УДК 003.26.09

Канкулов А.М.
студент
Кабардино-Балкарский государственный университет,
Россия, г. Нальчик
Научный руководитель: Казиев В.М., кандидат физико-математических наук
доцент Кабардино-Балкарского государственного университета,
Россия, г. Нальчик

КРИПТОГРАФИЯ: ХЕШИ И ХЕШИРОВАНИЕ

Аннотация. *В статье рассмотрены основы истории и алгоритмов криптографии, в частности, способы шифрования и дешифрования данных. Приведены основные функции защиты информации, конфиденциальности и контроля целостности информации в условиях построения цифровой экономики.*

Ключевые слова: *криптография, шифрование, дешифрование, ключ.*

Annotation. *The article discusses of the history basics and cryptography algorithms of encryption and decryption. The functions of information protection, confidentiality and information integrity control in the context of building a digital economy are considered.*

Key words: *cryptography, encryption, decryption, key.*

Актуальность работы заключается в новых, повышенных требованиях криптозащищенности систем цифровой экономики, цифрового бизнеса и повышении сложности и изощренности атак на такие системы. В частности, по итогам 2018 года «Лаборатория Касперского» отметила снижение общего количества DDoS-атак на 13% по сравнению со статистикой за предыдущий месяц [1].

Объект исследования – криптосистемы, криптоалгоритмы, защищенность систем.

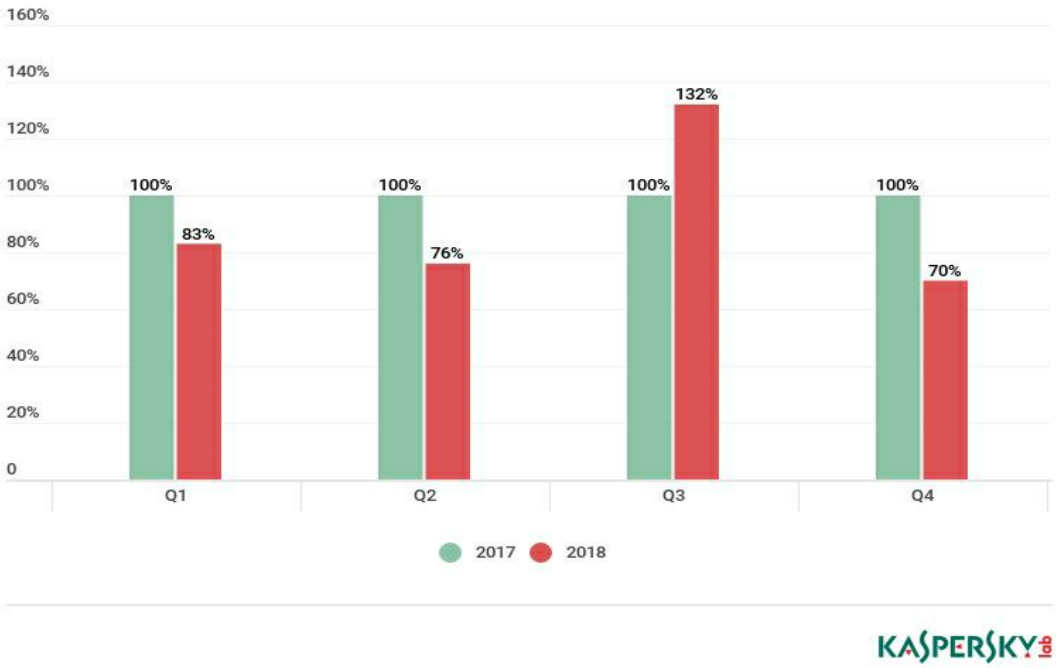

Рис.1. Поквартальное сравнение количества DDoS-атак в 2017–2018 гг. (за 100% принято количество атак в 2017 г.)

Криптография – «наука секретного письма», древнее искусство. Первое документированное использование криптографии в письменной форме относится к Египту 1900 года до нашей эры. Некоторые эксперты утверждают, что криптография появилась спонтанно после того, как была изобретена письменность, начиная от дипломатических посылок и заканчивая военными планами сражений. Поэтому неудивительно, что новые формы криптографии появились вскоре после повсеместного развития компьютерных коммуникаций.

Основными функциями криптографии являются обеспечение нижеследующих свойств, механизмов.

1. Конфиденциальность – обеспечение того, чтобы никто не мог прочитать сообщение, кроме предполагаемого получателя.
2. Аутентификация – процесс подтверждения личности.
3. Целостность – заверение получателя в том, что полученное сообщение никак не изменилось по сравнению с оригиналом.

4. Безотказность – механизм, позволяющий доказать, что отправитель действительно отправил это сообщение.
5. Обмен ключами – метод, с помощью которого криптографические ключи распределяются между отправителем и получателем.

Существует несколько способов классификации криптографических алгоритмов. Для целей данной работы они будут классифицированы на основе количества ключей, которые используются для шифрования и дешифрования, и далее определяются их применением и использованием. Рассмотрим три типа алгоритмов:

- криптография с секретным ключом (SKC), которая использует один ключ для шифрования и дешифрования; также называется симметричным шифрованием, используется больше для конфиденциальности;
- криптография с открытым ключом (PKC), использует один ключ для шифрования и другой для дешифрования; также называется асимметричным шифрованием и используется чаще для аутентификации, анонимности и обмена ключами;
- хеширование, использование хэш-функций, математических преобразований для «необратимого» (относительно получателя, например) шифрования информации, используется обычно для обеспечения целостности сообщений.

Симметричное шифрование – алгоритм, при котором для шифрования и дешифрования используется один и тот же ключ. Ассиметричное шифрование – алгоритм, при котором используются два ключа: открытый (для шифрования) и закрытый (для дешифрования).

Распространенные криптоалгоритмы – RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptosystem), DH (Diffie-Hellman), El Gamal.

Хэш-функция или процесс хеширования – алгоритм, вычисляющий хеш-значение фиксированной длины на основе открытого текста, что делает невозможным восстановление содержимого (длины) открытого текста. Хеш-

алгоритмы обычно используются для предоставления цифрового отпечатка содержимого файла, паролей, гарантии того, что файл не был изменен злоумышленником или вирусом. Таким образом, хэш-функции предоставляют механизм для обеспечения целостности файла, функция, которая превращает входные данные большого файла в данные фиксированного размера и оптимизирует таблицы, базы данных, поиск в них. Если входные данные неизвестны, весьма трудно восстановить входное значение или эквивалентную альтернативу, зная сохраненное значение хеш-функции.

Длина хеш-функции обычно от 128 бит, что достаточно, чтобы для случайного поиска двух документов A и B, имеющих одинаковое значение хеширования, потребуется осуществить хеширование 2^{64} документов. Для устойчивости против нападения, неуязвимости допустимая длина хеш-функции определяется с учетом прогноза развития средств криптоанализа.

Хеширование – алгоритмически генерирует бит-строку задаваемой длины, результат называется свёрткой. Алгоритмов – много, они различаются по длине (разрядности), устойчивости (стойкости к взлому). Например, 128-битное хеширование данного текста в шестнадцатеричном виде даст на выходе шестнадцатеричные сообщения типа: «c4ca4238b0b923920dcc519a6f65849c». Если изменить в тексте знак, результат хеширования полностью изменится, что важно для сохранения-восстановления, защиты паролей, ЭЦП и др.

У вход-выхода нет устойчивой связи (известный принцип Дирихле). Когда хеш-функция сводит одинаковые сообщения в одинаковые свертки, это – коллизия (столкновение). Вероятность коллизий – оценка качественности хеширования. «Качественное» генерирует коллизий минимум. Например, функция поиска по модулю 2 остатка от деления входного потока на полином с хеш-кодом из значений коэффициентов остатка.

Безопасность часто отдают на аутсорсинг, как непрофильную работу (бизнес-процедуру) небольшой компании экономящей финансово-информационные ресурсы. Здесь важно уметь оценивать сложность и

ресурсоемкость процессов на аутсорсинг. Если аутсорсинг и увеличивает «короткие» расходы, затем обязательно снизит «длинные». Аутсорсер несет ответственность за полноту своих услуг, за работу.

Если аутсорсер, при стоимости i-го процесса $s^{(i)}$ наблюдения, сможет составить матрицу вероятностей уязвимостей, нарушений вида

$$P^{(m)} = \left\| p_{ij}^{(m)} \right\|, \qquad i,j = 1,2,\dots,n; \;\; m = 1,2,\dots,M,$$

то используя ее можно выстраивать стратегию защиты. Определив стратегию защиты, аудита можно приступить к ее комплексному обеспечению с помощью аутсорсинга.

Приводим статистическую обработку (табл. 1) и гистограмму по компьютерным преступлениям в РФ за последнее время (рис. 2).

Таблица 1. Статистика по компьютерным преступлениям за 2000-2019 гг.

Регрессионная статистика	
Множественный R	0,76586366
R-квадрат	0,58654715
Нормированный R-квадрат	0,56357755
Стандартная ошибка	3,90829705
Количество наблюдений	20

Рис.2. Гистограмма компьютерных преступлений за 2000-2019 гг. (данные 2019 года приведены за 8 месяцев).

Библиографический список

1. Лаборатория Касперского. Отчёты по DDoS-атакам. DDoS-атаки в четвертом квартале 2018 года. [Электронный ресурс]. URL: https://securelist.ru/ddos-attacks-in-q4-2018/93384/.
2. Адаменко, М. Основы классической криптологии. Секреты шифров и кодов // Михаил Адаменко. – Москва: Машиностроение, 2014. – 256 с.
3. Даниленко, А. Ю. Безопасность систем электронного документооборота. Технология защиты электронных документов // А. Ю. Даниленко. – М.: Ленанд, 2015. – 232 с.
4. Здор, С. Е. Кодированная информация. От первых природных кодов до искусственного интеллекта // С. Е. Здор. - М.: Либроком, 2012. – 168 с.