АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К КЛАССИФИКАЦИИ МЕТОДОВ ШИФРОВАНИЯ

Алефиренко Виктор Михайлович,
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

E-mail: alefirenko@bsuir.by

Ефремова Александра Юрьевна,
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

E-mail: al617e13@gmail.com

Асиненко Алексей Михайлович,
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

E-mail: asinenko2016@mail.ru

Аннотация. Статья посвящена систематизации существующих методов криптографической защиты информации. Рассмотрены основные методы шифрования, используемые алгоритмы и их принцип работы. Описаны варианты применения методов шифрования, их достоинства и недостатки. Показано различие между классическими методами и квантовым шифрованием.

Ключевые слова: шифрование, криптографические алгоритмы, классификация методов.

Наряду с аппаратными методами защиты информации от несанкционированного использования, в инфокоммуникационных технологиях активно используются криптографические методы, основанные на шифровании данных.

Шифрование – это совокупность методов, используемых для защиты информации от несанкционированного доступа путем преобразования исходных данных в другой их вид, который можно прочитать с помощью соответствующего ключа дешифрования [1].

В шифровании информацию разделяют на «открытый текст», означающий, что информация представлена в первоначальном виде, и «зашифрованный текст», обозначающий уже зашифрованную информацию. Существуют различные методы шифрования, используемые для защиты данных, хранящихся на устройстве или отправляемых по сети [2].

Методы шифрования могут классифицироваться по различным признакам: по типу ключа, по типу данных, по способу применения и по алгоритму (рисунок 1).

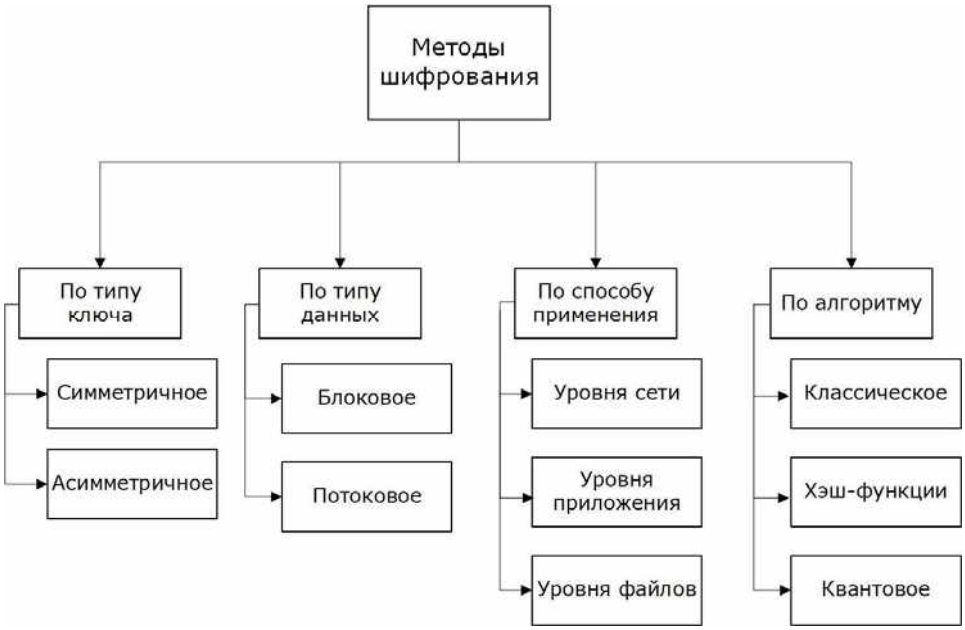

Рис. 1 Классификация методов шифрования

Первый параметр, на основе которого классифицируют методы шифрования – это тип ключа. Криптографические ключи являются центральными элементами операций шифрования и дешифрования.

Ключ – это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из всей совокупности возможных вариантов для данного алгоритма. По типу ключа шифрование делится на симметричное и ассиметричное [3, 4].

Симметричное шифрование является фундаментальным методом, в котором для преобразования информации используется один и тот же ключ. Наиболее распространенными алгоритмами симметричного шифрования принято называть *DES* (относительно устаревший, использует ключ в 56 бит), *Triple DES* (улучшенная версия *DES*, использующая три итерации шифрования), *AES* (более безопасный по сравнению с *Triple DES*, поддерживает длины ключей в 128, 192 и 256 бит).

Среди преимуществ симметричного шифрования выделяют скорость и простоту. Данный метод позволяет быстрее обрабатывать большие объемы данных, а также требует меньше вычислительных ресурсов.

К недостаткам метода относят уязвимость, так как безопасность симметричного шифрования зависит от секретного ключа, скомпилировав который, можно дешифровать данные.

Однако несмотря на относительно невысокий уровень безопасности, симметричное шифрование широко используется в различных приложениях, например, для защиты файлов и данных на жестких дисках (*BitLocker*), передачу данных через защищенные каналы (*SSL/TLS*), а также для шифрования *VPN* соединений.

Асимметричное шифрование – это более сложный метод шифрования, который использует два ключа: открытый (публичный) и закрытый (приватный). Использование двух ключей обеспечивает высокий уровень безопасности, а также является основой многих современных систем. Открытый ключ используется для шифрования данных и находится в открытом доступе для пользователей, отправляющих зашифрованное сообщение. Закрытый ключ используется для расшифровки полученных данных и известен только владельцу.

К наиболее используемым алгоритмам ассиметричного шифрования относят *RSA* (алгоритм, основывающийся на факторизации больших простых чисел) и *ECC* (алгоритм, предлагающий аналогичную безопасность с меньшим размером ключа (256 бит) по сравнению с предыдущим, что делает его более эффективным) [2; 3].

К преимуществам асимметричного шифрования относят простоту реализации ввиду отсутствия необходимости передачи секретного ключа, что снижает риск его компрометации, а также высокую степень защищенности.

Значительными недостатками рассматриваемого метода шифрования принято считать низкую скорость по сравнению с симметричным ввиду необходимости выполнения более сложных математических операций, а также то, что метод не подходит для шифрования больших объемов данных. Высокий уровень безопасности позволяет применять ассиметричное шифрование во многих сферах. Например, шифрование используют для создания и проверки цифровых подписей, которые подтверждают подлинность сообщений.

Ассиметричное шифрование применяют также и в протоколах передачи данных, таких как *SSL/TLS*, для защиты информации, передаваемой в Интернете. Еще одной сферой использования является обеспечение безопасности транзакций криптовалюты.

По типу данных методы шифрования классифицируют на блочное и потоковое [5].

Блочное шифрование – это метод шифрования, основывающийся на разделении информации на блоки фиксированного размера, обычно, от 32 до 128 бит, которые, в следствие преобразования с использованием ключа, обрабатываются по несколько байт за одну итерацию.

Преобразование проходит по принципам рассеивания и перемешивания. Рассеивание, изменяя знаки незашифрованной информации или ключа, позволяет скрыть статистические свойства «открытого текста». Перемешивание путем различных преобразований затрудняет получение статистических зависимостей между шифром и «открытым текстом».

Существуют различные алгоритмы, которые используются в блочном шифровании, такие как *AES* (алгоритм, используемый в правительственных учреждениях и для защиты коммерческих данных при помощи ключей размером 128, 192 и 256 бит), *3DES* (улучшенная версия алгоритма *DES*, использующая три ключа шифрования) и *Blowfish*: (алгоритм, использующий ключи от 32 до 448 бит).

Блочное шифрование широко применяется для защиты конфиденциальной информации, такой как пароли и номера кредитных карт, а также в протоколах шифрования, таких как *SSL/TLS* для обеспечения защищенного обмена данными в интернете.

Среди достоинств блочного шифрования часто выделяют: скорость шифрования, стандартизацию, высокий уровень безопасности, гибкость, а также возможность сжатия данных.

К недостаткам обычно относят необходимость придерживаться размеров блока, уязвимость к паттернам, необходимость управлять ключами, а также низкая скорость обработки данных ввиду зависимости между блоками.

Потоковое шифрование – это метод шифрования данных, при котором информация шифруется поочередно и последовательно одним битом или байтом за раз. Для шифрования используется ключ, который может оставаться статичным или изменяться в процессе шифрования.

Существуют различные алгоритмы для реализации потокового шифрования, например, *Salsa20* и *ChaCha* (параллельные потоковые шифры, которые обеспечивают высокий уровень безопасности и производительности).

Принцип потокового шифрования можно описать следующим образом: генератор случайных чисел выдает числовые последовательности, последняя из которых накладывается на шифруемую информацию с применением операции «исключающее ИЛИ», что приводит к получению уже зашифрованных данных [5].

К преимуществам потокового шифрования часто относят возможность работать с данными переменной длины, эффективность, а также малую задержку.

Среди недостатков выделяют уязвимость метода и сложности управления ключом.

Несмотря на уязвимость, метод применяется в таких протоколах как *SSL/TLS, SSH*, а также в обеспечении безопасности при обмене сообщениями.

По способу применения шифрование разделяют на шифрование на уровне сети, шифрование на уровне приложений и шифрование файлов [4]. Шифрование на уровне сети выполняет функции защиты данных, передаваемых по сети, шифрование на уровне приложения – защиты данных приложений, шифрование файлов – защиты файлов или папок.

По алгоритму шифрование разделяют на классическое, шифрование с использованием хэш-функций и квантовое [6].

Классическое шифрование – это совокупность методов шифрования, имеющая простую математическую структуру и основанная на понятиях замены и перестановки данных [1-4].

В основе классического шифрования заложены методы, которые использовались еще до появления современных компьютерных алгоритмов. Среди таких шифров можно выделить шифр Цезаря (метод заключается в сдвиге алфавита на фиксированное число позиций), шифр Виженера (метод, в котором применяется ключевое слово для управления сдвигами), шифр *Playfair* (шифр, использующий квадрат символов 5x5 для шифрования биграмм), шифр транспозиции (шифр, использующий перестановку символов в тексте согласно определенной схеме, не изменяя сами символы), а также уже известное шифрование с использованием ключей.

Хэш-функции представляют собой совокупность математических функций, преобразующих входные данные произвольной длины в данные фиксированного размера. Хэш-функции обычно работают следующим образом: пользователь подает данные некоторой длины, после чего хэш- функция обрабатывает их с помощью математических и логических операций, в результате чего данные преобразуются в строку фиксированной длины, представленную в виде шестнадцатеричного или двоичного формата.

Существует множество хэш функций, например, *MD*5 (создает 128-битный (16 байт) хэш), *SHA*-1 (функция, создающая 160-битный (20 байт) хэш, является более надежной, чем предыдущая), *SHA*-256 (широко используемая функция, принадлежащая к семейству *SHA*-2, создает 256- битный хэш), *SHA*-3 (функция, использующая алгоритм *Keccak* с более высоким уровнем безопасности) [6].

Среди преимуществ хэш-функций обычно выделяют фиксированность длины выходных данных (например, *A*-256 всегда генерирует хэш длиной 256 бит), скорость обработки данных, невозможность восстановить исходные данных из хэша, легкость реализации, а также необратимость.

К недостаткам хэш-функций обычно относят возможность возникновения большого количества коллизий, уязвимость к атакам с радужной таблицы, необходимость контроля за целостностью данных и низкая скорость вычислений при обработке большого количества данных.

Высокий уровень надежности хэш-функций сделал их широко используемыми в различных направлениях защиты информации. Так, например, хэш-функции используются при шифровании цифровых подписей, проверке целостности файлов, в качестве альтернативы хранения паролей, а также для обеспечения безопасности в работе с базами данных.

Квантовое шифрование – это метод шифрования, основанный на использовании квантовых битов для передачи и защиты информации, что обеспечивает высокий уровень безопасности.

Для квантового шифрования характерны следующие принципы: квантовая суперпозиция (квантовый бит может находиться не только в состоянии 0 или 1, но и в комбинированном), принцип неопределенности (при изменении состояния бита, его значение изменяется) и квантовая запутанность (состояния квантовых битов влияют друг на друга даже на большом расстоянии).

Для осуществления квантового шифрования существуют различные протоколы, например, *BB84*, который использует четыре состояния поляризации фотонов для передачи информации, что приводит к их изменению в случае, если злоумышленник попытается их измерить, и *E91*, основывающийся на использовании запутанных пар частиц и их измерении для создания секретного ключа.

К преимуществам квантового шифрования обычно относят высокий уровень безопасности, возможность обнаружения злоумышленных действий при попытке перехватить сообщение, а также возможность создавать более сложные ключи шифрования.

Среди недостатков квантового шифрования отмечают необходимость использования сложного оборудования и технологий, трудности при передаче данных на большие расстоянии и подверженность влиянию внешних факторов [7].

Таким образом, можно отметить, что на сегодняшний день существуют различные методы шифрования, которые можно классифицировать по различным признакам, однако наиболее подходящий метод может быть выбран только исходя из конкретной поставленной задачи по защите информации в том или ином канале ее передачи.

Литература:

1. Шифрование и расшифровка данных [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru/windows/win32/seccrypto/data-encryption-and-decryption

2. Криптоалгоритмы [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/336578/

3. Криптографические ключи [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru/windows/win32/seccrypto/cryptographic-keys

4. Бернет С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М. Бином-Пресс, 2002. –384 с.

5. Отличия блочных шифров от потоковых [Электронный ресурс]. – Режим доступа: https://chinapads.ru/c/s/potochnyiy_shifrosnovnyie_otlichiya_potochnyih_shifrov_ot_blochnyih

6. О повышении криптостойкости однонаправленных хеш-функций / В.Ю. Левин // Фундаментальная и прикладная математика. – 2009. – Т. 15, № 5. – С. 171-179.

7. Квантовая криптография [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/530362/