Шифрование данных

Что это такое

Шифрование данных — это процесс преобразования информации в такой вид, чтобы её нельзя было прочитать без специального ключа.

Типы шифрования

- симметричное
- асимметричное

Ключ

Ключ — это случайная последовательность битов, которая используется для шифрования или расшифровывания данных.

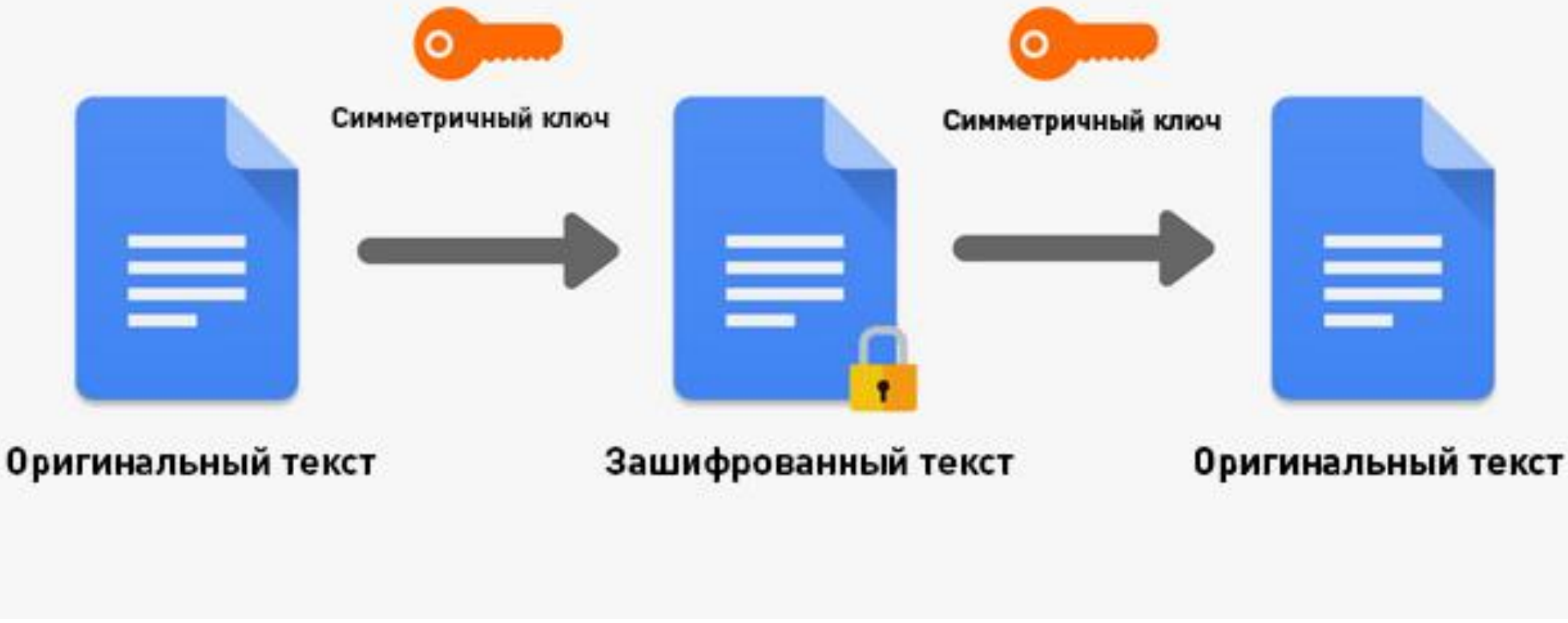
Длина ключа влияет на сложность взлома шифра, поэтому современные стандарты требуют длину ключа в 128 или 256 бит.

Симметричное шифрование

- это метод шифрования, в котором используется один и тот же ключ для зашифровывания и расшифровывания информации.

Симметричное шифрование

Простое в реализации и может быть быстрым, но имеет ограничения, так как один и тот же ключ должен быть доступен обеим сторонам для шифрования и расшифровывания информации. Это может представлять серьёзную опасность, если ключ попадет не в те руки.


Симметричный ключ
Симметричный ключ
Оригинальный текст
Зашифрованный текст
Оригинальный текст

Достоинства

+ Простота
+ Эффективность

Недостатки

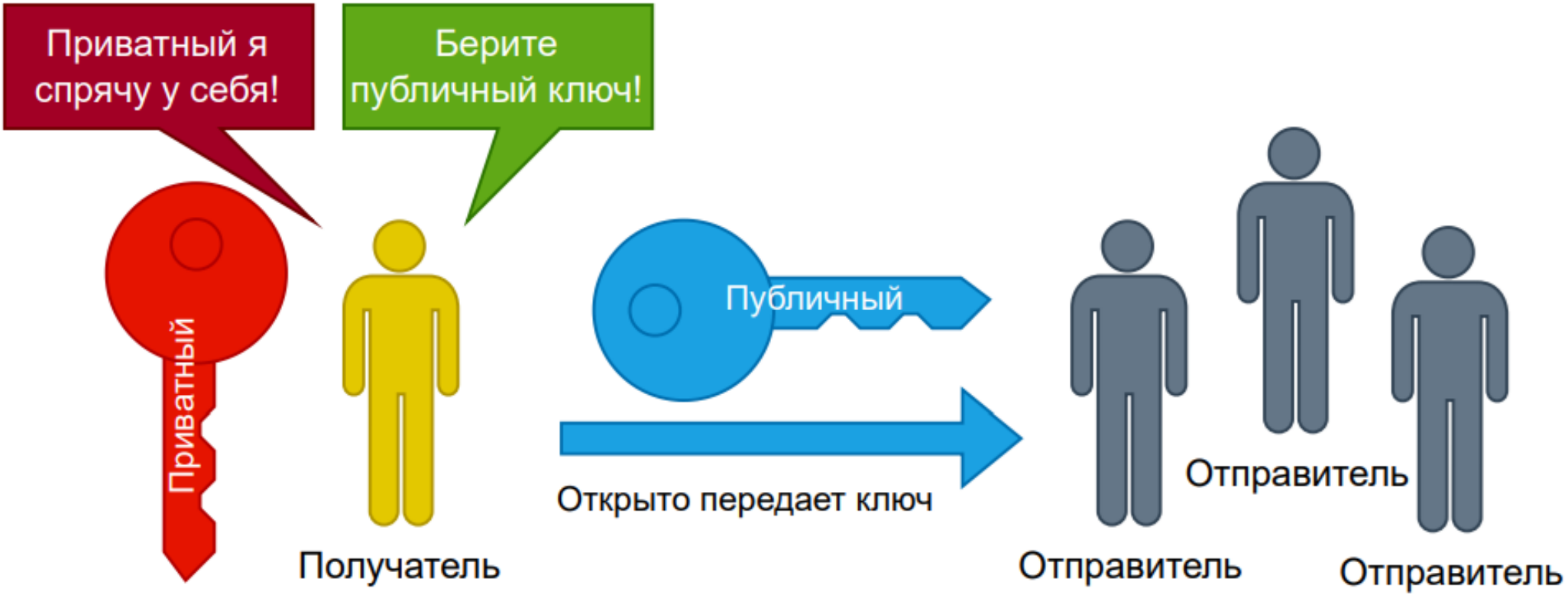
- Необходимость совместного использования ключа

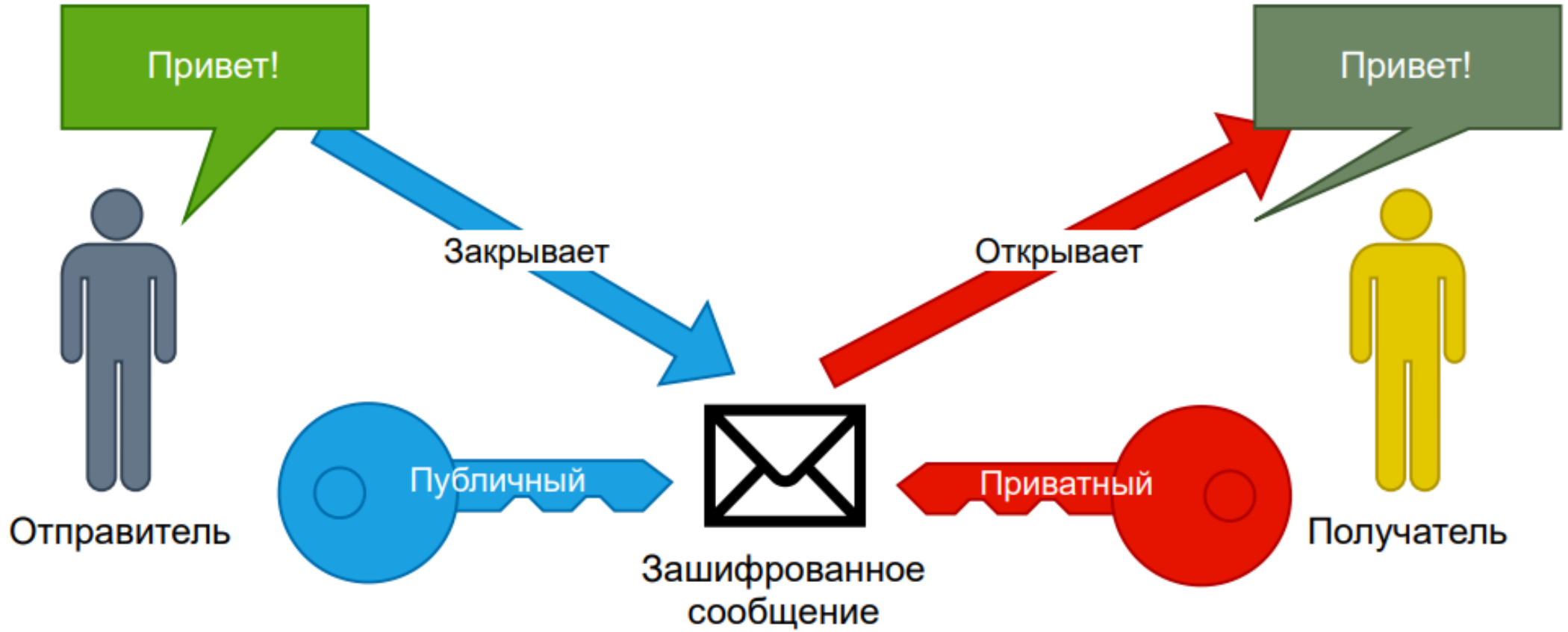
Асимметричное шифрование

- это тип шифрования, в котором для шифрования и дешифрования данных используют разные ключи. Для шифрования используется открытый ключ, а для дешифрования закрытый ключ.

Асимметричное шифрование

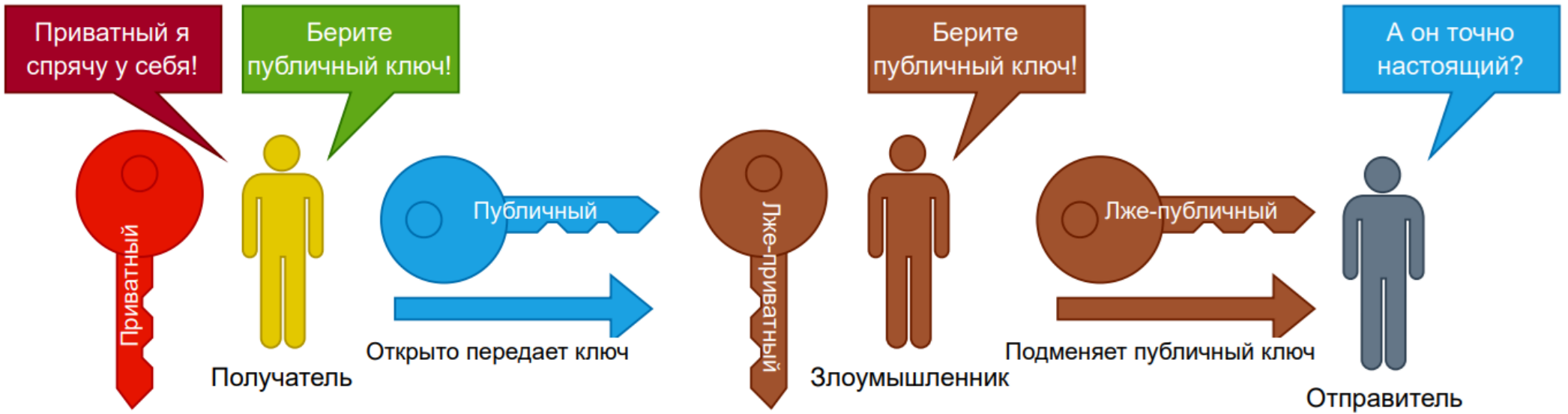
У каждого пользователя два ключа, открытый и закрытый. Открытый ключ можно отправлять всем желающим, а закрытый ключ хранится в безопасности. Для шифрования используется открытый ключ, а для расшифровки закрытый.


Приватный я спрячу у себя!
Берите публичный ключ!
Приватный
Получатель
Публичный
Открыто передает ключ
Отправитель
Отправитель
Отправитель


Привет!
Привет!
Закрывает
Открывает
Публичный
Приватный
Отправитель
Получатель
Зашифрованное
сообщение

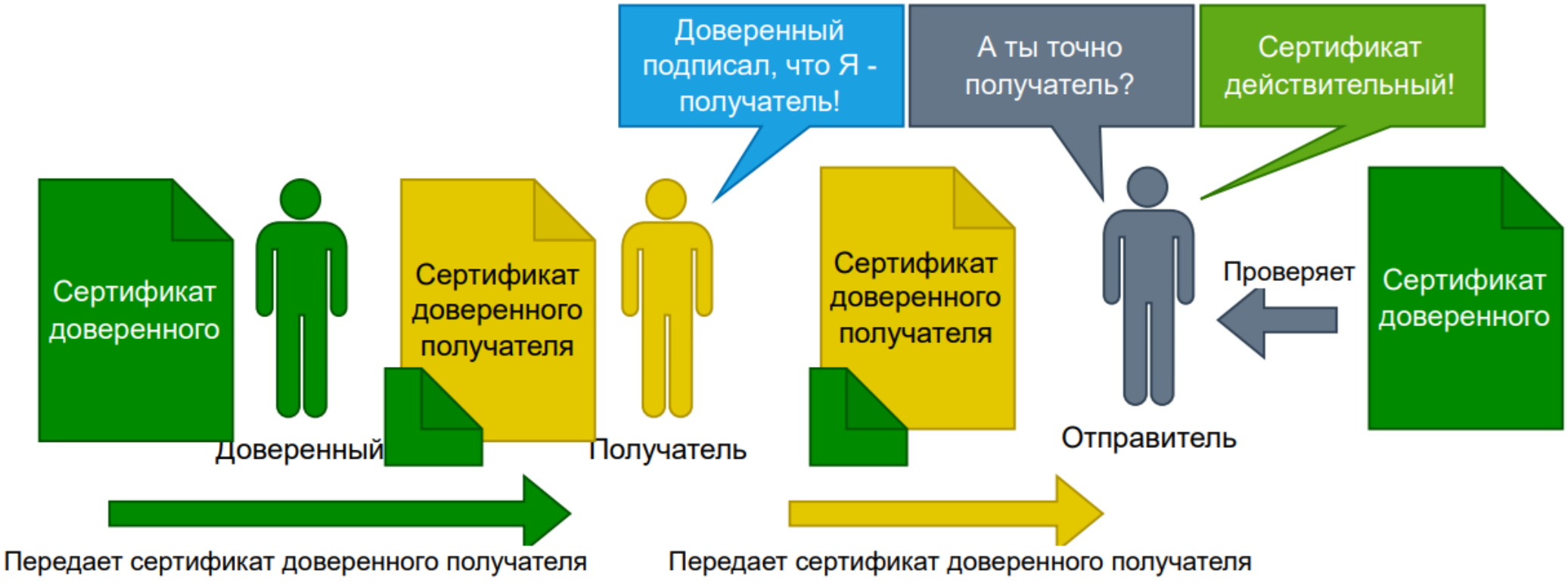
Сертификаты

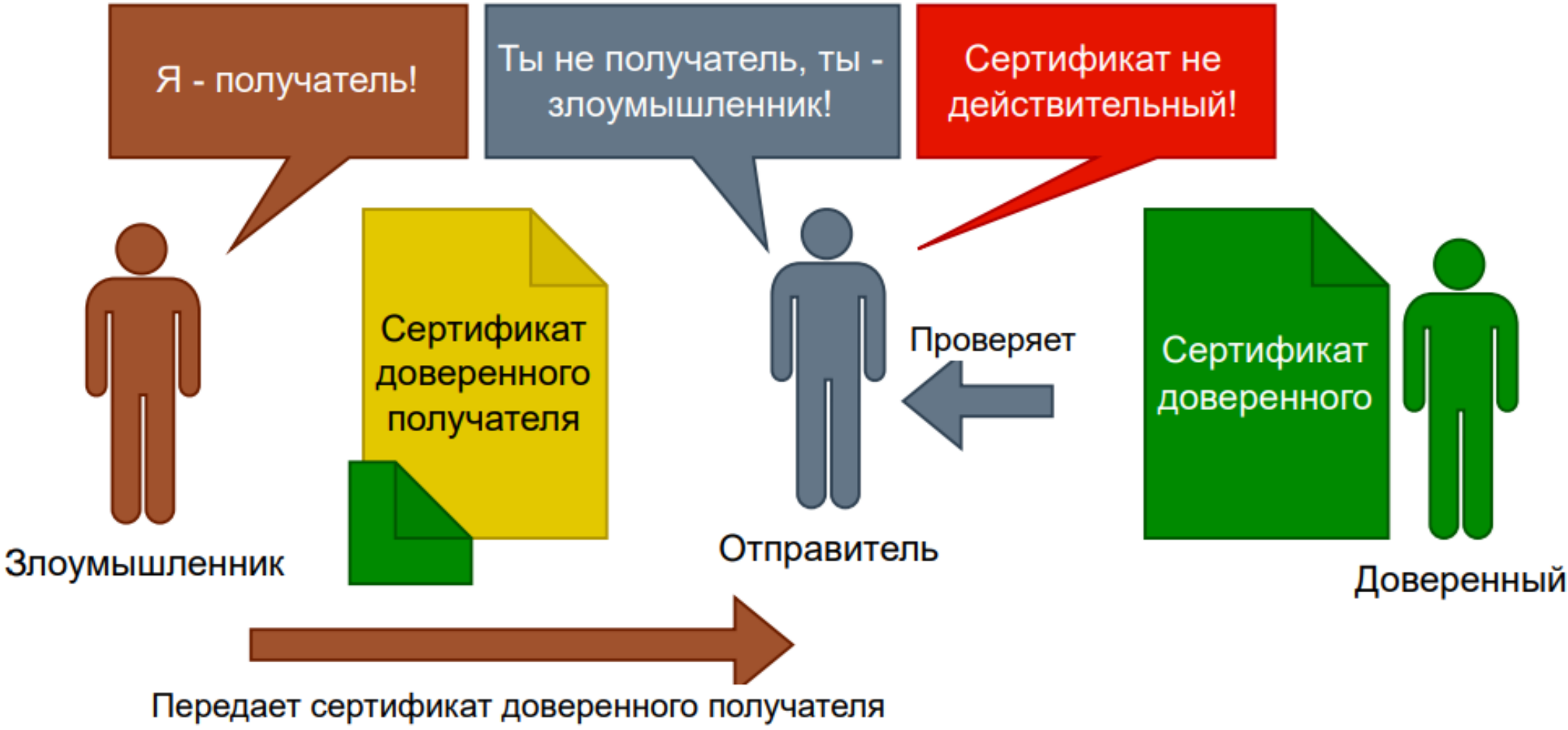
Этот шифр подвержен атакам. Одна из таких - подмена ключа или "атака посредника". Злоумышленник может перехватить публичный ключ и подменить его своим. Отправитель будет шифровать сообщение ключом злоумышленника, злоумышленник будет читать сообщение, шифровать ключом получателя и пересылать получателю.

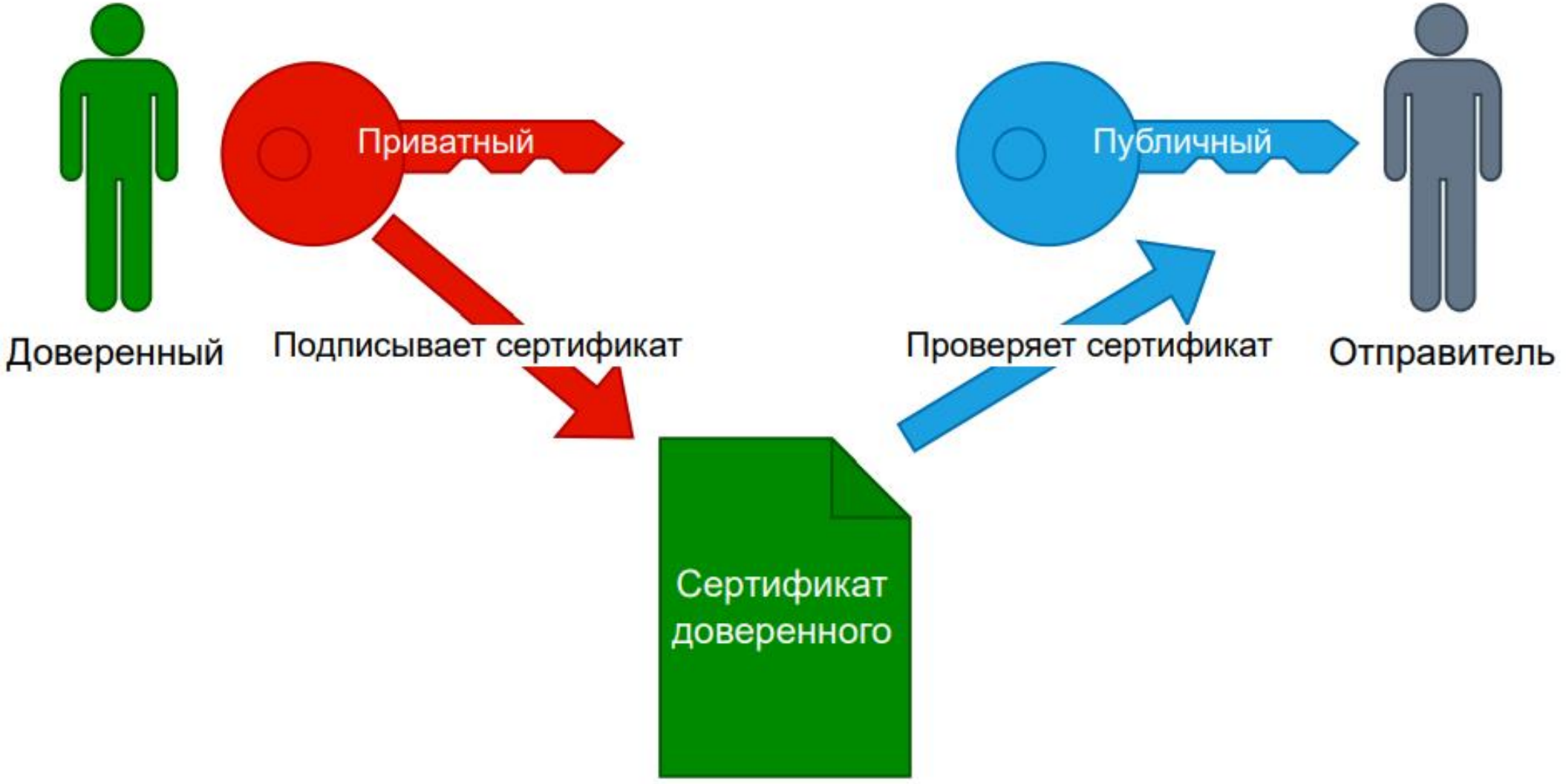

Приватный я спрячу у себя!
Берите публичный ключ!
Приватный
Получатель
Публичный
Открыто передает ключ
Берите публичный ключ!
Лже-приватный
Злоумышленник
Лже-публичный
Подменяет публичный ключ
А он точно настоящий?
Отправитель

Сертификаты

Для решения этой проблемы можно использовать третье лицо - доверенного. Доверенный будет подтверждать, что получатель - тот за кого себя выдает. Доверенный подписывает сертификат, в котором указана подтверждаемая информация. Отправитель проверяет подлинность сертификата и его подписи и убеждается, что получатель - верный.


Доверенный подписал, что Я - получатель!
А ты точно получатель?
Сертификат действительный!
Сертификат доверенного
Сертификат доверенного получателя
Сертификат доверенного получателя
Проверяет
Сертификат доверенного
Доверенный
Получатель
Отправитель
Передает сертификат доверенного получателя
Передает сертификат доверенного получателя


Я - получатель!
Ты не получатель, ты - злоумышленник!
Сертификат не действительный!
Сертификат доверенного получателя
Проверяет
Сертификат доверенного
Злоумышленник
Отправитель
Доверенный
Передает сертификат доверенного получателя


Приватный
Публичный
Доверенный
Подписывает сертификат
Проверяет сертификат
Отправитель
Сертификат доверенного

Преимущества

+ необходимость передачи только открытого ключа

+ невозможность восстановления закрытого ключа из открытого

+ возможность подписи электронных сообщений, что позволяет подтвердить их аутентичность

Недостатки

- Медленность
- Уязвимость к взлому ключей
- сложность установления и обслуживания

Метод шифрования

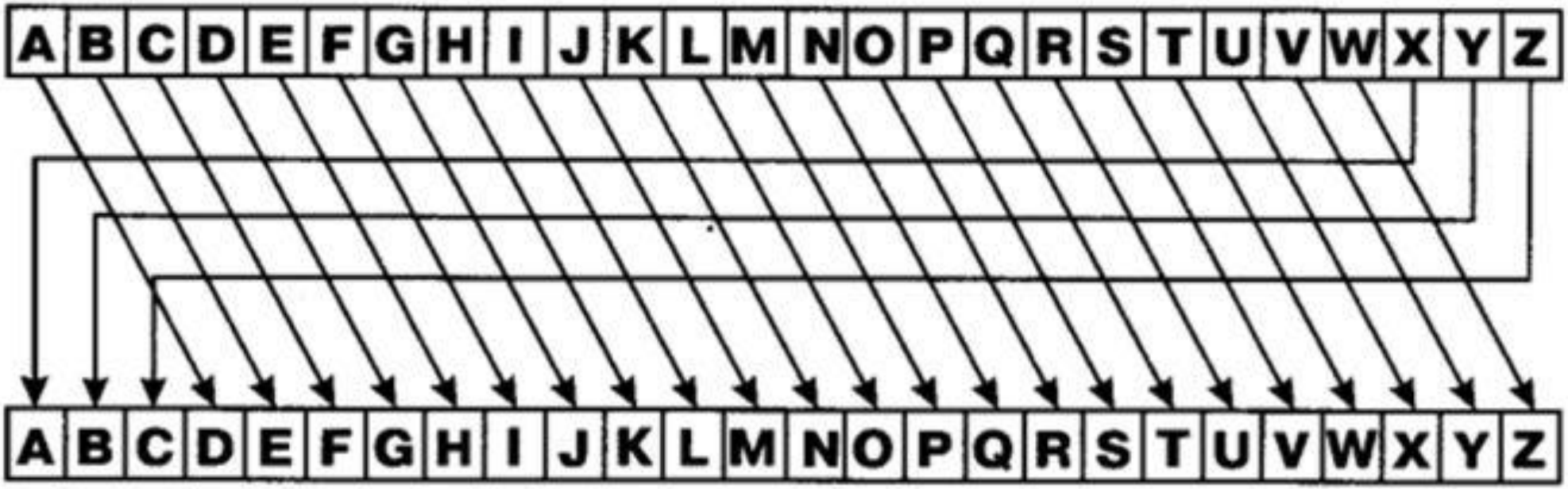
Существует множество различных методов шифрования, таких как подстановочный метод, перестановочный метод и блочный метод. Каждый из этих методов имеет свои сильные и слабые стороны, и выбор метода зависит от конкретных потребностей и требований.

Шифр подстановки

это простой метод шифрования, при котором каждая буква в открытом тексте заменяется другой буквой или символом. Преобразование исходных букв в новые символы определяется ключом, который должен храниться в секрете для обеспечения безопасности зашифрованного сообщения.

Шифр Цезаря

— это тип шифра подстановки, в котором каждая буква сдвигается на определенное количество позиций вниз по алфавиту. Например, при смещении на 3 буква «А» будет заменена на «Д», «В» на «Е» и так далее. Шифр Цезаря легко взломать, так как существует всего 33 возможных ключа, которые может легко проверить криптоаналитик.



Ключ: 3

Открытый текст:

P = HELLO CAESAR CIPHER

Зашифрованный текст:

C = KHOOR FDHVDU FLSKHU

Шифр перестановки

Перестановочный метод шифрования — это один из самых простых методов шифрования, основанный на перестановке букв или символов в тексте.

Шифр перестановки

1. Определяется некоторая ключевая перестановка символов в алфавите.

2. Исходный текст переставляется согласно ключевой перестановке.

3. Для расшифровки текста используется обратная ключевая перестановка.

Шифр перестановки

Listen

Анаграмма

Скитала

Шифр перестановки

Основным преимуществом перестановочного метода шифрования является его простота и быстрота выполнения. Однако, этот метод имеет много ограничений, так как он не достаточно безопасен для защиты важных данных. Он может легко взломать с помощью методов анализа текста, таких как частотный анализ

Блочное шифрование

Метод шифрования в котором данные разбиваютмя на блоки одинаковой длины и каждый из них зашифровывается отдельно. Для шифрования используется ключ, который задает правила замены блоков данных.

Блочное шифрование

Блочные методы шифрования бывают как симметричными, так и асимметричными

AES

AES (Advanced Encryption Standard) - это симметричный алгоритм шифрования, который используется для защиты конфиденциальности данных. Он был выбран в качестве стандарта шифрования правительством США в 2001 году и заменил предыдущий стандарт DES (Data Encryption Standard).

AES

AES шифрует данные в блоках фиксированного размера (обычно 128 бит) и использует один и тот же ключ для шифрования и дешифрования данных. Длина ключа может быть 128, 192 или 256 бит, и чем длиннее ключ, тем сложнее взломать шифр.

Алгоритм работы

Алгоритм AES работает по принципу замены и перестановки битов в блоке данных. Блок данных разбивается на несколько столбцов и строк, которые затем проходят через несколько раундов шифрования.

Алгоритм работы

1. Замена байтов (SubBytes)
2. Сдвиг строк (ShiftRows)
3. Смешивание столбцов (MixColumns)
4. Добавление ключа (AddRoundKey)

Расшифровка

После выполнения раундов шифрования, последний раунд не включает шага "MixColumns", чтобы упростить процесс дешифрования. Для расшифровки блока данных выполняются обратные операции с использованием ключа дешифрования.

RSA

RSA — широко используемый алгоритм шифрования с открытым ключом. Впервые он был описан Роном Ривестом, Ади Шамиром и Леонардом Адлеманом в 1977 году, и его безопасность основана на математической сложности факторизации больших чисел.

Алгоритм работы

Генерация ключей: отправитель и получатель генерируют пару открытых и закрытых ключей. Закрытый ключ хранится в секрете, а открытый ключ доступен другим.

Алгоритм работы

Шифрование: когда отправитель хочет отправить сообщение получателю, он использует открытый ключ получателя для шифрования сообщения. Затем зашифрованное сообщение отправляется по незащищенному каналу.

Расшифровка: получатель использует свой закрытый ключ для расшифровки сообщения, раскрывая исходный открытый текст.

RSA

Безопасность RSA заключается в том, что, хотя легко зашифровать сообщение с помощью открытого ключа получателя, чрезвычайно сложно расшифровать сообщение без соответствующего закрытого ключа. Это связано с математическими проблемами, связанными с разложением на множители больших чисел, которые используются в качестве основы для алгоритма RSA.