Научная статья
Original article

Использование отрицаемого шифрования для защиты информации

Турышев А.А
ФГБОУ ВО «Уральский государственный экономический университет», Екатеринбург, Россия
Автор-корреспондент: artem.turyshev@vk.com

Аннотация: В наше время, когда большинство данных хранится в электронном виде появляется необходимость их защищать от разного рода атак. Статья исследует применение отрицаемого шифрования в контексте обеспечения безопасности информации. Авторы рассматривают принципы отрицаемого шифрования и его основные характеристики, такие как аутентификация, конфиденциальность и целостность данных. Они анализируют преимущества и ограничения данного подхода, включая его эффективность, противодействие криптоанализу и возможности применения в различных сферах, таких как финансы, здравоохранение и правоохранительная деятельность. В заключение, авторы обсуждают перспективы развития отрицаемого шифрования и его роль в современных системах защиты информации.

Ключевые слова: отрицаемое шифрование, сети, защита, безопасность.

Для цитирования: Турышев А.А Использование отрицаемого шифрования для защиты информации. Умная цифровая экономика. 2023. Т.3, №2, с. 103-111

The use of denied encryption to protect information

Turyshev A.A.
Ural State University of Economics, Yekaterinburg, Russia
Corresponding author: artem.turyshev@vk.com

Abstract: In our time, when most data is stored electronically, it becomes necessary to protect them from all sorts of attacks. The article explores the use of deniable encryption in the context of information security. The authors consider the principles of deniable encryption and its main characteristics, such as authentication, confidentiality and data integrity. They analyze the advantages and limitations of this approach, including its effectiveness, resistance to cryptanalysis, and applications in various fields such as finance, healthcare, and law enforcement. In conclusion, the authors discuss the prospects for the development of deniable encryption and its role in modern information security systems.

Keywords: denied encryption, networks, protection, security.

For citation: Turyshev A.A. Using deniable encryption to protect information. Smart digital economy. 2023. Vol. 3, №2, pp. 103-111

Введение

Для шифрования трафика в сети интернет чаще всего используют симметричный и асимметричный типы шифрование, которые зарекомендовали себя временем, но в ряде случаев отрицаемое шифрование позволяет с большей вероятностью защитить информацию от нежелательного владения.

В практике защиты информации в социальных сетях в компьютерных и мобильных приложениях пароли используется прием, который получил название «двойное дно». Двойное дно – это способ защиты информации путем создания аккаунта-клона, на который будут приходить весь нежелательный трафик.

В данной статье изложены примеры ситуаций, в которых отрицаемое шифрование, и частный случай «двойное дно», становится альтернативой нынешних средств защиты информации.

Целью данной статьи является предложить модель защиты информации с использованием алгоритма отрицаемого шифрования для пользователей одноранговых и многоранговых сетей.

Основная часть

Для того чтобы, выявить наиболее благоприятные сферы применения отрицаемого шифрования, кротко сравним наиболее популярные типы шифрования [1], где отдельным типом будем считать отрицаемое шифрование [4].

Таблица 1 – Сравнение симметричного асимметричного и отрицаемого шифрования

Критерии	Симметричное	Асимметричное	Отрицаемое
Определение	Способ шифрования, в котором для шифрования и дешифрования используется один и тот же ключ	Способ шифрования, в котором для шифрования используется один ключ, а дешифрования используется другой ключ	Способ шифрования, в котором можно по-разному расшифровать один и тот же шифр-текст
Способ шифровки	Одно секретное сообщение - одни закрытый ключ	Одно секретное сообщение - один открытый ключ	Одно сообщение для отвода внимания - один открытый; один закрытый ключ – одно секретное сообщение
Способ дешифровки	Одни закрытый ключ - одно секретное сообщение	Один закрытый ключ - одно секретное сообщение	Один открытый - одно сообщение для отвода внимания и (или) один закрытый ключ - одно секретное сообщение

Плюсы	Требует относительно малой вычислительной мощи для шифровки/дешифровки	Для передачи ключа не нужен закрытый канал; открытый ключ может быть свободно распространён	Представлено ниже в статье
Минусы	Требуется защищённый канал для передачи закрытого ключа.	Требует относительно большой вычислительной мощи для шифровки/дешифровки	Представлено ниже в статье
Применение	Блокчейн, мессенджеры.	Электронная подпись, мессенджеры.	Предложено ниже

Рассмотрим угрозу разрешения, которой невозможно без участия 3-его дружественного лица для симметричного и асимметричного шифрования, но возможно благодаря отрицаемому шифрованию.

Представим следующую ситуацию, Евгений, любящий ночные прогулки зашел не в самый благополучный район своего города. На пути встретились грабители, которые решили ограбить его. Не найдя бумажника, злоумышленники угрозами заставлять Евгения перевести деньги в онлайн банке на карту грабителя. Евгений, поскольку на кону стоит его здоровье, а возможно даже жизнь. Евгений вводит пароль от онлайн банка и по требованию одного из злоумышленников переводит все имеющиеся деньги.

В последствии, преступников не получается поймать, поскольку карта на которые пришли деньги не принадлежала ни одному из грабителей и деньги были сняты почти сразу же после грабежа, а банк отказывается вернуть деньги ссылаясь на общепринятые нормы поведения в обществе, в нарушении которых вступает угловой кодекс РФ.

Но все могло пойти иначе, если бы онлайн банк применил отрицаемое шифрование через пароль (частный случай отрицаемого шифрования -«Двойное дно»).

Рассмотрим альтернативную ситуацию: онлайн банк использует отрицаемое шифрование при авторизации пользователя это значит, что Евгений заранее создал два аккаунта с разными паролями на доступ и с разными суммами на счетах. И при неблагоприятной ситуации, которую я описал выше, Евгений вводит пароль от аккаунта, на котором денег меньше, что для грабителей смотрелось бы естественно и не вызвало бы подозрений.

На самом деле, паролем может служить даже выражение лица. В СберБанке уже сейчас можно подтверждать транзакцию и даже снимать деньги в банкоматах своими биометрическими данными. Я предлагаю улучшить данную функцию алгоритмом отрицаемого шифрования, в контексте ситуации с Евгением, следующим образом. При загрузке своих биометрических данных в приложении составить сценарии основываясь на выражении глаз, бровей или губ.

К примеру, если человек хочет снять деньги с аккаунта №1, то он должен при вводе своих биометрических данных улыбнуться, если он хочет снять деньги с аккаунта №2, то он должен нахмурить брови. Данные сценарии помогут клиенту банка выглядеть естественно

для окружающих (может быть для злоумышленников), вовремя в снятии наличных, переводов или же при покупке в магазине.

Отрицаемое шифрование

Данное преобразование, где в шифр-тексте совместно зашифровываются два или более сообщений на двух или более ключах и расшифровывается в зависимости от сложившихся обстоятельств, называется отрицаемым шифрованием.

Первые упоминания (использования) об отрицаемом шифровании были замечены в статье Ранна Канетти, Синтии Дворк, Мони Нора и Рафаила Островски «Deniable Encryption» в 1996 году [7].

Первое использования отрицаемого шифрования было использовано в программе Rubberhose в 1997 году, она с учетом размера информации (i), которую нужно было обезопасить, создавала том, размеры которого были значительно больше i, перемешивала биты в томе и при разных ключах давала разную интерпретацию зашифрованной информации.

Если использовать передачу данных в одноранговых и многоранговых сетях по алгоритму отрицаемого шифрования, то получится обезопасить объекта атаки не только пассивного прослушивания, но и от внешнего воздействия [3].

Таблица 2 – Сравнение одноранговой и многоранговей сети

	Одноранговая сеть [5]	Многоранговая сеть [6]
Определение	это компьютерная сеть, в состав которой входят равноправные компьютеры, администрация которых происходит самим пользователем	это компьютерная сеть, в состав которой входят один или несколько выделенных серверов. Остальные компьютеры выступают в роли клиентов
Преимущества сети	Простая и дешевая в создании; Не требует управляющих компьютеров; Работа сети не зависит от работоспособности отдельных узлов	Высокая скорость и производительность Сети; Использование выделенных серверов, что облегчает работу с ресурсами и упрощает контроль за их использованием; Наличие дублирующих систем, позволяющих защитить данные и сделать доступ к ним бесперебойным; Централизованные обновления операционной системы и программного обеспечения; Полный контроль над пользователями сети;

		Высокий уровень безопасности данных; Продвинутые средства мониторинга работоспособности сети; Легкая расширяемость сети
Недостатки сети	Отсутствует централизованное хранилище Ресурсов; Отсутствует возможность административного управления пользователями и ресурсами; Каждый пользователь должен самостоятельно следить за состоянием программного обеспечения; За обновление антивирусных баз (и другого программного обеспечения) отвечает пользователь; Низкий уровень защиты информации.	Дорогая в создании и обслуживании; Постоянная необходимость в системном администраторе.

Отрицаемое шифрование в одноранговых сетях

Рассмотрим алгоритм отрицаемого шифрования в одноранговых сетях, где каждый клиент на прямую общается с другим клиентом (рис.1).

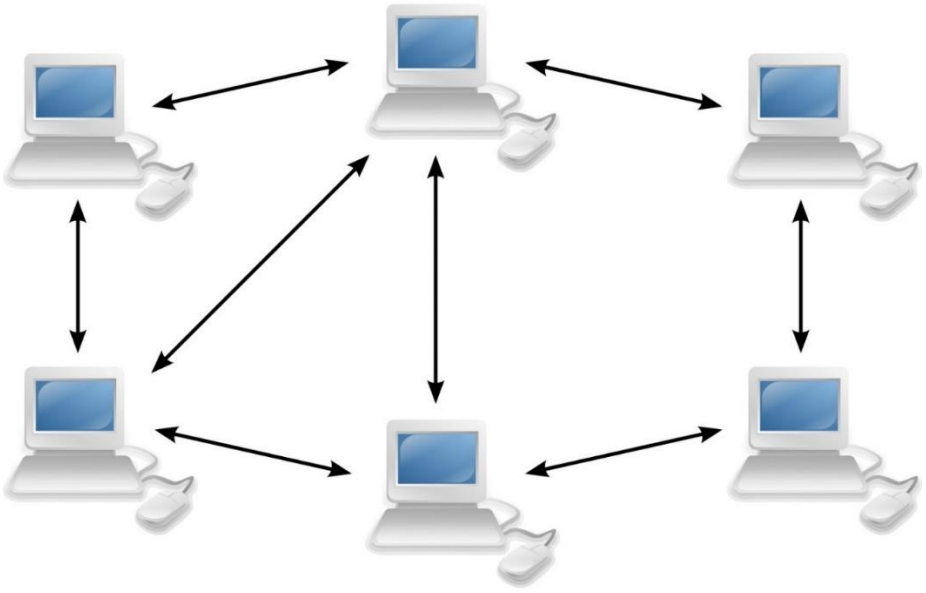

Рисунок 1 – Одноранговая сеть

В данном случаи я предлагаю следующий сценарий:

Клиенту 1 требуется отослать конфиденциальную информацию клиенту 2. С целью увеличения защиты информации клиент 1 отсылает сообщение 1(С.1) которое содержит

истинную информацию и сообщение 2(С.2), которое содержит ложную информацию. Для решения этой задачи предлагается использовать алгоритм отрицаемого шифрования, поскольку он позволяет сгенерировать как минимум два ключа с разной силой шифрования, тем самым обезопасить конфиденциальную информацию от пассивного прослушивания и корректной дешифровки (см. рисунок 2). С.1 кодируется ключом 1 = f1. С.2 ключом 2 = f2. Шифр-текст = {{f1, f2, Ключ2} или {f1, f2}}. Криптографическая стойкость f2<<f1 поэтому предполагаемый злоумышленник может достаточно легко подобрать ключ для f2 (или же, просто, перехватить вместе с шифр-текстом, как показано на рис.2) и расшифровать С.2 [2].

Поскольку в открытых источниках мало картинок, отображающих принцип работы отрицаемого шифрование визуализацию работы алгоритма пришлось изобразить автору.

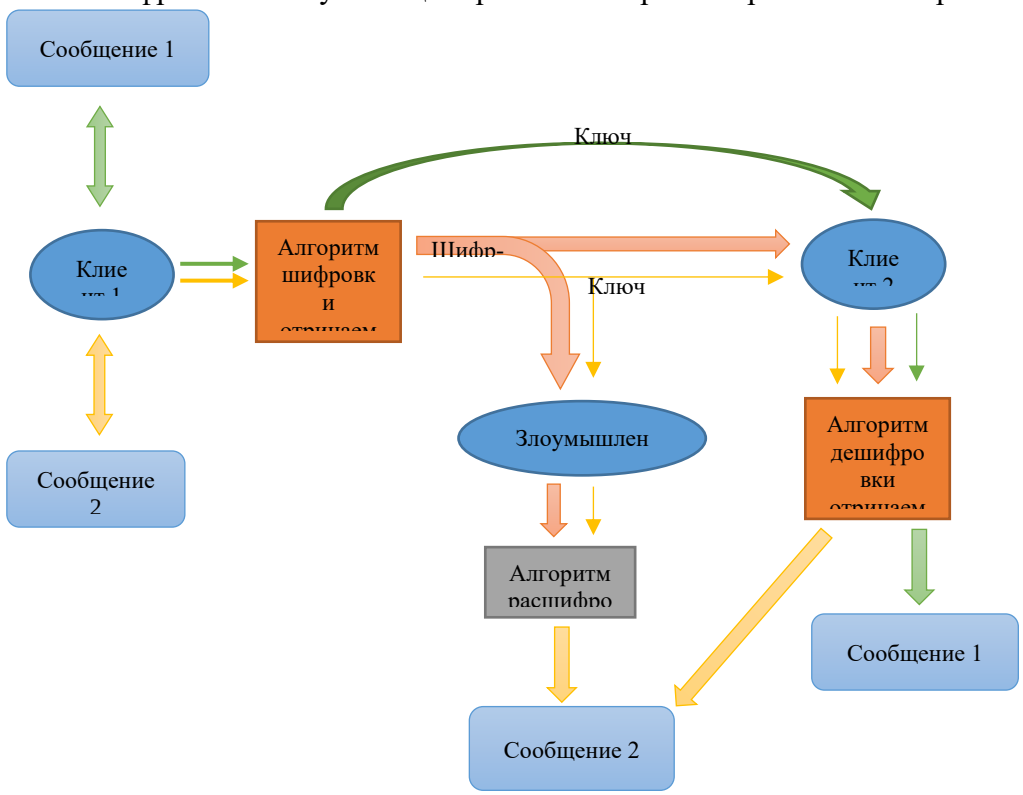

Рисунок 2 – Модель использования отрицаемого шифрования в одноранговых сетях

На данный момент присутствует статья в который описывается алгоритм отрицаемого шифрования на основе блочных шифров, который удовлетворяет ГОСТ 28147-89. [1]

Основные минусы отрицаемого шифрования в одноранговых сетях:

- При расшифровке шифр-текста одни из двух ключей, в шифр-тексте остаются не задействованы биты, которые могут выдать, что шифр-текст скрывает не одно сообщение.
- Перед каждой отправкой сообщения нужно самостоятельно или при помощи программы (которой еще нет) нужно шифровать сообщение.
- По сравнению с симметричное и асимметричное шифрование нужно одно сообщение весит больше.

Отрицаемое шифрование в многоранговых сетях

Рассмотрим алгоритм отрицаемого шифрования в многоранговых сетях, где клиент общается с сервером.

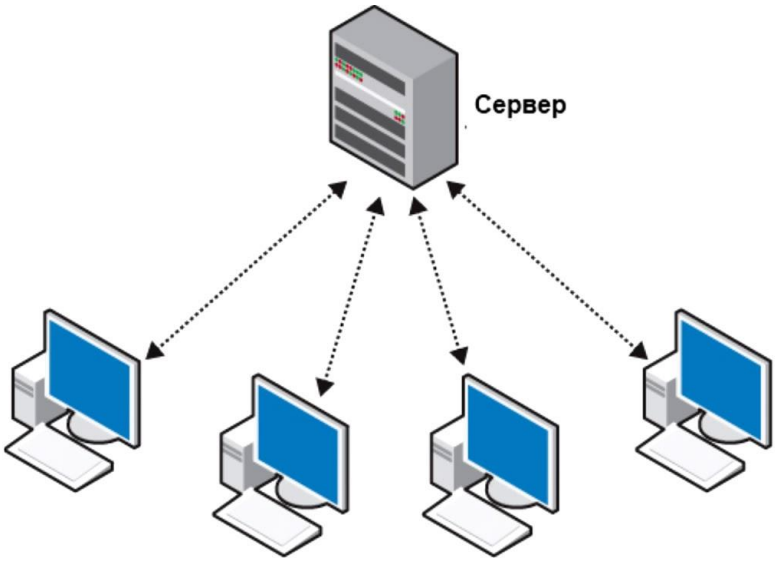

Рисунок 3 – Многоранговая сеть

В случаи с многоранговой сетью (рис.3) можно пойти по принципу изложенному в главе посвященной одноранговой сети, а можно сделать проще:

Предположим, что у пользователя существует два аккаунта, один из которых с менее важной информацией дрогой с более важной. Технически сервис (рис.4) с отражаемым шифрованием в многоранговых сетях организован так, что эти аккаунты находятся на разных серверах. Злоумышленник получает доступ к аккаунту 1, который не содержит значимой информации и при этом не имеет информации, что существует аккаунты 2 на сервере 2.

В случаи информационной охоты на пользователя в сети, важно, чтоб пароль от «подставного» сервера совпадал с другими паролями с более распространённых ресурсов (VK, twitter и пр.). Поскольку, спрос взлома аккаунтов на этих ресурсах наиболее востребованы и наверняка у тесного круга лиц, оказывающих данные услуги, есть методы получения пароля с этих ресурсов. Присутствует, большая вероятность, что исполнители информационной охоты попробуют ввести украденный пароль для ресурса с отрицаемым шифрование, что приведет их на «подставной» сервер.

Если информационная охота перешла в реальный мир, и под влиянием неопределимых факторов третья сторона [Злоумышленник] вынуждает ввести пароль, то пользователь вводит пароль от «подставного» сервера, чтобы протекания процесса требования пароля выглядело более естественно и безопасно, чем отвечать: «Не знаю» или «Забыл»; и чтобы сохранить информацию на «хорошем» сервере. А такое может происходить хотя бы потому, что законодательство РФ обязывает предприятия, связанные с государственными органами, и фирмы, занимающиеся гос. подрядами, иметь человека, отвечающего за информационную безопасность.

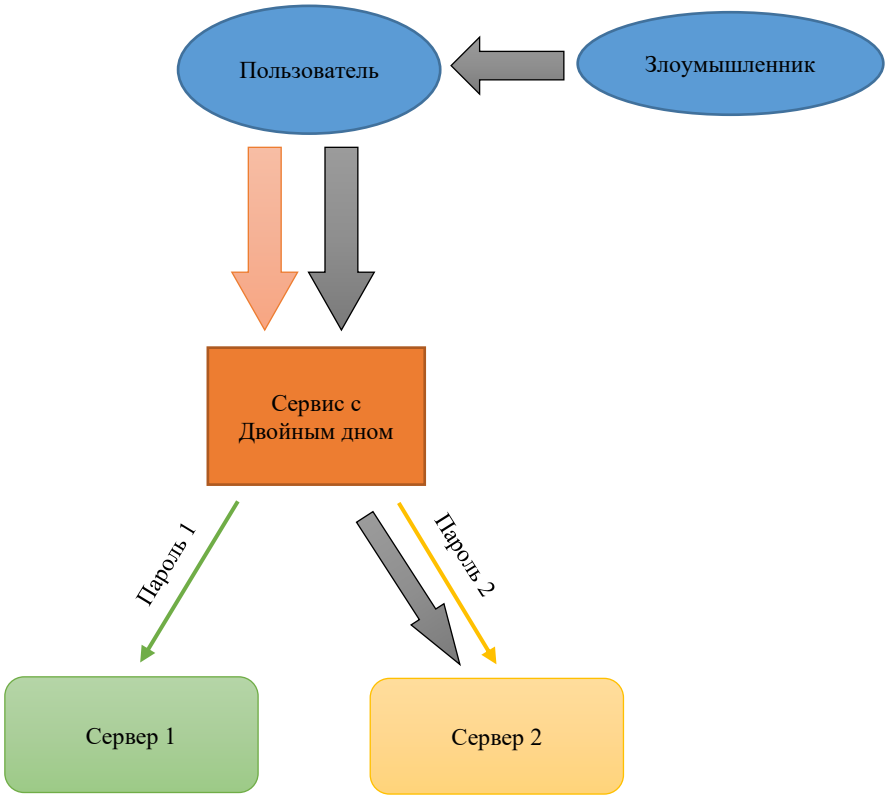

Рисунок 4 – Модель алгоритма отрицаемого шифрования в одноранговых сетях

При желании пользователя, можно завести несколько аккаунтов, либо создать пароль или ввести ограничение попыток входа на полное удаление информации со всех аккаунтов [3].

Данный алгоритм является частным случаем отрицаемого шифрования. В интернете дали ему название – «двойное дно».

Данный алгоритм использует команда белорусских разработчиков в проекте Postufgram. Данный проект в качестве расширения предназначен для мессенджера Telegram.

Поскольку, для защиты информации в данном алгоритме важна секретность и анонимность пользователя использующего, как традиционный алгоритм отрицаемого шифрования, так и частного случая «Двойное дно», то информации об использовании таких проектах крайне мало.

Необходимо иметь ввиду, что при выходе приложений, использующих алгоритм отрицаемого шифрования, доступ к данной технологии появится в том числе и у злоумышленников, который захотят использовать алгоритм для сокрытия информации от гос. органов. В такие случаи по запросу гос. органов нужно будет представить ключи или же весь пласт информации имеющихся у пользователя.

Минусы «Двойного дна»:

Если погрузка приложение происходит напрямую с устройства, то при соотношении размера подгружаемых данных и данных присутствующем на аккаунте можно сделать вывод, что присутствует еще один аккаунт.

Если третья сторона захочет проверит, присутствует ли еще один аккаунт, то забраудфорсив пароль рано или поздно пароль от 2-ого аккаунта найдется, если пользователь не предусмотрел данный факт.

Требует дополнительных ресурсов в виде еще одного сервера.

Заключение

В рамках данной статьи была разработана модель для защиты электронных данных в одноранговых и многоанговых сетях. Следует отметить, что в российские науки недостаточно публикаций о возможном применении отрицаемого шифрования для пользователей сети интернет. Рассмотренные модели мало применяются в современном мире, несмотря на ряд преимуществ по сравнению с другими типами шифрования.

Список литературы

1. Андреев, С. А. Методы защиты пользователей в сети Интернет: темные паттерны / С. А. Андреев, Д. М. Назаров // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики : Материалы X Международной научно-практической очно-заочной конференции, Екатеринбург, 02 декабря 2022 года / Ответственные за выпуск: А.Ю. Коковихин, Д.М. Назаров, ответственный редактор: С.В. Бегичев. – Екатеринбург: Уральский государственный экономический университет, 2023. – С. 3-6. – EDN PRNDDC.

2. Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В. Способ отрицаемого шифрования // Вопросы защиты информации. 2013. № 2. С. 18–21.

3. Зацепина А.И. Шифрование данных / А.И Зацепина // Текст научной статьи по специальности «Компьютерные и информационные науки». – 2013– URL: https://cyberleninka.ru/article/n/shifrovanie-dannyh

4. Морозова Е.В. Способы отрицаемого шифрования с разделяемым ключом / Е.В Морозова, Я. А. Мондюкова // Текст научной статьи по специальности «Компьютерные и информационные науки». – 2013– URL: https://cyberleninka.ru/article/n/sposoby-otritsaemogo-shifrovaniya-s-razdelyaemym-klyuchom

5. Техническая документация Microsoft: официальный сайт. – Microsoft Learn, 2023. – URL: https://learn.microsoft.com/ru-ru/windows/win32/p2psdk/what-is-peer-networking-

6. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2017. - 960 с.

7. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption // Advances in Cryptology – CRYPTO 1997: Proc. P. 90–104.

8. Ran Canetti Deniable Encryption/ Ran Canetti, Cynthia Dwork, Moni Naor, Rafall Ostrovsky// 1996 – URL: https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/Deniable_Encryption.pdf