Из табл. следует, что численные значения верхней граничной частоты полосы пропускания АЧХ $f_В$ и времени нарастания ПХ $\tau_н$, найденные экспериментально, согласуются друг с другом согласно известному соотношению ($f_В \approx 350/\tau_н$, где частота $f_В$ выражена в мегагерцах, а время $\tau_н$ – в наносекундах). Измерение емкости с применением матричного коммутатора целесообразно вести на частотах до 100 кГц.

Представленный матричный модуль коммутации разработан для автоматизированного измерительного комплекса в рамках ГНТП «Эталоны и научные приборы» [1].

Литература

1. Лисенков, Б. Н. Измерительный комплекс на основе матричного коммутатора / Б. Н. Лисенков, Н. В. Грицев // Приборостроение-2019 : матерериалы 12 международной науч.-техн. конф., 18–20 ноября 2019 г., Минск, Белорус. нац. техн. ун-т / редкол. : О. К. Гусев [и др.]. – Минск : БНТУ, 2019. – С. 46–47.

2. Лисенков, Б. Н. Проверка метрологических характеристик матричного коммутатора / Б. Н. Лисенков, Н. В. Грицев, А. А. Бруек // Опто-, микро- и СВЧ-электроника – 2018 : сборник научных статей Первой международной науч.-техн. конф. – Минск, 2018. – С. 82–85.

УДК 004.056.5

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ РАСШИРЕННОГО АЛГОРИТМА ОБМЕНА КЛЮЧАМИ В СРЕДСТВАХ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Марченков С.Д., Лебедев А.Н.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. Представлен расширенный алгоритм обмена ключами со строгой аутентификацией сторон на основе алгоритма Диффи–Хэллмана с заменой операций в конечном коммутативном кольце. Основное внимание уделяется введенной арифметической операции и методу доставки ключевых параметров взаимодействующим сторонам. Рассмотрено возможное применение алгоритма в информационных системах, использующих открытый канал связи и средства криптографической защиты информации.
Ключевые слова: конечное поле, конечное коммутативное кольцо, криптография, протокол Диффи–Хеллмана, рассылка защищенных данных, аутентификация.

PERSPECTIVES OF EXTENDED KEY EXCHANGE ALGORITHM IN CRYPTOGRAPHIC SECURITY TOOLS

Marchenkov S., Lebedev A.

Bauman Moscow State Technical University
Moskow, Russia

Abstract. The extended key exchange algorithm with strong side authentication based on the Diffie-Hellman algorithm with replacement of operations in a finite commutative ring is presented. Arithmetic operation and the way of passing key parameters to the interacting parties are analyzed. The possibilities of using the algorithm in information systems using an open communication channel and cryptographic tools for information protection are considered.
Key words: finite field, finite ring, cryptography, Diffie-Hellman protocol, authentication, secured data distribution.

Адрес для переписки: Марченков С.Д., Россия, Москва, ул. 2-я Бауманская, 5, г. Москва 105005, Россия
e-mail: marchenkovsd@student.bmstu.ru

Чтобы гарантировать целостность и конфиденциальность информации при обмене данными между двумя абонентами сети используются гибридные системы, в которых применяются алгоритмы ассиметричного шифрования для выработки секретного ключа и последующего симметричного шифрования непосредственно конфиденциальных данных. Протоколы такого типа используют алгоритмы обмена ключами для установления безопасного канала передачи данных. Для обмена ключами и проверки их подлинности в настоящее время используются комбинации алгоритмов, основанные на модификации классического алгоритма Диффи–Хеллмана [1].

Протокол. В статье [2] была предложена модель передачи зашифрованных данных с доступом легитимного пользователя в определенный период времени. При этом ключевые параметры необходимо хранить на защищенных аппаратных носителях информации.

Предполагается использование схемы протокола, приведенного далее, где S – сервер, U – клиент, M – открытый текст, C – шифртекст, E – операция шифрования, D – операция расшифрования.

Подготовительный этап. Сторона *S* выбирает основание p, по модулю которого будут производиться операции, выбирает m и k, причем $m, k \in \{1, 2 \ldots p-1\}$.

$$Ks_{priv} = Ks_{rand} + \frac{k}{m} = Ks_{rand} + (km^{-1}), \quad (1)$$

где Ks_{rand} – случайное число, 2048 бит [3].

Также необходимо, чтобы НОД(m, p) = 1. Числа m, k записываются в защищенную память обоих абонентов заранее.

Этап выработки ключей. Защищенный файл на носителе информации передан получателю, с этого момента сторона *U* может сгенерировать свой секретный ключ.

$$Ku_{priv} = Ku_{rand} + \frac{k}{m} = Ku_{rand} + (km^{-1}). \quad (2)$$

U обращается к *S* через TCP соединение. *S* посылает *U* данные g и p, тем самым обозначая, что он активен и готов к обменуы.

$$S \rightarrow U: Ku_{pub} = g^{Ku_{priv}} \bmod p = \\ = g^{Ku_{rand}+(km^{-1})} \bmod p. \quad (3)$$

U вырабатывает открытый ключ.

$$S \leftarrow U: Ku_{pub} = g^{Ku_{priv}} \bmod p = \\ = g^{Ku_{rand}+(km^{-1})} \bmod p. \quad (4)$$

S вырабатывает сессионный ключ.

$$S: K_{sess} = \left(Ku_{pub}\right)^{Ks_{priv}} = \left(g^{Ku_{priv}}\right)^{Ks_{priv}}. \quad (5)$$

$$K_{sess} = \frac{\left(Ku_{pub}\right)^{mKs_{priv}}}{g^{km^{-1}}} \bmod p = \\ = \frac{g^{m[Ku_{rand}+(km^{-1})][Ks_{rand}+(km^{-1})]}}{g^{km^{-1}}}. \quad (6)$$

Этап шифрования. *S* зашифровывает сообщение на сессионном ключе K_{sess} и отправляет получателю *U*.

$$S \rightarrow U: C = E_{K_{sess}}(M). \quad (7)$$

При наступлении определенного условия, например, определенного времени, происходит следующий обмен:

$$S \rightarrow U: Ks_{pub} = g^{Ks_{priv}}. \quad (8)$$

$$U: K_{sess} = \left(g^{Ku_{priv}}\right)^{Ks_{priv}}. \quad (9)$$

$$U: M = D_{K_{sess}}(C). \quad (10)$$

Введенные операции. Описанная схема имеет смысл, если введенные операции (11) и (12), предложенные в [4, 5], удовлетворяют аксиомам поля:

$$x \oplus y = (x + k/m) + (y + k/m) - k/m, \quad (11)$$

$$x \otimes y = m(x + k/m)(y + k/m) - k/m. \quad (12)$$

Доказательство коммутативности аддитивной операций приведено на формуле (13):

$$x \oplus y = x + y + k/m = y + x + k/m = y \oplus x. \quad (13)$$

Коммутативность мультипликативной операций в соответствии с формулой (14):

$$x \otimes y = m(x + k/m)(y + k/m) - k/m = \\ = m(y + k/m)(x + k/m) - k/m = y \otimes x. \quad (14)$$

Для доказательства ассоциативности аддитивной операции необходимо рассмотреть левую (15) и правую (16) части равенства:

$$(x \oplus y) \oplus z = (x + y + k/m) \oplus z = \\ = (x+y+k/m+z+k/m) = x+y+z+2k/m, \quad (15)$$

$$x \oplus (y \oplus z) = x \oplus (y + z + k/m) = \\ = (x+y+z+k/m+k/m) = x+y+z+2k/m. \quad (16)$$

Ассоциативности мультипликативной операции проверяется равенством (17, 18):

$$(x \otimes y) \otimes z = [m(x + k/m)(y + k/m) - k/m] \otimes z = \\ = m^2(x + k/m)(y + k/m)(z + k/m) - k/m. \quad (17)$$

$$x \otimes (y \otimes z) = x \otimes [m(y + k/m)(z + k/m) - k/m] = \\ = m(x + k/m)m(y + k/m)(z + k/m) - k/m. \quad (18)$$

Дистрибудивность проверяется равенством уравнения $x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z$:

$$x \otimes (y \oplus z) = x \otimes (y+z+k/m) = \\ = m(x+ k/m)(y+z+ 2k/m) - k/m). \quad (19)$$

$$x \otimes y \oplus x \otimes z = [m(x+k/m)(y+ k/m)–k/m] \oplus \\ \oplus [m(x+k/m)(z+ k/m)–k/m] = \\ = m(x+ k/m)(y+z+ 2k/m) - k/m). \quad (20)$$

Нейтральным элементом относительно аддитивной операции: $(-k/m)$, обратный элемент: $(-x-2k/m)$.

Для мультипликативной операции нейтральный элемент $(1-k)/m$, нулевой элемент $(-k/m)$, обратный элемент $(1-k^2-kmx)/[\ m^2(x+k/m)]$ при условии $x \neq -k/m$.

Практическое применение. Приведенный алгоритм может быть использован в средствах криптографической защиты информации предназначеных для хранения закрытых ключей в защищенной памяти устройства, такими устройствами на данный момент являются токены выполненные в форм-факторе флеш-накопителей и взаимодейтсвующих с программным обеспечением.

Примером такого токена является JaCarta PKI, который имеет удобный SDK для использования в сторонних проектах, носитель содержит энергонезависимую память, разделенную на несколько отдельных областей, в которых находится информация с различной степенью защиты.

Приведем некоторые примеры, для которых может подойти данное программно-аппаратное средство:

1. Экзаминация обучающихся для передачи отдельных пакетов данных с материалами для прохождения аттестации с расшифрованием данных в назначенное время.

2. Обновление лицензии программного обеспечения без необходимости пересылки идентификатора лицензии в открытом виде или трудоемкой повторной доставке данной информации.

Данные варианты подразумевают пересылку по открытому каналу передачи данных определенного количества файлов соответствующего количеству ключей, хранящихся на токене, для последующего последовательного их расшифрования.

Вывод. За счет предварительного распространения ключевых параметров *m, k* обеих сторон обеспечивается аутентификация ключей, случайный выбор *x* и *y* гарантирует, что обе стороны могут быть уверены в создании нового сессионного ключа в каждом сеансе протокола [6].

Реализация протокола с применением криптографических токенов является наглядной и понятной схемой для конечного пользователя.

Литература

1. Diffie, W. New Directions in Cryptography / W. Diffie, M. Hellman // IEEE Transactions on Information Theory. – 1976. – Vol. 22, № 6. – P. 644–654.

2. Лебедев, А. Н. Способ рассылки защищенных данных с регулированием доступа к отдельным их разделам / А. Н. Лебедев // Вопросы кибербезопасности. – 2015. – Т. 13, № 5. – С. 70–72.

3. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. NIST. – [Электронный ресурс]. Режим доступа: https://nvlpubs.nist.gov. – Дата доступа: 21.04.2021.

4. Лебедев, А. Н. Обобщенный протокол Диффи-Хеллмана с аутентификацией сторон / А. Н. Лебедев // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша. – М. : МГУ, 2018. – С. 123–127.

5. Лебедев, А. Н. Новые арифметические операции конечного коммутативного кольца и их использование в криптографии / А. Н. Лебедев // Безопасные информационные технологии : сборник трудов IX Всероссийской научно-технической конференции. – Москва, 2018. – 8 с.

6. Matsumoto, T. On seeking smart publickey-distribution systems / T. Matsumoto, Y. Takashima, H. Imai // Trans. Inst. Electron. Commun. Eng. Jpn. Sect. E. – 1986. – Vol. 69,№ 2. – P. 99–106.

УДК 004.056

ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЛЕКСА БОРТОВОГО ОБОРУДОВАНИЯ ГРАЖДАНСКОГО ВОЗДУШНОГО СУДНА НА БАЗЕ ОТКРЫТОЙ СЕТЕВОЙ АРХИТЕКТУРЫ

Медведев Н.В.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. Предлагаются принципы построения защищенного комплекса управления гражданского воздушного судна, основанные на трех информационных доменах и открытой сетевой структуре.
Ключевые слова: гражданское воздушное судно, информационный домен, защищенный сервер, единая информационно-вычислительная платформа, комплекс.

CONSTRUCTION PRINCIPLES OF A CIVIL AIRCRAFT COMPLEX BASED ON OPEN NETWORK ARCHITECTURE

Medvedev N.

Bauman State Technical University
Moscow, Russia

Abstract. The principles of building a secure civil aircraft control complex based on three information domains and an open network structure are proposed.
Key words: civil aircraft, information domain, secure server, unified information and computing platform, complex.
Адрес для переписки: Медведев Н.В., ул. Вторая Бауманская, 5, г. Москва 105005, Российская Федерация
e-mail: medvedevnick54@yandex.ru

Современные распределенный и интегрированный принципы построения комплекса бортового оборудования гражданского воздушного судна (БО ГВС) на базе открытой сетевой архитектуры и единой информационно-вычислительной платформы обусловили повышение степени внутренней информационной связности ГВС [1]. Это существенно повысило степень внешней информационной связности ГВС и привело к появлению концепции информационного связанного (E-enabled) ВС с поддержкой внешних сервисов, как показано на рис. 1 [2].

Связанным воздушным судам необходимо быть самостоятельными узлами в Авиационных самоорганизующихся сетях (AANET), повсеместно общаясь с наземной инфраструктурой и други-