центр Hewlett-Packard, Биллингем, Великобритания; Дата-центр IBM, Сиракьюс, США.

Литература

1. Андрей Москаленко.Стойко-место(рус.)//Бизнес-журнал: журнал. – М., 2015.– Октябрь (№ 10 (234)).

Криптография как наука. Типы криптосистем

Лахцутко П.А., Мяделец А.В.
Научный руководитель: КовальковаИ.А.
Белорусский национальный технический университет

Стремление узнавать секреты является глубоко укоренившейся, неотъемлемой чертой человеческой натуры; даже самый нелюбопытный ум воодушевляется перспективой узнать что-то такое, что утаивается от других. [2]

Криптография представляет собой совокупность методов преобразования данных (шифрования), направленных на то, чтобы сделать эти данные бесполезными для противника, то есть на сокрытие их содержания. Слово «криптография» («cryptography») происходит от греческих слов «kryptus» – тайный, «graphein» – писать, т.е. дословно «тайнопись».

История криптографии насчитывает около 4 тысяч лет. Древние египтяне защищали свои секреты шифр-иероглифами, римляне – шифром Цезаря, венецианцы – шифровальными дисками Альберти.

Криптография в прошлом использовалась, прежде всего, в военных целях. Однако сейчас, по мере образования информационного общества, криптография становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию. Криптографические методы защиты информации представляют собой мощное оружие в борьбе за информационную безопасность.

Наряду с подсистемой разграничения доступа к ресурсам, обеспечение конфиденциальности различных данных основано на применении криптографических преобразований защищаемой информации. Использование криптографических преобразований позволяет скрыть защищаемую информацию путём перевода её в нечитаемый вид. При этом чтение информации возможно только после дешифрования сообщения на секретном ключе, известном легальным пользователям и неизвестном

злоумышленнику. Стойкость криптографических преобразований основана только на секретности ключа дешифрования.

Важнейшими характеристиками алгоритмов шифрования являются длина ключа, скорость шифрования и криптостойкость (способность противостоять криптоаналитическому вскрытию, то есть насколько получаемый шифр трудно дешифровать). Алгоритмы шифрования, дополненные схемами распределения и управления ключами, представляют собой криптографическую систему (криптосистему).

Различают криптосистемы двух типов: симметричные и асимметричные.

1. Симметричные криптосистемы (secretkeysystems – с секретным ключом) построены на основе сохранения в тайне ключа шифрования. Процессы шифрования и расшифрования используют один и тот же ключ. Секретность ключа является постулатом. Основная проблема при применении симметричных криптосистем для связи заключается в сложности передачи обеим сторонам секретного ключа. Однако данные системы обладают высоким быстродействием. Раскрытие ключа злоумышленником грозит раскрытием только той информации, что была зашифрована на этом ключе. Американские и российский стандарты шифрования AES, DES и ГОСТ28.147-89 имеют секретные ключи. [3]

2. В асимметричных криптосистемах (publickeysystems – системы открытого шифрования, с открытым ключом и т. д.) для шифрования и расшифрования используются разные преобразования. Шифрование является абсолютно открытым для всех, а расшифрование – секретным. Таким образом, любой, кто хочет что-либо зашифровать, пользуется открытым преобразованием, но расшифровать и прочитать это сможет лишь тот, кто владеет секретным преобразованием. В настоящий момент во многих асимметричных криптосистемах вид преобразования определяется ключом, то есть у пользователя есть два ключа – секретный и открытый. [3]

Традиционные симметричные криптосистемы:

- *Шифрование методом замены* (*подстановки*): шифры простой замены (шифр простой замены Атбаш, шифр Цезаря, шифр с использованием кодового слова, шифр простой моноалфавитной замены, шифр Гронсфельда); шифрование методом Вернама.
- *Шифрование методами перестановки*: метод простой перестановки; алгоритм Гамильтона.
- *Шифрование методом гаммирования* (наложение на открытые данные по определённому закону гаммы шифра, то есть двоичного числа, сформированного на основе генератора случайных чисел).

Открытый ключ используется для шифрования информации, является доступным для всех пользователей и может быть опубликован в общедоступном месте для использования всеми пользователями криптографической сети. Дешифрование информации с помощью открытого ключа невозможно.

Секретный ключ является закрытым и не может быть восстановлен злоумышленником из открытого ключа. Этот ключ используется для дешифрования информации и хранится только у одного пользователя – сгенерировавшего ключевую пару.

Открытый ключ публикуется в общедоступном месте, и каждый, кто захочет послать сообщение этому пользователю, зашифровывает текст открытым ключом. Расшифровать его сможет только упомянутый пользователь с секретным ключом. Таким образом, решается проблема передачи секретного ключа, существующая для симметричных систем. Однако асимметричные криптосистемы, как правило, более трудоёмки и медлительны, чем симметричные. [4]

Криптостойкость асимметричных систем базируется в основном на алгоритмической трудности решить за приемлемое время задачу дешифрования. Если всё же злоумышленнику удастся построить такой алгоритм, то дискредитирована будет вся криптосистема и дешифрованы все сообщения этой системы. В этом состоит главная угроза безопасности информации при использовании асимметричных криптосистем. К асимметричным криптосистемам относятся RSA, Рабина и др.

У. Диффи и М. Хеллман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы:

1. Вычисление ключевой пары (ОК, СК) должно быть достаточно простым.

2. Отправитель, зная открытый ключ получателя, может легко получить шифротекст.

3. Получатель, используя свой секретный ключ, может легко из шифротекста восстановить исходное сообщение.

4. Знание открытого ключа злоумышленником не должно влиять на криптостойкость системы. При попытке вычислить злоумышленником закрытый ключ по открытому, он должен наталкиваться на непреодолимую вычислительную проблему. [1]

Сравнивая симметричные криптосистемы с асимметричными, можно выявить ряд достоинств и недостатков:

Достоинства:

- скорость (по данным AppliedCryptography– на 3 порядка выше);
- простота реализации (за счёт более простых операций);
- меньшая требуемая длина ключа при сопоставимой стойкости;

• изученность.

Недостатки:

• сложность управления ключами в большой сети, которые постоянно надо генерировать, передавать, хранить и уничтожать;

• сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам. Для компенсации недостатков симметричного шифрования в настоящее время широко применяется комбинированная (гибридная) криптографическая схема, где с помощью асимметричного шифрования передаётся сеансовый ключ, используемый сторонами для обмена данными с помощью симметричного шифрования. Отличительным свойством симметричных шифров является невозможность их использования для подтверждения авторства, так как ключ известен каждой стороне. [4]

К шифрам, используемым для криптографической защиты информации, предъявляется ряд следующих требований:

1. Зашифрованный текст должен поддаваться чтению только при наличии секретного ключа шифрования.

2. Закон Керхоффа – знание алгоритма шифрования не должно влиять на надёжность защиты, стойкость шифра должна определяться только секретностью ключа.

3. При знании криптоаналитиком шифротекста и соответствующего ему открытого текста для нахождения ключа шифрования необходим полный перебор ключей (невозможность криптоаналитической атаки по открытому тексту).

4. Незначительное изменение ключа шифрования или открытого текста должно приводить к существенному изменению вида шифротекста.

5. Алгоритм шифрования должен допускать как программную, так и аппаратную реализацию. [6]

Литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. – Самара: СГАСУ, 2014.

2. Саймон Сингх: Книга шифров. Тайная история шифров и их расшифровки: Москва, 2007

3. Криптографические методы и средства защиты информации. Режим доступа : http://itsphera.ru/it/cryptographic-methods-and-tools-for-information-protection.html

4. Прохорова, О.В. Информационная безопасность и защита информации: учеб. пособие / О.В. Прохорова. – Самара: СГАСУ, 2014. – 114 с.

5. Корячко, В.П. Информатика и информационные технологии в профессиональной деятельности: учеб. пособие / Корячко В.П., Купцова М.И. – Рязань. – 2016.

6. Основы криптографии / А. П. Алферов [и др.]. – М: Гелиос АРВ, 2002. – С. 93.

Криптовалюта – что это такое. Виды криптовалют. Криптовалютные кошельки. Главные угрозы для криптовалют, способы атаки на криптовалюту. Способы защиты криптовалют

Пилецкая Е.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

С появлением интернета стали популярны и платежи в сети – таким образом, появились самые различные электронные валюты (Яндекс.Деньги, WebMoney и другие). В 2009 году аноним Сатоши Никамото представил на суд общественности своё решение: выпустил информационную валюту «Биткоин», которую предложил использовать в качестве средства обмена. Финансовые операции начали проводить лишь через два года, когда появились электронные кошельки.

За девять лет мир электронных денег настолько разросся, что уследить за действиями в нём просто нереально. Назвать точную цифру просто невозможно, потому, что каждый день появляются новые виды цифровых денег.

Криптовалюта – это один из видов цифровой валюты, электронных денег. Но в отличие от традиционных систем, где все данные хранятся на централизованном сервере, криптовалюты децентрализованы. Все криптовалюты основаны на криптографии: очень надёжных механизмах шифрования. Взломать такую систему практически невозможно.Стоимость той или иной криптовалюты определяется спросом и предложением на рынке.

Криптовалюта храниться в *криптовалютных кошельках* – это программа, позволяющая отправлять и получать криптовалюту. Кошельки используются для хранения секретных ключей – это длинные шестнадцатеричные коды, известные только вам и кошельку.Кошельки бывают разными. Это может быть устройство, которое подключается к Интернету лишь время от времени, для выполнения транзакций (в