Иван В. Нечта
Сибирский государственный университет телекоммуникаций и информатики,
ул. Кирова, 86, г. Новосибирск, 630102, Россия
e-mail: ivannechta@gmail.com, http://orcid.org/0000-0003-0361-2742

КРИПТОГРАФИЧЕСКАЯ СХЕМА РАССЫЛКИ ГРУППОВЫХ ПАРОЛЕЙ ДЛЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

DOI: http://dx.doi.org/10.26583/bit.2019.1.09

Аннотация. В настоящей работе предложена новая схема передачи паролей для групп пользователей по скрытому каналу связи. Известные ранее модели в явном виде демонстрировали наличие паролей и не могут быть использованы в тайном канале связи. Рассматриваемая модель обмена сообщениями предполагает наличие координатора, регулирующего состав групп и являющегося источником подавляющей доли сообщений. Состав групп заранее не известен и может меняться в процессе передачи сообщений. Предполагается, что передаваемые в контейнере данные будут состоять из двух частей: служебной части, в которой передаются сведения о составах групп и паролях, и полезной части, в которой находится целевое сообщение, зашифрованное групповым паролем. Схема базируется на теореме Кронекера-Капелли. Для нахождения группового пароля абонент-приемник, входящий в группу, находит произведение корней совместной системы линейных алгебраических уравнений. Указанная система состоит из $\boldsymbol{n}$ уравнений и содержит $\boldsymbol{n+1}$ неизвестную. Для стороннего абонента, не входящего в группу, система уравнений не имеет единственного решения. Абонент, входящий в группу, способен вычислить одну неизвестную по заранее определенной формуле. Следовательно, система уравнений для такого абонента имеет единственное решение. В статье описан процесс изменения состава групп абонентов: создание, добавление участника, удаление. Удаление пользователей из группы реализовано через переобъединение старых участников группы. Схема предусматривает возможность объединения созданных ранее подгрупп в большие группы без существенных накладных расходов. Предлагаемая схема может быть использована на практике некоторой организацией для управления своими филиалами при связи по скрытым каналам передачи данных.
Ключевые слова: групповые пароли, стеганография, криптография.
Для цитирования: НЕЧТА, Иван В. КРИПТОГРАФИЧЕСКАЯ СХЕМА РАССЫЛКИ ГРУППОВЫХ ПАРОЛЕЙ ДЛЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ. Безопасность информационных технологий, [S.l.], p. 87-97, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1184>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.09.

Ivan V. Nechta
Siberian state university of telecommunications and information sciences,
Kirova st., 86, Novosibirsk, 630102, Russia
e-mail: ivannechta@gmail.com, http://orcid.org/0000-0003-0361-2742

Cryptographic scheme for group passwords distribution in steganographic systems

DOI: http://dx.doi.org/10.26583/bit.2019.1.09

Abstract. This paper proposes a new scheme of passwords distribution for user groups via a hidden communication channel. The previously known models explicitly demonstrated the presence of passwords and cannot be used in any hidden communication channel. The considered model assumes the presence of a coordinator who regulates the composition of the groups and is the source of the overwhelming proportion of messages. The composition of the groups is not known in advance and may change during transmission messages. It is assumed that the data transmitted in a container will consist of two parts: a service part, which contains information about groups and passwords, and a useful part, which contains the target message that encrypted with a group-password. The scheme is based on the Kronecker-Capelli theorem. To find a group password the subscriber-receiver, is included in the group, calculates the product of the roots of a joint system of linear algebraic equations. This system consists of $\boldsymbol{n}$ equations and contains $\boldsymbol{n+1}$variables. For an outside subscriber, who is not included in the group, the system of equations has not a single solution. A subscriber in the group is able to calculate one variable by a predefined formula. Consequently, the system of equations for such subscriber has the unique solution. The paper describes the processes of changing a composition of groups: creating, adding a

participant, removing. The removing users from a group is realized by reuniting members of the old group. The scheme provides the possibility of combining previously created subgroups into large group without significant overhead costs. The proposed scheme can be used in practice by some organization to manage its branches when communicating via hidden data transmission channels.
Keywords: group passwords, steganography, cryptography.
For citation: NECHTA, Ivan V. Cryptographic scheme for group passwords distribution in steganographic systems. IT Security (Russia), [S.l.], p. 87-97, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1184>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.09.

Введение

При выборе абонентами каналов связи для передачи данных, представляющих коммерческое значение, большое внимание уделяют вопросам информационной безопасности. В ряде случаев достаточно ограничения доступа к данным с помощью некоторого секретного ключа. Такая задача может быть успешно решена при помощи методов криптографии.

Классическая задача криптографии, сформулированная в работах [1, 2], предполагает двух участников обмена сообщениями: Алису и Боба. В частности, в теории криптографии главной проблемой является ограничение доступа к данным, передаваемым по открытому каналу связи с помощью некоторого секретного ключа, известного только отправителю и адресату.

При обмене сообщениями по открытому каналу связи иногда требуется скрыть сам факт передачи сообщения от третьих лиц. В частности, политика информационной безопасности организации может предписывать сокрытие резервных каналов экстренной связи. Например, при атаке отказом в обслуживании DDoS [3] на известные каналы организация может поддерживать связь со своими отделениями или филиалами по альтернативным каналам, обеспечивая таким образом живучесть системы управления.

Последняя задача может быть эффективно решена при помощи методов стеганографии [4]. Для сокрытия факта передачи секретного сообщения абонент выбирает безобидный на внешний вид (не привлекающий внимания третьих лиц) объект данных, так называемый контейнер. С помощью специальных алгоритмов абонент встраивает секретное сообщение в контейнер и передает его по открытому каналу связи. Сам факт передачи контейнера не вызывает подозрения. Свойства стеганографических алгоритмов таковы, что даже при анализе контейнера третьими лицами нельзя однозначно утверждать о наличии факта внедрения.

Следует отметить, что перед внедрением в контейнер секретное сообщение предварительно шифруют. Шифрование необходимо для того, чтобы третье лицо, способное извлечь сообщение, не смогло провести эффективный стегоанализ. В противном случае наличие осмысленного сообщения в контейнере раскрывает факт передачи секретного сообщения. Контейнер и метод встраивания подбирается таким образом, чтобы сообщение, извлеченное из пустого контейнера, было статистически неотличимо от зашифрованного сообщения (т. е. сообщения из заполненного контейнера), что обеспечивает устойчивость к анализу.

В современных методах стеганографии всегда присутствует баланс между скрытностью (вероятностью передачи данных без обнаружения) и скоростью передачи. Причем скрытность имеет первостепенное значение. Ряд методов, описанных в работах [5-7], для повышения скрытности имитируют статистические свойства пустого контейнера, используя добавление избыточности в сообщение или заполняя контейнер не полностью. Указанная стратегия всегда влечет за собой уменьшение скорости передачи информации.

Одной из важных задач, решаемых в криптографии, является обмен паролями между абонентами по открытому каналу связи. Для стеганографии данная задача также является актуальной. Решение было впервые предложено в работах У. Диффи и М. Хэллмана [8]. С

развитием сетей связи возникли методы, организующие процесс обмена секретными сообщениями с большим количеством участников.

Например, известна пороговая схема разделения секрета, предложенная в работе Шамира [9], когда секретом могут воспользоваться абоненты при наличии кворума. Рассмотрим схему более подробно. Пусть имеется группа из $\boldsymbol{n}$ пользователей, необходимо воспроизведение секрета при участии $\boldsymbol{k}$ пользователей, где $\boldsymbol{k} \leq \boldsymbol{n}$. Схема базируется на формировании полинома степени $\boldsymbol{k}$ в котором свободный член $\boldsymbol{d_0}$ является искомым секретным параметром (формула 1). Каждый участник обладает координатами точки, принадлежащей заданному полиному. В силу теоремы о существовании и единственности решения задачи алгебраической интерполяции $\boldsymbol{k}$ пользователей могут воспроизвести полином $\boldsymbol{k-1}$ порядка единственным образом и найти секретный параметр $\boldsymbol{d_0}$.

$$f(x) = d_{k-1}x^{k-1} + \ldots d_2x^2 + d_1x + d_0(modp)\,, \tag{1}$$

где $\boldsymbol{p}$ – простое число. При отсутствии кворума задача имеет множество равновероятных решении, что не позволяет реализовывать атаки на указанную схему путем прямого перебора.

В работе [10] была предложена схема разделения ключа, базирующаяся на модификации алгоритма Диффи-Хэллмана. Группа из $\boldsymbol{r}$ пользователей выбирает простые числа $\boldsymbol{p_i}$ так, чтобы $\frac{\boldsymbol{p_i-1}}{\boldsymbol{2}}$ – было нечетным и взаимно простым с другими $\boldsymbol{p_i}$. Выбор осуществляется с тем расчетом, чтобы вычисление дискретного логарифма по модулю $\boldsymbol{p_i}$ осуществлялось за приемлемое время. Затем вычисляется общий модуль $\boldsymbol{m = p_1 * p_2 *\ldots * p_r}$ и выбирается определенным образом общее число $\boldsymbol{g}$: $\mathbf{1} < g < m$. Когда абонент **A** хочет присоединиться к системе, он предоставляет свой $\boldsymbol{ID_A}$ идентифицирующий его как абонента, и получает от системы $\boldsymbol{s_A = t * log_{(g)}\left(ID_A^2\right)\left(mod\varphi(m)\right)}$, где $\boldsymbol{t}$ – случайный множитель, $\boldsymbol{\varphi}$ – функция Эйлера. Знание разложения $\boldsymbol{m}$ на простые множители позволяет (при помощи Китайской теоремы об остатках [11]) быстро вычислять дискретный логарифм.

Для отправки зашифрованного сообщения абоненту **B** используется шифрование заранее оговоренным алгоритмом и ключом $\boldsymbol{K_{AB} = (ID_B)^{2S_A}(modm)}$. Абонент **B** принимает пару $\boldsymbol{\{ID_A,}$ **шифротекст**$\}$, получает симметричный ключ шифрования $\boldsymbol{K_{BA} = (ID_A)^{2\cdot S_B} = g^{v\cdot S_B\cdot S_A} = K_{AB}(modm)}$, где $\boldsymbol{v = t^{-1}\left(mod\varphi(m)\right)}$ и расшифровывает сообщение. Схема была подвергнута критике [11] как не обеспечивающая требуемого уровеня доверия и надежности.

В научной литературе, например, в [12], встречаются более сложные схемы разделения секрета для группы абонентов, когда имеется злонамеренный участник обмена сообщениями, который пытается либо помешать воспроизведению секрета, либо получить дополнительное знание о секретных параметрах других участников.

Известно множество протоколов распределения ключей между пользователями [13-17]. Которые можно условно разделить на три типа:

- протоколы предварительного распределения ключей;
- протоколы совместной выработки ключа;
- протоколы передачи сгенерированных ключей.

Предварительное распределение ключей согласно стандарту NIST [18] и [19] может быть осуществлено при личной встрече (вручную) с помощью некоторого доверенного центра либо по выделенному защищенному каналу связи. Совместная выработка ключа осуществляется на основе динамического взаимодействия абонентов. Например, к таким относится алгоритм Диффи-Хеллмана.

Протоколы передачи сгенерированных ключей можно подразделить на два типа:

- передача с использованием симметричного шифрования, например, [20];
- передача с использованием асимметричного шифрования, например, [21, 22].

Как видно из названия, в первом случае абоненты должны иметь некоторую общую секретную информацию. Во втором случае используется пара (открытый и закрытый) ключ, как, например, в шифре RSA. В указанных алгоритмах предусмотрено противодействие разного рода атакам (подмена сообщения, злоумышленник посередине и т.д.) при помощи аутентификационных кодов сообщений, сертификатов и цифровой подписи, предусмотренных стандартами [23, 24].

В общем случае протоколы можно разделить на два класса: централизованное распределение ключей и децентрализованное. Централизованное распределение базируется на некотором доверенном центре и позволяет минимизировать объем хранимой вспомогательной информации у абонентов, необходимой для выработки общего ключа. Децентрализованное распределение эффективно применять, когда число абонентов велико и их постоянное взаимодействие с единственным доверенным центром затруднительно.

Настоящая работа посвящена усовершенствованию стеганографической информационно-технологической системы в части рассылки групповых паролей. В отличие от ранее известных схем обмена паролями, предлагаемая схема предназначена для стеганографических систем и включает присутствие координатора, являющегося источником сообщений. Разработанный алгоритм может быть с легкостью адаптирован для обычной криптографической системы, в которой отсутствует ограничение на сокрытие факта передачи секретных сообщений. Новизна предлагаемой схемы заключается в следующем. Во-первых, минимизирован обмен сообщениями между абонентами, так как в стеганографических системах любой обмен всегда несет потенциальный риск обнаружения тайного канала связи. В предлагаемой схеме, источником сообщений является только координатор Алиса. Таким образом, новая схема относится к централизованному типу схем распределения ключей и использует симметричную криптографию. Во-вторых, схема базируется на невозможности нахождения корней уравнений при недостаточном числе уравнений в отличие от ранее известных схем, которые базируются на субэкспоненциальной сложности задачи факторизации или невозможности отыскания единственного полинома степени $\boldsymbol{n}$ при известных $\boldsymbol{n+1}$ точек. Предполагается, что противодействие против известных типов атак (злоумышленник посередине, подмена сообщения) будет осуществляться ранее известными средствами (т.е. специальных мер не предусмотрено в предлагаемой схеме).

1. Постановка задачи

Предлагаемая в данном исследовании схема обмена сообщениями описывается следующим образом. Путь имеется $\boldsymbol{A_N}$ – множество из $\boldsymbol{N}$ абонентов. Среди них присутствует единственный абонент-координатор: Алиса, которая координирует работу других абонентов и является основным источником скрытых сообщений, то есть доля числа передаваемых сообщений от Алисы к другим абонентам является подавляющей. Имеется стороннее лицо: Ева, которая может анализировать все передаваемые сообщения. Задача состоит в организации скрытого процесса передачи секретных сообщений по открытому каналу связи от Алисы к другим абонентам.

Будем называть $\boldsymbol{G_M}$ группой из $\boldsymbol{M}$ абонентов подмножество абонентов такое, что $\boldsymbol{G_M \subseteq A_N}$. На практике новая схема может быть применена для рассылки головной организацией некоторых секретных инструкций или сведений своим филиалам (отделениям). Например, головная организация встраивает секретные сообщения в видеофайлы (допустим, рекламу) и выкладывает их в открытый доступ, используя некоторый публичный хостинг или облако. С точки зрения посторонних лиц, видеофайлы не содержат каких-либо секретных сведений. Абоненты схемы могут извлекать сообщения, но расшифровать сможет только та группа (например, филиал), которая обладает ключом для заданного сообщения в контейнере, т.е. Алиса изначально отправляла сообщение для конкретной группы.

Зафиксируем следующие требования к схеме (далее – Требования):

1. Сообщения передаются с помощью заранее оговоренных методов стеганографии и криптографии. Внедренное в контейнер скрытое сообщение предварительно зашифровано ключом, известным Алисе и группе абонентов $\boldsymbol{G_M}$, которым предназначается данное сообщение.
2. По решению Алисы состав групп меняется, причем состав групп заранее не известен.
3. Абоненту разрешается входить в несколько групп одновременно.
4. Абонент или группа идентифицируются некоторым натуральным числом.
5. Передача данных от абонентов к Алисе, внутри и между группами осуществляется с помощью известных ранее схем и не рассматривается в данной работе из-за незначительной доли в общем числе передаваемых сообщений.
6. Пересылаемый контейнер имеет временную метку его создания (**TIME_STAMP**).
7. В общем случае сообщение в контейнере состоит из двух частей, размеры которых варьируются:
   - служебной информации, которая определяет новые составы групп и их пароли;
   - полезной информации, которую необходимо передать группе.
8. Каждый абонент имеет личный пароль, известный только ему и Алисе.
9. Групповой пароль могут вычислить все абоненты, входящие в группу.
10. Абонент, не входящий в группу, не может вычислить групповой пароль.
11. Любой абонент, кроме Алисы, не может вычислить личный пароль другого абонента.
12. Алиса знает все ключи шифрования всех абонентов и способна воспроизвести все вычисления любого абонента.
13. Алиса не входит ни в одну из групп.

2. Описание предлагаемой схемы

Опишем процесс предварительной подготовки абонентов, выполняемый до передачи данных. Во-первых, абоненты выбирают большое простое число $\boldsymbol{p}$. Во-вторых, оговаривается применяемая функция $\boldsymbol{h(x)}$. Схема предусматривает несколько вариантов функции $\boldsymbol{h(x)}$**:** криптографическая хэш-функция, генератор псевдослучайных чисел, инициализированный параметром x или блоковый шифр, шифрующий заранее оговоренную последовательность с ключом $\boldsymbol{x}$. В-третьих, абоненты подготавливают следующие ключи, которые впоследствии не меняются:

- ключ для служебной информации $\boldsymbol{CommonKey}$– задается Алисой и является известным для всех абонентов в системе. Ключ необходим для защиты от Евы, выявляющей факт передачи секретного сообщения;
- личный ключ абонента $\boldsymbol{key}$, выбираемый абонентом. Кроме абонента ключ известен Алисе (п. 12 Требований).

Процесс подготовки и передачи ключей между Алисой и другими абонентами на этом этапе осуществляется известными ранее алгоритмами и выходит за рамки предлагаемой схемы.

На следующем этапе Алиса последовательно выполняет следующие шаги: определение состава группы, вычисление группового пароля. Далее формирует, шифрует и встраивает сообщение в контейнер с последующей его передачей другим абонентам по открытому каналу связи.

Рассмотрим процесс вычисления группового пароля. Пусть группа состоит из $\boldsymbol{k}$ абонентов. Алиса вычисляет для каждого абонента группы его текущий ключ $\boldsymbol{X_{id}}$ по формулам (2) и (3):

$$X_{id} = id^{h(F(time, key_{id}))} mod p, \quad (2)$$

где $\boldsymbol{id}$ – идентификатор абонента такой, что $\mathbf{1} < id < p - 1$, $time$ – временная метка контейнера (п. 6 Требований),

$$F(time, key_{id}) = time^{key_{id}} modp \quad (3)$$

Затем Алиса вычисляет значения $\boldsymbol{B_i} = \boldsymbol{X_{id_i}} \oplus \boldsymbol{X_{id_{i+1}}}$, где $\boldsymbol{id}$ – идентификаторы абонентов группы, отсортированные в порядке возрастания, $\boldsymbol{i}$– порядковый номер абонента в группе. Далее в служебную часть сообщения записывается состав группы, которому предназначается сообщение и множество чисел $\boldsymbol{B_i}$, необходимое абонентам для вычисления группового пароля. Служебная часть шифруется ключом $\boldsymbol{CommonKey}$. Полезная часть сообщения шифруется ключом $\boldsymbol{Gpwd_{id}}$ по формуле:

$$Gpwd_{id} = \prod X_i \, modp \quad (4)$$

Далее всё сообщение передается абонентам с помощью выбранного ранее стеганографического алгоритма.

Абонент при получении контейнера, извлекает сообщение и расшифровывает служебную часть ключом $\boldsymbol{CommonKey}$. Если абонент включен в группу, то выполняет следующие действия:

1. Вычисляет собственный текущий ключ $\boldsymbol{X_{id}}$ по формулам (2) и (3).
2. Составляет систему уравнений и вычисляет текущие ключи других абонентов:

$$\begin{cases} X_{id_1} \oplus X_{id_2} = B_1 \\ X_{id_2} \oplus X_{id_3} = B_2 \\ X_{id_3} \oplus X_{id_4} = B_3 \\ \dots \\ X_{id_{k-1}} \oplus X_{id_k} = B_{k-1} \end{cases} \quad (5)$$

   В каждом уравнении системы два неизвестных. Уравнения состоят из текущих ключей абонентов, входящих в группу, и записываются в систему в порядке возрастания идентификаторов абонентов ($\boldsymbol{id_1} < \boldsymbol{id_2} < \dots < \boldsymbol{id_k}$). Вторая переменная уравнения всегда совпадает с первой переменной последующего уравнения в системе. Таким образом, получив от Алисы множество $\boldsymbol{B_i}$ и зная собственный текущий ключ $\boldsymbol{X_{id}}$, каждый абонент, входящий в группу, сможет вычислить остальные текущие ключи других абонентов.
3. Вычисляет групповой ключ $\boldsymbol{Gpwd_{id}}$, перемножая текущие ключи абонентов группы согласно формуле (4).

Для упрощения процесса восприятия информации приведем простой пример. Допустим, что имеется 5 абонентов. Передается сообщение $\boldsymbol{M}$ для абонентов № 1, 2, 3 и 5. Алиса передает в служебной части сообщения состав группы, например, в виде битовой строки значений $\boldsymbol{B_i}$: $\{\mathbf{11101}, B_1, B_2, B_3, B_5\}$ и зашифрованное групповым паролем сообщение $\boldsymbol{M'}$ в полезной части сообщения.

Каждый абонент выполняет следующие шаги, для примера рассмотрим действия абонента №5. Он вычисляет по формулам (2) и (3) значение $\boldsymbol{X_5}$ и составляет систему уравнений (6):

$$\begin{cases} X_1 \oplus X_2 = B_1 \\ X_2 \oplus X_3 = B_2 \\ X_3 \oplus X_5 = B_3 \end{cases} \quad (6)$$

Имея значение $\boldsymbol{B_3}$ и собственный текущий ключ $\boldsymbol{X_5}$, абонент №5 находит ключ $\boldsymbol{X_3}$ абонента №3 и аналогично находятся остальные текущие ключи ($\boldsymbol{X_2}$ и $\boldsymbol{X_1}$) других абонентов. Система уравнений всегда имеет решение, так как Алиса ранее вычислила значения $\boldsymbol{B_i}$ из актуальных текущих ключей.

Перемножая найденные ключи по формуле (4), абонент получает групповой ключ и расшифровывает им сообщение $\boldsymbol{M'}$. Стоит отметить, что абонент № 4, не входящий в

состав группы, не сможет решить систему уравнений, зная только значения $\boldsymbol{B_i}$, что подробнее объясняется в разделе *обсуждение предложенной схемы*.

3. Описание процессов работы с группами

Очевидно, что при возрастании числа абонентов могут возникать трудности с указанием состава групп. Объем передаваемых данных в контейнере ограничен и увеличение служебной части всегда идет в ущерб полезной. Предлагаемая в настоящей работе схема позволяет объединять в группы не только одиночных абонентов, но и ранее созданные группы.

Рассмотрим систему уравнений 6, в которой каждое значение $\boldsymbol{X_{id}}$ является текущим ключом абонента. Схемой предусмотрено использование текущих ключей группы абонентов, значение которых вычисляется по следующей формуле:

$$X_{Gr} = Gr^{h\left(F(time, Gpwd_{Gr})\right)} modp, \tag{7}$$

где $\boldsymbol{Gr}$– идентификатор группы. Идентификаторы как групп, так и абонентов являются натуральными числами на интервале $(\mathbf{1}; \boldsymbol{p} - \mathbf{1})$ и различаются только значениями.

Значения текущих ключей групп X_{Gr} остаются неизменными до тех пор, пока состав группы не изменится. Данные ключи аналогично используются в системе уравнений (5).

Будем называть *участником* одного абонента или подгруппу, которая участвует в работе схемы. При добавлении одного участника к уже созданной группе проводятся следующее действия. Алиса высылает идентификаторы объединяемых участников и одно значение $\boldsymbol{B} = \boldsymbol{Gpwd_{old}} \oplus \boldsymbol{X_{add}}$, где $\boldsymbol{Gpwd_{old}}$ – значение группового пароля группы, а $\boldsymbol{X_{add}}$ – текущий ключ добавляемого участника. Из полученного от Алисы значения $\boldsymbol{B}$ группа, вычисляет $\boldsymbol{X_{add}} = \boldsymbol{B} \oplus \boldsymbol{Gpwd_{old}}$ и по формуле (8) вычисляет новое значение группового пароля $\boldsymbol{Gpwd_{new}}$. Добавляемый участник аналогично вычисляет $\boldsymbol{Gpwd_{old}} = \boldsymbol{B} \oplus \boldsymbol{X_{add}}$ и, соответственно, вычисляет $\boldsymbol{Gpwd_{new}}$:

$$Gpwd_{new} = Gpwd_{old} \cdot X_{add} modp. \tag{8}$$

Удаление из группы происходит путем создания новой группы, в которой отсутствует часть участников. В связи с тем, что первоначальная группа может содержать в себе большое число абонентов создание новой группы с незначительным уменьшением ее размера потребует передачи большого объема служебной информации в ущерб полезной. В этой связи рациональнее создавать большую группу из более мелких подгрупп. В последнем случае доля служебной информации может быть значительно сокращена.

Теорема 1. Пусть $\boldsymbol{Gsize}$ – максимальное количество участников в любой подгруппе, тогда для удаления одного абонента из группы, включающей $\boldsymbol{N}$ абонентов, достаточно переобъединить $\boldsymbol{log_{Gsize}(N)} * (\boldsymbol{Gsize} - \mathbf{1})$ участников.

Доказательство. Рассмотрим рисунок 1. Состав всей группы представлен в виде дерева. Кругами обозначены подгруппы, квадратами – абоненты, включаемые в новую группу, а ромбом показан удаляемый абонент. Каждая подгруппа (узел дерева) включает в себя по $\boldsymbol{Gsize} = \mathbf{3}$ участника (ветви). Для удаления одного абонента из всей группы необходимо переобъединять все подгруппы уровня, за исключением одной, содержащей удаляемого абонента (на рис. 1 показано овалом), т.е. $\boldsymbol{Gsize} - \mathbf{1}$. Далее рекурсивно объединяются оставшиеся участники для каждого последующего уровня дерева. Так как высота дерева составляет $\boldsymbol{log_{Gsize}(N)}$, то потребуется не более $\boldsymbol{log_{Gsize}(N)} * (\boldsymbol{Gsize} - \mathbf{1})$ объединений.

В качестве значения $\boldsymbol{Gsize}$ следует взять максимальное число элементов $\boldsymbol{B_i}$ свободных членов системы (5), которое указывается в служебной части сообщения. При таком размере подгрупп количество объединяемых абонентов в одном контейнере будет максимальным. Соответственно, удаление абонентов из большой группы будет максимально быстрым.

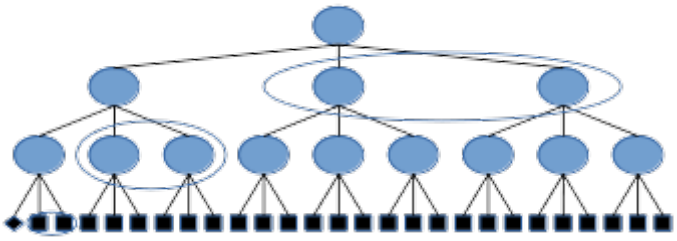

Рис. 1. Объединение подгрупп
(Fig. 1. Uniting of groups)

4. Обсуждение предложенной схемы

В данном разделе исследуются параметры предложенных алгоритмов.

Схема предназначена для стеганографической системы. Классические алгоритмы Диффи-Хеллмана и другие позволяют обмениваться паролями, но в явном виде демонстрируют факт передачи секретных сведений. Предложенная схема, напротив, направлена на создание тайного канала связи. Наличие личных паролей абонентов предполагает дублирование данных, зашифрованных для каждого абонента в отдельности, что существенно увеличит объем передаваемых данных. При малом количестве абонентов возможно заранее предусмотреть все возможные составы групп и соответствующие им групповые пароли, но при большом числе участников такой подход неэффективен.

Требование о наличии временной метки контейнера (п. 6 Требований) необходимо для синхронизации вычислений всеми участниками текущих ключей при создании группы. Наличие текущего ключа, который меняется у участника при создании новой группы, препятствует вычислению группового пароля участником, не входящим в группу, и позволяет сохранить в тайне личные ключи абонентов. На практике файлы всегда имеют временную метку создания, следовательно, не требуется дополнительно передавать какие-либо переменные, выполняющие ту же функцию.

Обратим внимание на то, что текущий ключ вычисляется с помощью двух формул: (2) и (3). В случае использования только формулы (3) возможно нарушение п. 11 Требований. Так, если участники группы обнаружат совпадающие значения переменных в системе уравнений, то это однозначно указывает на совпадении личных ключей, что вполне вероятно, так как абонент самостоятельно выбирает пароль. При использовании формул (2) и (3) в предлагаемой схеме факт совпадения ключей имеет случайную природу и не компрометирует личные ключи абонентов.

Удаление участника из группы реализовано через создание новой группы по следующим причинам. На этапе перед удалением участнику известны все текущие ключи в группе. Следовательно, любые новые данные от Алисы не позволят обеспечить удаления, так как исключенный участник сможет воспроизвести все вычисления новой группы. Изменения текущего ключа любого участника новой группы не может быть просчитано другими участниками и требует дополнительных данных от Алисы, эквивалентных по объему данным для создания новой группы.

Корректность схемы базируется на следствии теоремы Кронекера-Капелли [25]. Так, для группы из $\boldsymbol{k}$ участников всегда формируется система из $\boldsymbol{k-1}$ линейных алгебраических уравнений с $\boldsymbol{k}$ неизвестными (формула 5). Следовательно, по вышеупомянутой теореме система является совместной и имеет множество равновероятных решений для абонента, не входящего в группу. Участник группы, напротив, способен вычислить собственный текущий ключ, входящий в систему уравнений и далее найти ее оставшиеся $\boldsymbol{k-1}$ неизвестных и групповой пароль.

Стоит отметить, что потенциально уязвимым местом следует считать используемые в формулах вычисления: возведение в степень по модулю. В научной литературе предложены атаки, позволяющие вычислять дискретный логарифм за полиномиальное

время на квантовом компьютере [26]. Однако в настоящий момент на современных ЭВМ известные атаки не могут быть реализованы за приемлемое время.

Заключение

В настоящей работе предложена схема обмена групповыми паролями для стеганографических систем. Предложенный алгоритм позволяет создавать группы произвольного состава. Включение абонента в группу не компрометирует его личный пароль и пароли других абонентов. Показано, что групповой пароль не может быть вычислен абонентом вне группы. При устранении ограничения на скрытность передачи данных предложенная схема может быть легко адаптирована для криптографических систем.

СПИСОК ЛИТЕРАТУРЫ:

1. Lindell Y., Katz J. Introduction to modern cryptography. – Chapman and Hall/CRC. 2014. URL: https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie /Introduction%20to%20Modern%20Cryptography.pdf (дата обращения 23.01.2019).
2. Stinson D.R. Cryptography, Theory and Practice. – CRC Press, Boca Raton. 2014. URL: http://www.ksom.res.in/files/RCCT-2014-III-CM/CryptographyTheoryandpractice(3ed).pdf (дата обращения: 23.01.2019).
3. Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks. 2004. V. 44. No. 5. P. 643 – 666. URL: https://www.sciencedirect.com/science/article/abs/pii/S1389128603004250 (дата обращения: 23.01.2019).
4. Simmons G. J. The prisoners' problem and the subliminal channel // Advances in Cryptology. – Springer, Boston, MA. 1984. P. 51 – 67. URL: https://link.springer.com/chapter/10.1007/978-1-4684-4730-9_5 (дата обращения: 23.01.2019).
5. L. Xiang et al. A novel linguistic steganography based on synonym run-length encoding. IEICE transactions on Information and Systems. 2017. V. 100. No. 2. P. 313 – 322. URL: https://www.jstage.jst.go.jp/article/transinf/E100.D/2/E100.D_2016EDP7358/_pdf (дата обращения: 23.01.2019).
6. Denemark T., Bas P., Fridrich J. Natural Steganography in JPEG Compressed Images. Electronic Imaging. 2018. V. 2018. No. 7. P. 1 – 10. URL: https://hal.archives-ouvertes.fr/hal-01687194/document (дата обращения: 23.01.2019).
7. Nechta I. Steganography in social networks. Data Science and Engineering (SSDSE), 2017 Siberian Symposium on. – IEEE. 2017. P. 33 – 35. URL: https://ieeexplore. ieee.org/document/8071959/ (дата обращения: 23.01.2019).
8. Diffie W., Hellman M. New directions in cryptography. IEEE transactions on Information Theory. 1976. V. 22. No. 6. P. 644 – 654. URL: https://ee.stanford.edu/~hellman/publications/24.pdf (дата обращения: 23.01.2019).
9. Shamir A. How to share a secret. Communications of the ACM. 1979. V. 22. No. 11. P. 612 – 613. URL: https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf (дата обращения: 23.01.2019).
10. Maurer U. M., Yacobi Y. A non-interactive public-key distribution system. Designs, Codes and Cryptography. 1996. V. 9. No. 3. P. 305 – 316. URL: https://link.springer. com/article/10.1007/BF00129771 (дата обращения: 23.01.2019).
11. Dingyi P., Arto S., Cunsheng D. Chinese remainder theorem: applications in computing, coding, cryptography. – World Scientific. 1996. DOI: 10.1142/3254.
12. Bai L., Zou X. K. A proactive secret sharing scheme in matrix projection method. International Journal of Security and Networks. 2009. V. 4. No. 4. P. 201 – 209. URL: https://cs.iupui.edu/~xzou/Papers/IJSN09-PSSS-MPM.pdf (дата обращения: 23.01.2019).
13. Tseng Y. M., Jan J. K. ID-based cryptographic schemes using a non-interactive public-key distribution system. Computer Security Applications Conference, 1998. Proceedings. 14th Annual. – IEEE. 1998. P. 237 – 243.
14. Huang D., Medhi D. A secure group key management scheme for hierarchical mobile ad hoc networks. Ad Hoc Networks. 2008. V. 6. No. 4. P. 560 – 577.
15. Piao Y. et al. Polynomial-based key management for secure intra-group and inter-group communication. Computers & Mathematics with Applications. 2013. V. 65. No. 9. P. 1300 – 1309.
16. Srinivasan R. et al. Secure Group Key Management Scheme for Multicast Networks. IJ Network Security. 2010. V. 10. No. 3. P. 205 – 209.
17. Rezai A., Keshavarzi P., Moravej Z. Key management issue in SCADA networks: a review. Engineering science and technology, an international journal. 2017. V. 20. No. 1. P. 354 – 363.
18. Barker E., Dang Q. NIST Special Publication 800–57 Part 1, Revision 4. – 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf (дата обращения 07.02.2019).

19. Алферов А. П. и др. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп.—М.: Гелиос АРВ, 2005. 480 с, ил. 2002.
20. Будзко В. И., Мельников Д. А., Фомичев В. М. Протоколы обеспечения ключами пользователей информационно-технологических систем высокой доступности с использованием симметричной криптографии. Системы высокой доступности. 2014. Т. 10. № 3. С. 36 – 51.
21. Будзко В. И., Мельников Д. А., Фомичёв В. М. Способы согласования ключей пользователями информационно-технологических систем высокой доступности на основе ассиметричных криптографических методов. Системы высокой доступности. 2015. Т. 11. №. 4. С. 17 – 31.
22. Будзко В. И., Фомичёв В. М., Мельников Д. А. Способы доставки ключей пользователям информационно-технологических систем высокой доступности на основе ассиметричных криптографических методов. Системы высокой доступности. 2015. Т. 11. №. 4. С. 32 – 44.
23. Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher. ISO/IEC 9797-1:2011 URL: https://www.iso.org/standard/50375.html (дата обращения: 07.02.2019).
24. Information technology - Security techniques - Authenticated encryption // ISO/IEC 19772:2009 URL: https://www.iso.org/standard/46345.html (дата обращения: 07.02.2019).
25. Kronecker L. Vorlesungen über die Theorie der Determinanten: Erste bis Einundzwanzigste Vorlesungen. – BG Teubner. 1903. V. 2.
26. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE. 1994. P. 124 – 134.

REFERENCES:

[1] Lindell Y., Katz J. Introduction to modern cryptography. – Chapman and Hall/CRC. 2014. URL: https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie /Introduction%20to%20Modern%20Cryptography.pdf (accessed: 23.01.2019).
[2] Stinson D.R. Cryptography, Theory and Practice. – CRC Press, Boca Raton. 2014. URL: http://www.ksom.res.in/files/RCCT-2014-III-CM/CryptographyTheoryandpractice(3ed).pdf (accessed: 23.01.2019).
[3] Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks. 2004. V. 44. No. 5. P. 643 – 666. URL: https://www.sciencedirect.com/science/article/abs/pii/S1389128603004250 (accessed: 23.01.2019).
[4] Simmons G. J. The prisoners' problem and the subliminal channel. Advances in Cryptology. – Springer, Boston, MA. 1984. P. 51 – 67. URL: https://link.springer.com/chapter/10.1007/978-1-4684-4730-9_5 (accessed: 23.01.2019).
[5] L. Xiang et al. A novel linguistic steganography based on synonym run-length encoding. IEICE transactions on Information and Systems. 2017. V. 100. No. 2. P. 313 – 322. URL: https://www.jstage.jst.go.jp/article/transinf/E100.D/2/E100.D_2016EDP7358/_pdf (accessed: 23.01.2019).
[6] Denemark T., Bas P., Fridrich J. Natural Steganography in JPEG Compressed Images. Electronic Imaging. 2018. V. 2018. No. 7. P. 1 – 10. URL: https://hal.archives-ouvertes.fr/hal-01687194/document (accessed: 23.01.2019).
[7] Nechta I. Steganography in social networks. Data Science and Engineering (SSDSE), 2017 Siberian Symposium on. – IEEE. 2017. P. 33 – 35. URL: https://ieeexplore. ieee.org/document/8071959/ (accessed: 23.01.2019).
[8] Diffie W., Hellman M. New directions in cryptography. IEEE transactions on Information Theory. 1976. V. 22. No. 6. P. 644 – 654. URL: https://ee.stanford.edu/~hellman/publications/24.pdf (accessed:23.01.2019).
[9] Shamir A. How to share a secret. Communications of the ACM. 1979. V. 22. No. 11. P. 612 – 613. URL: https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf (accessed: 23.01.2019).
[10] Maurer U. M., Yacobi Y. A non-interactive public-key distribution system. Designs, Codes and Cryptography. 1996. V. 9. No. 3. P. 305 – 316. URL: https://link.springer. com/article/10.1007/BF00129771 (accessed: 23.01.2019).
[11] Dingyi P., Arto S., Cunsheng D. Chinese remainder theorem: applications in computing, coding, cryptography. – World Scientific. 1996. DOI: 10.1142/3254.
[12] Bai L., Zou X. K. A proactive secret sharing scheme in matrix projection method. International Journal of Security and Networks. 2009. V. 4. No. 4. P. 201 – 209. URL: https://cs.iupui.edu/~xzou/Papers/IJSN09-PSSS-MPM.pdf (accessed: 23.01.2019).
[13] Tseng Y. M., Jan J. K. ID-based cryptographic schemes using a non-interactive public-key distribution system. Computer Security Applications Conference, 1998. Proceedings. 14th Annual. – IEEE. 1998. P. 237 – 243.
[14] Huang D., Medhi D. A secure group key management scheme for hierarchical mobile ad hoc networks. Ad Hoc Networks. 2008. V. 6. No. 4. P. 560 – 577.
[15] Piao Y. et al. Polynomial-based key management for secure intra-group and inter-group communication. Computers & Mathematics with Applications. 2013. V. 65. No. 9. P. 1300 – 1309.
[16] Srinivasan R. et al. Secure Group Key Management Scheme for Multicast Networks. IJ Network Security. 2010. V. 10. No. 3. P. 205 – 209.

[17] Rezai A., Keshavarzi P., Moravej Z. Key management issue in SCADA networks: a review. Engineering science and technology, an international journal. 2017. V. 20. No. 1. P. 354 – 363.
[18] Barker E., Dang Q. NIST Special Publication 800–57 Part 1, Revision 4. – 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf (accessed 07.02.2019).
[19] Alferov A. P. et al. Osnovi kriptografii [Cryptography fundamentals]: Uchebnoe posobie [Tuturial]. 3 edition, M.: Gelios ARV, 2005. 480 p, ill, 2002.
[20] Budzko V.I., Melnikov D.A., Fomichev V.M. Protokoly obespechenija kljuchami pol'zovatelej informacionno-tehnologicheskih sistem vysokoj dostupnosti s ispol'zovaniem simmetrichnoj kriptografii [Keys management protocols based on symmetric cryptography for users of high availability information systems]. Sistemy vysokoj dostupnosti [High availability systems]. 2014. V. 10. No. 3. P. 36 – 51.
[21] Budzko V. I., Melnikov D. A., Fomichev V. M. Sposoby soglasovanija kljuchej pol'zovateljami informacionno-tehnologicheskih sistem vysokoj dostupnosti na osnove assimetrichnyh kriptograficheskih metodov [Secret key agreement mechanisms based on asymmetric cryptography for users of high availability information technology systems]. Sistemy vysokoj dostupnosti [High availability systems] 2015. V. 11. N. 4. P. 17 – 31.
[22] Budzko V. I., Fomichev V. M., Melnikov D. A. Sposoby dostavki kljuchej pol'zovateljam informacionno-tehnologicheskih sistem vysokoj dostupnosti na osnove assimetrichnyh kriptograficheskih metodov [Key transport mechanisms based on asymmetric cryptography for users of high availability information systems]. Sistemy vysokoj dostupnosti [High availability systems] 2015. T. 11. №. 4. P. 32-44.
[23] Information technology - Security techniques - Message Authentication Codes (MACs) Part 1: Mechanisms using a block cipher. ISO/IEC 9797-1:2011 URL: https://www.iso.org/standard/50375.html (accessed 07.02.2019).
[24] Information technology - Security techniques - Authenticated encryption. ISO/IEC 19772:2009. URL:https://www.iso.org/standard/46345.html (accessed: 07.02.2019).
[25] Kronecker L. Vorlesungen über die Theorie der Determinanten: Erste bis Einundzwanzigste Vorlesungen. – BG Teubner. 1903. V. 2.
[26] Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE. 1994. P. 124 – 134.

Поступила в редакцию – 17 января 2019 г. Окончательный вариант – 18 февраля 2019 г.
Received – January 17, 2019. The final version – February 18, 2019.