КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Шабанов Нурлан 315R

Криптология — наука о защите информации – делится на две части: криптографию и криптоанализ.

Криптография – это часть криптологии, связанная с проектированием секретных систем,
наука о том
- как сделать информацию конфиденциальной, избирательно доступной (шифрование)
- как обеспечить целостность данных
- как обеспечить аутентификацию (достоверную идентификацию)
  - субъекта: аутентичность информационного источника
  - объекта: пользователя, процесса
- как обеспечить доказательность действия (неотказуемость)
- как обеспечить контроль доступа (авторизацию)

Криптоанализ – это часть криптологии, связанная со взломом секретных систем.

Основные задачи криптографии

конфиденциальность данных:
цель: сделать данные «нечитаемыми» для непосвященных
метод: шифрование

целостность и имитостойкость данных
цель: исключить возможность умышленного и неумышленного изменения (искажения) данных неуполномоченными лицами
метод: хэш, имитовставка, электронно-цифровая подпись

аутентификация субъекта – доказательство того, что субъект действия является именно тем, за кого себя выдает

аутентификация источника данных – доказательство того, что данные изданы определенным субъектом и являются подлинными (т.е. никем другим не искажены; в этом смысле – аутентификация источника данных автоматически обеспечивает их целостность)

обеспечение неотказуемости – невозможности для субъекта, выполнившего некоторое действие, впоследствии отказаться от факта выполнения этого действия

Криптограф ищет методы, обеспечивающие секретность и/или подлинность информации путём шифрования исходного текста.

Криптоаналитик пытается выполнить обратную задачу, раскрывая шифр или подделывая сообщение так, чтобы выдать их за подлинные.

Криптографические примитивы

Симметричное шифрование. Заключается в том, что обе стороны-участники обмена данными имеют абсолютно одинаковые ключи для шифрования и расшифровки данных. Данный способ осуществляет преобразование, позволяющее предотвратить просмотр информации третьей стороной.

Асимметричное шифрование. Предполагает использовать в паре два разных ключа — открытый и секретный. В асимметричном шифровании ключи работают в паре — если данные шифруются открытым ключом, то расшифровать их можно только соответствующим секретным ключом и наоборот — если данные шифруются секретным ключом, то расшифровать их можно только соответствующим открытым ключом. Использовать открытый ключ из одной пары и секретный с другой — невозможно. Каждая пара асимметричных ключей связана математическими зависимостями. Данный способ также нацелен на преобразование информации от просмотра третьей стороной.

Цифровые подписи. Цифровые подписи используются для установления подлинности документа, его происхождения и авторства, исключает искажения информации в электронном документе.

Хеширование. Преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хеш-кодом, контрольной суммой или дайджестом сообщения (англ. message digest). Результаты хэширования статистически уникальны. Последовательность, отличающаяся хотя бы одним байтом, не будет преобразована в то же самое значение.

Симметричные криптосистемы: трудности

- Для шифрования и дешифрования используется ***общий ключ.***
- И передатчик, и получатель должны знать общий ключ.
- Общий ключ должен быть передан по второму секретному каналу связи.
- Создание и передача длинного секретного ключа.
- Непрактичны для большого числа передатчиков и получателей.

Симметричные криптосистемы: достоинства

- Простота и быстрота построения и реализации.
- Высокое быстродействие.
- Все классические криптосистемы симметричные.

Известные симметричные криптосистемы:

- Известные симметричные криптосистемы с : DES, AES.
- DES: разработан фирмой IBM для правительства США. Национальный стандарт шифрования США в 1977-2000 годах.
- AES: создан Дейманом и Рейманом в Бельгии. Национальный стандарт шифрования США с 2000 года.

Симметричные криптосистемы: примеры

Шифр Цезаря:
построен по алгоритму:
читать четвертую букву вместо первой, т.е. ключ равен 3.
В шифре Цезаря ключ равен 3 (величине сдвига букв алфавита).

Пример:
Открытый текст: **meet me at central park**
Шифр: phhw ph dw fhqwudo sdun

Недостаток криптосистемы: легко можно раскрыть шифр

Шифр Виженера:

построен по следующему алгоритму:

заменить каждую букву английского языка цифрой 0-25: A ↔ 0, B ↔ 1, …, Z ↔ 25,

в качестве ключа рассмотреть любую последовательность букв английского языка,

заменить ключ последовательностью цифр согласно пункту 1,

заменить открытый текст последовательностью цифр согласно пункту 1,

записать под последовательностью цифр открытого текста последовательность цифр ключа, при этом последовательность цифр ключа записать необходимое число раз,

сложить попарно эти две последовательности, при этом если сумма равна или больше 26, то вычесть 26.

Заменить полученные цифры буквами английского языка согласно пункту 1.

Пример:

Открытый текст: **meet me at central park**

Ключ: **cipher**

Согласно алгоритму ключ *cipher* заменяется последовательностью цифр (2,8,15,7,4,17),

согласно алгоритму открытый текст *meet me at central park* заменяется последовательностью цифр (12,4,4,19,12,4,0,19,2,4,13,19,17,0,11,15,0,17,10),

в качестве шифра исходного открытого текста получим последовательность *omtaqvcbrlrmtiaweim*.

Асимметричные криптосистемы: основные свойства

Для шифрования и дешифрования используются *различные ключи.*
Для шифрования сообщений используется *открытый ключ,* являющийся общедоступным.
Для дешифрования сообщений используется *закрытый ключ,* являющийся секретным.
Знание открытого ключа не даёт возможность определить закрытый ключ.

Асимметричные криптосистемы: достоинства

- Не требуется секретный общий ключ.
- Простая схема обеспечения секретности (не требуется доверяемая третья сторона).
- Удобна для защиты информации в открытой многопользовательской среде.