Задание № 1

Что нужно сделать

Приведите протокол подписи одного и того же документа одновременно двумя пользователями с помощью хэш-функций при условии, что пользователи не доверяют друг другу.

Решение:

Протокол подписи документа двумя пользователями с помощью хэш-функций:

1. Инициализация:

Пользователи Алиса и Боб имеют свои закрытые и публичные ключи для цифровой подписи;

Алиса и Боб выбирают безопасную хэш-функцию (например, SHA-256, Secure Hash Algorithm 256-bit).

2. Подготовка документа:

Алиса создает документ, который необходимо подписать обоими сторонами.

3. Хеширование документа:

Алиса вычисляет хэш документа с помощью выбранной хэш-функции.

4. Цифровая подпись хэша документа Алисой:

Алиса подписывает хэш документа с помощью своего закрытого ключа и отправляет подписанный хэш и исходный документ Бобу.

5. Проверка подписи Алисой:

Боб проверяет подпись Алисы, используя ее публичный ключ. Если проверка проходит успешно, он приступает к следующему этапу.

6. Хеширование и подпись документа Бобом:

Боб также вычисляет хэш документа с помощью выбранной хэш-функции.

Боб подписывает этот хэш с помощью своего закрытого ключа.

7. Объединение подписей:

Подписи обоих пользователей объединяются в одном документе, который содержит исходный документ, подписанный хэш Алисы и подписанный хэш Боба.

8. Отправка подписанного документа:

Боб отправляет подписанный документ Алисе для завершения процесса.

Обоснование:

Использование хэш-функций гарантирует, что любое изменение в документе приведет к совершенно другому хэшу. Когда каждый пользователь подписывает хэш документа своим закрытым ключом, они подтверждают свою одобрительную позицию по отношению к содержанию документа.

Если один из пользователей решит изменить документ после того, как он был подписан другой стороной, это будет легко обнаружено из-за несоответствия хэшей или неудачной проверки цифровой подписи.

Таким образом, данный протокол позволяет двум недоверяющим друг другу сторонам подписать один и тот же документ, сохраняя при этом его целостность и достоверность.

Вывод:

Протокол подписи документа двумя пользователями, основанный на использовании хэш-функций, обеспечивает надежное и эффективное средство для обеспечения целостности и подлинности документа при сотрудничестве двух недоверяющих друг другу сторон.

Задание № 2

Что нужно сделать
Докажите, что в криптосистемах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и электронной подписи.

Решение:

Доказательство того, что в криптосистемах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и электронной подписи:

1. Основное понимание:

В криптосистемах на основе открытых ключей обычно имеется пара ключей: открытый (публичный) и закрытый (приватный). Открытый ключ используется для шифрования, а закрытый ключ - для расшифрования. В случае электронной подписи, закрытый ключ используется для создания подписи, а открытый ключ - для её верификации.

2. Отсутствие недвусмысленности:

Использование одной и той же пары ключей для обеих целей уничтожает недвусмысленность операций. Если вы получите зашифрованный текст, вы не можете быть уверены, предназначался ли он для конфиденциальности (шифрования) или для аутентификации (подписи).

3. Специфические свойства операций:
Операции шифрования и подписи обычно имеют разные криптографические свойства и требования. Например, безопасное шифрование может потребовать, чтобы ключи менялись чаще, чем ключи для подписи.

4. Компрометация приватного ключа:

Если приватный ключ будет скомпрометирован (например, если кто-то узнает закрытый ключ, используемый для шифрования), все ранее подписанные сообщения станут уязвимыми. То же самое будет справедливо и наоборот: если ключ для подписи будет скомпрометирован, все зашифрованные этим ключом данные будут уязвимыми.

5. Потенциальная угроза:

Если бы одна и та же пара ключей использовалась как для шифрования, так и для подписи, то любое зашифрованное сообщение, отправленное кому-то, могло бы быть интерпретировано как "подписанный" контент. Это создает возможность для многочисленных атак.

6. Пример атаки (“Человек посередине”):

• **Сценарий:**
Анна хочет отправить конфиденциальное сообщение Борису, используя его публичный ключ для шифрования. Она также хочет подписать это сообщение, чтобы Борис мог верифицировать его подлинность. Она использует свой закрытый ключ для подписи. Однако предположим, что они оба используют одну и ту же пару ключей для обоих этих действий.

• **Атака:**
Елена, злоумышленник, решает вмешаться в коммуникацию. Она перехватывает сообщение Анны перед тем, как оно достигнет Бориса.

• **Дешифрование и подмена:**
так как Елена имеет публичный ключ Анны (который предполагается открытым), она может проверить подпись и убедиться, что сообщение действительно от Анны. Елена теперь может дешифровать сообщение с использованием своего закрытого ключа, внести изменения, а затем повторно зашифровать сообщение своим публичным ключом и направить его Борису.

• **Подмена подписи**:
Елена также может использовать свой закрытый ключ для подписи "нового" сообщения, прежде чем отправить его Борису. Поскольку она использует свой закрытый ключ, это будет выглядеть так, будто Анна является отправителем этого сообщения.

• **Результат:**
когда Борис получает сообщение, он думает, что это от Анны, потому что он может проверить подпись с помощью публичного ключа Анны и дешифровать сообщение своим закрытым ключом. Однако на самом деле сообщение было подменено Еленой, и оно может содержать ложную или вредоносную информацию.

Вывод:
Для обеспечения безопасности и надежности криптосистем на основе открытых ключей важно разделять ключи для шифрования и электронной подписи. Это обеспечивает, что даже если один из ключей будет скомпрометирован, это не повлияет на другую операцию, и помогает избежать потенциальных атак и угроз безопасности.

Задание № 3

Что нужно сделать
Напишите, что общего между собственноручной и электронной подписью и чем они различаются.

Решение:

Сходства между собственноручной и электронной подписью:

1. Подтверждение авторства: как собственноручная, так и электронная подписи служат средством подтверждения авторства документа или сообщения. Они показывают, что определенный человек утверждает или одобряет содержание.

2. Юридическая значимость: во многих странах обе эти формы подписи имеют юридическую силу. Это означает, что они могут использоваться в суде как доказательства согласия или одобрения.

3. Уникальность: и собственноручная, и электронная подписи должны быть уникальными для каждого индивида. Это уникальность делает подпись трудной для подделки.

Различия между собственноручной и электронной подписью:

1. Формат: собственноручная подпись — это физическое представление именной или уникальной марки, сделанной на бумаге или другом физическом носителе. Электронная подпись — это цифровая марка, созданная с использованием специализированных алгоритмов и ключей.

2. Технология: электронная подпись обычно создается с использованием криптографических методов, что делает ее безопаснее и устойчивее к подделке, чем собственноручную.

3. Применение: в то время как собственноручные подписи чаще используются в традиционных документах, электронные подписи идеально подходят для цифровых документов и онлайн-транзакций.

4. Доказательная база: подтверждение аутентичности собственноручной подписи может потребовать экспертов по графологии, тогда как электронная подпись предоставляет криптографическое подтверждение своей аутентичности.

5. Временные рамки: электронные подписи могут включать в себя временные метки, показывающие, когда документ был подписан. Это сложно или невозможно добиться с собственноручной подписью без дополнительных доказательств.

Вывод:
И собственноручная, и электронная подписи играют важную роль в подтверждении авторства и утверждении содержания документа. Однако с ростом цифровой интеграции электронные подписи становятся все более ценными из-за их удобства, безопасности и мгновенного развертывания в цифровых средах.