 1: Сравнение симметрических и асимметричных криптосистем

| **Характеристика** | **Симметричное шифрование** | **Асимметричное шифрование** |
| --- | --- | --- |
| **Принцип работы** | Один и тот же ключ используется для шифрования и расшифровки | Используются два разных ключа: открытый для шифрования, закрытый для расшифровки |
| **Скорость** | Быстрое шифрование и расшифровка | Медленное шифрование и расшифровка |
| **Вычислительные затраты** | Низкие вычислительные затраты | Высокие вычислительные затраты |
| **Передача ключа** | Требует безопасного обмена секретным ключом | Не требует передачи секретного ключа, только открытого |
| **Безопасность** | Зависит от секретности ключа, уязвимо при утечке | Более безопасно, закрытый ключ остается в секрете |
| **Примеры алгоритмов** | AES, DES, 3DES, Blowfish | RSA, Диффи-Хеллман, DSA, Эллиптическая криптография (ECC) |
| **Область применения** | Шифрование больших объемов данных | Шифрование ключей, цифровые подписи, аутентификация |
| **Преимущества** | Высокая скорость, низкая сложность | Высокая безопасность, отсутствие необходимости передачи секретного ключа |
| **Недостатки** | Необходимость безопасного обмена ключом | Медленная работа с большими объемами данных |
| **Типичные применения** | Шифрование файлов, баз данных | HTTPS, цифровые подписи, обмен ключами, блокчейн |

## 3.2 Виды асимметричных криптосистем

1. RSA (Ривест-Шамир-Адлеман):

RSA основан на сложности разложения больших чисел на простые множители. Шифрование происходит с использованием открытого ключа, а расшифровка – с помощью закрытого. RSA широко применяется в интернет-протоколах, например, для защиты соединений HTTPS, а также для создания цифровых подписей.

Алгоритм RSA[3]:

* Возьмем два больших простых числа p и q.
* Определим n как результат умножения p на q:
* Выберем случайное число, которое назовем d. Это число должно быть **взаимно простым** (не иметь ни одного общего делителя, кроме 1) с результатом умножения:
* Определим такое число e, для которого истинно следующее соотношение:
* Назовем **открытым ключом** числа e и n, а **секретным ключом** — числа d и n.

Шифрование данных с использованием открытого ключа {e, n}:

* Разбиваем шифруемый текст на блоки, каждый из которых может быть представлен в виде числа ( M(i) ) так, чтобы:
* (т.е. каждый блок меньше n).
* Зашифруем текст, рассматриваемый как последовательность чисел ( M(i) ), по следующей формуле:

Расшифровка данных с использованием секретного ключа {d, n}:

Чтобы расшифровать данные, зашифрованные с помощью открытого ключа, необходимо выполнить следующие вычисления:

В результате получаем множество чисел , которые представляют собой исходный текст.

1. Алгоритм Диффи-Хеллмана:

Этот алгоритм позволяет двум сторонам безопасно обменяться секретным ключом по открытому каналу. После этого обмена ключ может использоваться для симметричного шифрования сообщений. Алгоритм Диффи-Хеллмана лежит в основе многих современных криптографических протоколов, таких как SSL/TLS. Алгоритм основан на принципе “сложности вычисления дискретного логарифма” (рис. 2).

При работе алгоритма каждая сторона:

* Генерирует случайное натуральное число a — закрытый ключ.
* Совместно с удалённой стороной устанавливает открытые параметры p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где:
  + p является случайным простым числом
  + (p-1)/2 также должно быть случайным простым числом (для повышения безопасности).
  + g является первообразным корнем по модулю p (также является простым числом).
* Вычисляет открытый ключ A, используя преобразование над закрытым ключом:
* Обменивается **открытыми ключами** с удалённой стороной.
* Вычисляет **общий секретный ключ** K, используя открытый ключ удалённой стороны B и свой закрытый ключ a:

К получается равным с обеих сторон, потому что:

В практических реализациях для a и b используются числа порядка и p порядка . Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

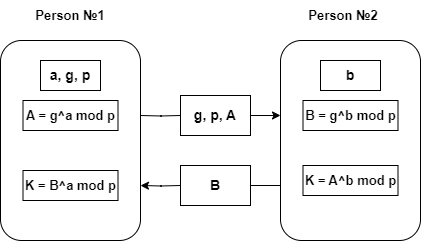


Рис. 2: Алгоритм Диффи – Хеллмана, где K – итоговый общий секретный ключ

1. Эллиптическая криптография (ECC):

Эллиптические кривые используются для создания более эффективных криптосистем. ECC обеспечивает высокий уровень безопасности при значительно меньших размерах ключей по сравнению с RSA. Это делает ECC популярной в таких областях, как мобильные устройства и встроенные системы, где ресурсы ограничены.

1. DSA (Алгоритм цифровой подписи):

DSA (Digital Signature Algorithm) был предложен в 1991 году и является стандартом для цифровых подписей. Алгоритм создает цифровую подпись, которая может быть проверена любой стороной с использованием открытого ключа.

# 4 Применение асимметричных криптосистем

1. HTTPS и SSL/TLS

Веб-сайты используют протокол HTTPS для обеспечения безопасного обмена данными между клиентом и сервером. Асимметричная криптография используется для обмена ключами и установления защищенного канала связи с помощью протоколов SSL или TLS.

1. Электронная почта (PGP, S/MIME)

Программы, такие как PGP (Pretty Good Privacy) и S/MIME, используют асимметричное шифрование для защиты электронной почты. С помощью этих технологий можно шифровать сообщения и подписывать их цифровой подписью, что гарантирует конфиденциальность и подлинность.

1. Цифровые подписи

Цифровые подписи используются для удостоверения подлинности документов, программного обеспечения и транзакций. Примеры применения: системы электронного документооборота, финансовые системы и юридические сделки.

1. Блокчейн и криптовалюты

Асимметричная криптография лежит в основе технологии блокчейн и криптовалют, таких как Bitcoin. Каждая транзакция подписывается закрытым ключом отправителя, что гарантирует безопасность и подлинность транзакций.

1. Мобильные платежные системы

Системы, такие как Apple Pay и Google Pay, используют асимметричное шифрование для безопасной передачи данных о транзакциях между пользователями и банками.

# 5 Заключение

Асимметричные криптосистемы играют важную роль в защите информации в современном мире. Они обеспечивают высокую безопасность при передаче данных, позволяют проверять подлинность документов и сообщений, а также используются в критически важных приложениях, таких как защита веб-сайтов, электронная почта и блокчейн.

# Список литературы

1. Адигеев М.Г. Введение в криптографию. Часть 1 // Ростов-на-Дону: Издательство РГУ. 2002.

2. Асимметричное шифрование [Электронный ресурс]. 2024. URL: <https://encyclopedia.kaspersky.ru/glossary/asymmetric-encryption/>.

3. RSA: Алгоритм асимметричного шифрования [Электронный ресурс]. 2024. URL: <https://e-nigma.ru/stat/rsa/>.