Доклад

Симметричные криптосистемы

Ле Тиен Винь

Содержание

[I.Цель работы 1](#_Toc177680626)

[II Определение и основные принципы 1](#_Toc177680627)

[III. Классификация симметричных криптосистем 1](#_Toc177680628)

[IV. Блочные шифры: DES, AES, Blowfish 2](#_Toc177680629)

[V. Преимущества и недостатки симметричных криптосистем 2](#_Toc177680630)

[VI. Алгоритмы аутентификации и целостности данных 2](#_Toc177680631)

[VII. Стандарты и протоколы симметричного шифрования 2](#_Toc177680632)

[VIII. Перспективы развития симметричной криптографии 3](#_Toc177680633)

[IX. Вывод 3](#_Toc177680634)

# I.Цель работы

Симметричное шифрование — это один из самых распространенных и эффективных методов защиты информации. Он основан на использовании одного и того же ключа для шифрования и дешифрования данных.

# II Определение и основные принципы

* Симметричное шифрование использует один секретный ключ для шифрования и дешифрования данных. Этот ключ должен быть известен как отправителю, так и получателю.
* Конфиденциальность: Обеспечение секретности данных, чтобы только авторизованные лица могли их прочитать.
* Целостность: Гарантирование, что данные не были изменены во время передачи или хранения.
* Аутентификация: Подтверждение личности отправителя и получателя данных.

# III. Классификация симметричных криптосистем

* Симметричные криптосистемы делятся на две основные категории: блочные шифры и поточные шифры.
* Обрабатывают данные блоками фиксированного размера.
* Обрабатывают данные по одному биту или байту за раз.

# IV. Блочные шифры: DES, AES, Blowfish

* DES: Один из первых широко используемых блочных шифров, но в настоящее время считается небезопасным.
* AES: Стандартный алгоритм шифрования, который используется в различных приложениях.
* Blowfish: Быстрый и эффективный алгоритм, который часто используется в программах и системах безопасности.

# V. Преимущества и недостатки симметричных криптосистем

* Симметричные криптосистемы обладают как преимуществами, так и недостатками.
* Преимущества: Высокая скорость шифрования и дешифрования, Простая реализация
* Недостатки: Сложность управления ключами, Риск компрометации ключа

# VI. Алгоритмы аутентификации и целостности данных

Алгоритмы аутентификации и целостности данных дополняют симметричное шифрование, - HMAC: Используется для проверки целостности данных и аутентификации сообщения. - CMAC: Алгоритм аутентификации сообщений, используемый в стандарте AES. - GCM : Режим аутентифицированного шифрования, который обеспечивает как конфиденциальность, так и целостность данных.

# VII. Стандарты и протоколы симметричного шифрования

Симметричное шифрование стандартизировано для обеспечения безопасности. - AES: Стандартный алгоритм симметричного шифрования, который используется во множестве приложений. - DES : Один из первых стандартов шифрования, который уже считается небезопасным. - RC4: Популярный поточный шифр, который используется в различных протоколах.

# VIII. Перспективы развития симметричной криптографии

* Разработка алгоритмов, которые будут устойчивы к атакам квантовых компьютеров.
* Появление новых алгоритмов с более высокой скоростью и надежностью. Развитие более эффективных и безопасных методов управления секретными ключами.

# IX. Вывод

Симметричное шифрование — один из самых популярных и эффективных методов защиты информации.