УДК 61:621 + 004.78.056

Применение программно-аппаратных средств защиты информации в телемедицине

Ю. М. Пенкин, В. Г. Кучеренко, А. Г. Литвинов, Г. И. Хара
Национальный фармацевтический университет, Харьков, Украина

Резюме

Введение. Для обеспечения целостности данных при их передаче в системах телемедицины в настоящее время используются два стандарта с протокольным типом защиты. Однако в коммуникационных сетях иных назначений широко используются более эффективные и более криптостойкие реализации программно-аппаратного стандарта AES. В статье обсуждается возможность использования в рамках этого стандарта метода динамической генерации ключей, закрытых для пользователей, который может быть использован для защиты данных в телемедицинских сетях.

Цель работы. Модификация алгоритма AES для защиты телемедицинских данных, передаваемых в открытых компьютерных сетях. Исследование одного из возможных вариантов динамической генерации ключа шифрования, закрытого для конечных пользователей. Практическая программная и аппаратная реализация исследуемого алгоритма.

Объект и методы. Анализ операций в виде нелинейных перестановок элементов квадратных матриц и построение множества перестановок с заданными свойствами. Моделирование предлагаемых алгоритмов с использованием персональных компьютеров (C++ Microsoft Visual Studio). Построение закрытого канала связи в открытой компьютерной сети посредством использования микроконтроллера типа MK20DX256VLH7 совместно с Wi-Fi модулем ESP8026).

Результаты. Построена компьютерная модель предлагаемого алгоритма и исследованы ее возможности по защите передаваемых в открытой сети данных. Создана программно-аппаратная реализация алгоритма передачи данных в беспроводной сети на основе микроконтроллеров.

Ключевые слова: защита данных; криптоалгоритм; метод динамической генерации ключа; телемедицинские системы.

Клін. інформат. і Телемед. 2017. Т.12. Вип.13. с.113–118. https://doi.org/10.31071/kit2017.13.14

1. Введение

Ключевыми моментами функционирования телемедицинских систем являются: создание, накопление, хранение и передача медицинских данных с использованием компьютерных сетей. Разумеется, оптимальным для обеспечения таких процессов является создание национальных специализированных закрытых сетей передачи данных. К сожалению, такое решение (по экономическим причинам) могут себе позволить далеко не все даже развитые страны мира. Большинство функционирующих сегодня систем телемедицины ориентировано на использование открытых сетей общего назначения (например, сети Internet) либо сетей гибридного типа. В обоих случаях, необходимость использования открытых каналов компьютерных систем требует применения специальных программных и аппаратных средств [1] для обеспечения конфиденциальности передаваемой медицинской информации.

Законодательными актами Украины предусмотрено право пациента на тайну информации о состоянии своего здоровья, врачебном диагнозе и сведениях, полученных в результате диагностических обследований (ст. 39-1 Основ законодательства Украины об охране здоровья), которое должно быть обеспечено и в телемедицинской практике. С этой целью законодательная база, касающаяся использования телемедицинских систем, постоянно совершенствуется. Однако, как отмечается в [1], существующая отечественная нормативно-правовая база не отображает в полной мере современные требования к защите медицинской информации, в отношении практической телемедицины. Такие обстоятельства требуют дальнейшего совершенствования государственных нормативно-правовых подходов, что составляет отдельный юридический аспект проблемы информационной безопасности в телемедицине. Другим направлением в обеспечении защиты медицинской информации является стандартизация структур специализированных баз данных, форматов представления данных, способов хранения и внешнего доступа к этим данным. В настоящее время для этого направления достаточно подробно разработаны как теоретические основы функционирования таких баз данных в телемедицинских системах (в том числе и в Украине), так и необходимые для этого программные средства [2–4]. Тем не менее, и в этом направлении еще предстоит приложить достаточно много усилий для внедрения разработок и их адаптации к условиям отечественной медицины.

В этом смысле не является исключением и вопрос защиты медицинской информации в процессе ее передачи (например, из базы данных к потребителю) по каналам открытых сетей. С одной стороны, в зарубежной практике уже используются установленные стандарты: стандарт для передачи текстовых документов разработчика Health Level Seven International с названием HL7 v.3.0 (действующая версия 2005 года) и стандарт для передачи графических файлов от разработчиков American College of Radiology and National Electrical Manufacturers Association, получивший название DICOM (действующая версия 2004 года). Отметим, что при передаче по сети любые файлы, как правило, должны быть подтверждены электронной подписью уполномоченных лиц. С другой стороны, указанный выбор стандартов является не оптимальным, а их применение на практике имеет ряд недостатков, связанных с тем, что в обоих стандартах защита передаваемой информации осуществляется протокольными средствами. Также один из методов

создания закрытых каналов связи в открытых компьютерных сетях – использование виртуальных частных сетей (VPN). Основные недостатки этой технологии: трудности внедрения для рассредоточенных клиентов, сложности в поддержке настроек и администрировании сети, и, наконец, невозможность обеспечить ее совмещение с каналами, уже имеющими свой собственный уровень протокольной защиты.

В связи с этим вопрос обеспечения оптимальной защиты телемедицинской информации при ее передаче по каналам открытых сетей остается актуальным и требует широкого обсуждения в научной печати.

Целью работы является представление разработанных авторами программно-аппаратных средств криптографической защиты телемедицинских данных, передаваемых в открытых компьютерных сетях.

2. Материалы и методы

Анализ криптографических методов защиты информации проведён на основании системного обзора специализированной литературы, например [6, 7], доступной по исследуемой тематике. Программное обеспечение для реализации предлагаемого способа кодирования/декодирования информационного потока в открытом коммуникационном канале создано средствами интегрированной среды Microsoft Visual Studio 2015. Для макетирования аппаратных устройств, использующих этот алгоритм шифрования, применялись микроконтроллеры на базе микропроцессоров типа MK20DX256VLH7, программное обеспечение для которых разрабатывалось с использованием Kinetis Design Studio (KDS).

3. Результаты и обсуждение

3.1. Основные свойства исходного алгоритма

В настоящее время характерным для технологических применений криптографических средств является рост требований к шифрам одновременно по стойкости, скорости и по простоте реализации [7]. Ужесточение требований по стойкости обусловлено достаточно широкими возможностями атакующей стороны учитывать особенности конкретных условий функционирования криптосистемы. Например: осуществить внешнее воздействие на устройство шифрования с целью вызова аппаратных сбоев, выполнить замер потребляемой мощности, определить время вычислений и т. п. Возросшие требования по скорости связаны с необходимостью сохранения высокой производительности систем после встраивания в них механизмов защиты. Простота аппаратной реализации необходима для снижения стоимости средств шифрования, поскольку наиболее экономичные решения позволяют изготовить более дешевые и более надежные устройства, а также снизить их потребляемую мощность. Также, разумеется, что в силу специфики представления информации в цифровых устройствах наибольший практический интерес представляют блочные шифры. Поэтому разработка скоростных блочных шифров является важной задачей прикладной криптографии, в том числе и для телемедицины.

Создание «с нуля» нового качественного алгоритма блочного шифрования/дешифрования является длительным процессом, требующим привлечения специалистов достаточно высокого класса. Вследствие этого авторами был взят за основу широко применяемый в настоящее время открытый алгоритм AES (Advanced Encryption Standard), который в сентябре 2000 года Национальным институтом стандартов и технологий (National Institute of Standards and Technology – NIST) США был утвержден в качестве стандарта шифрования с симметричным блочным ключом [6]. Следует отметить, что AES является шифром двойной (программной и аппаратной) ориентации и аппаратная реализация алгоритма AES уже включена в семейство современных процессоров STM32F4xx. С момента опубликования AES вызывал и продолжает вызывать пристальное внимание криптоаналитиков. Имеются публикации о «взломе» алгоритма шифрования AES [2], однако условия такого взлома носят чисто теоретический характер и не имеют ничего общего с реальными обстоятельствами применения алгоритма на практике.

Рассмотрим поочередно два проблемных вопроса использования алгоритма AES. Первый вопрос касается наличия закрытого ключа, которым должны обменяться две стороны, участвующие в передаче информации. Передача такого ключа по открытым каналам связи сопряжена с опасностью его потери. Кроме того, достаточно трудно организовать надежное и безопасное хранение закрытого ключа. Вторая проблема (присущая всем симметричным методам шифрования) заключается в том, что зашифрованные одним ключом одинаковые блоки данных будут одинаково выглядеть в шифрованном виде. Если, например, шифрованию подвергаются показания датчиков некоторого технологического процесса, то следует иметь ввиду, что эти показания имеют, как правило, достаточно стабильный характер. Зная типы датчиков и диапазоны измеряемых данных, «злоумышленник» может внести в шифрованный текст фальсифицированные значения передаваемых параметров. Подобная ситуация может возникать и при передаче по каналу связи однотипных электронных форм.

С целью устранения указанных недостатков, авторы предлагают дополнить алгоритм AES системой динамического формирования ключей шифрования, закрытых для конечного пользователя.

3.2. Модификация алгоритма AES

В рамках стандарта AES достаточно широко трактуется возможность выбора метода для создания закрытого ключа при сохранении всех остальных требований стандарта. Поэтому актуальной является разработка скоростных шифров нового поколения, допускающих экономичную аппаратную реализацию и сохраняющих высокую скорость шифрования при частой смене ключей. Предлагаемая модификация алгоритма AES основывается на динамическом формировании ключей и заключается в следующем:

1. Субъекты, участвующие в обмене (двустороннем или многостороннем) информацией, применяют для связи специальные приемопередающие устройства с программным управлением, осуществляющие шифрование/дешифрование и другие, необходимые для обмена функции;

2. Применяемые в процессе информационного обмена закрытые ключи хранятся в оперативной памяти аппаратных устройств, и недоступны лицам их использующим. Практически все современные процессоры позволяют после программирования закрыть доступ к коду программ и считывание этого кода невозможно даже при взломе устройства;

3. При необходимости, для защиты от хищения аппаратных устройств или их утери в состав устройств могут включаться средства аутентификации конкретного пользователя (по отпечаткам пальцев, по идентификации голоса и др.).

4. Для обеспечения защиты при передаче идентичных блоков данных используется синхронная модификация ключей в системе обмена данными, причем, передаваемый для синхронизации ключей модификатор занимает менее одного процента обменного трафика.

3.3. Алгоритм динамического формирования ключа

Большинство алгоритмов блочного шифрования активно используют для формирования ключей и кодирования данных операции ***подстановки*** (замена одних элементов данных на другие при установке взаимно однозначного соответствия между множествами, содержащими эти данные) и ***перестановки*** (изменение порядка следования элементов данных). Для дальнейшего использования уточним формальные определения этих операций.

Пусть имеется два конечных множества Ω_1 и Ω_2, каждое из которых содержит n различных элементов. *Подстановкой* σ будем называть взаимно однозначное отображение Ω_1 на Ω_2. Например $\Omega_1=(1,2,3)$, а $\Omega_2=(7,11,9)$. Одна из 6-ти возможных подстановок будет иметь вид:

$$\sigma=\begin{pmatrix}1,\ 2,\ 3\\ 7,\ 11,\ 9\end{pmatrix}$$

Если количество элементов в каждом из множеств – n, то количество возможных подстановок равно факториалу n (каждому элементу множества Ω_1 может соответствовать любой элемент из множества Ω_2).

В частном случае множества Ω_1 и Ω_2 могут совпадать. Взаимно однозначное отображение множества Ω на себя будем называть *перестановкой*. Например, если $\Omega=(1,2,3)$, существует 6 подстановок (3!):

$$\pi_1=\begin{pmatrix}1,\ 2,\ 3\\ 1,\ 2,\ 3\end{pmatrix},\quad \pi_2=\begin{pmatrix}1,\ 2,\ 3\\ 2,\ 3,\ 1\end{pmatrix},\quad \pi_3=\begin{pmatrix}1,\ 2,\ 3\\ 3,\ 1,\ 2\end{pmatrix},$$

$$\pi_4=\begin{pmatrix}1,\ 2,\ 3\\ 1,\ 3,\ 2\end{pmatrix},\quad \pi_5=\begin{pmatrix}1,\ 2,\ 3\\ 2,\ 1,\ 3\end{pmatrix},\quad \pi_6=\begin{pmatrix}1,\ 2,\ 3\\ 3,\ 2,\ 1\end{pmatrix}.$$

Пусть имеется Ω множество натуральных чисел 1,2,...,n. Латинским квадратом L называют квадратную таблицу $n\times n$, в которой в каждой строке и в каждом столбце каждый элемент множества Ω встречается точно один раз. Выберем n таким образом, чтобы $n=k^2$. Тогда латинский квадрат L $n\times n$ можно разбить на n непересекающихся квадратов размером $k\times k$. Потребуем дополнительно, чтобы в каждом малом квадрате $k\times k$ каждый элемент множества Ω также встречается точно один раз. Такой латинский квадрат назовем S-квадратом. Например, если $k=3$, то получим квадрат 9×9 (с 9-ю вложенными в него малыми квадратами 3×3), который является полем популярной логической головоломки «судоку». Малые квадраты S-квадрата имеют размер $k\times k$ и содержат $n=k^2$ элементов.

Пусть построен S-квадрат порядка $n=k^2$. Выберем один из малых квадратов и предположим, что он заполнен так, как изображено на рис. 1a. Такое расположение описывается перестановкой

$$\pi_1=\begin{pmatrix}1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11.\ 12,\ 13,\ 14,\ 15,\ 16\\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11.\ 12,\ 13,\ 14,\ 15,\ 16\end{pmatrix}$$

Переставив элементы квадрата так, как показано на рис. 1b, получим перестановку, изображенную на рис. 1c.

$$\pi_2=\begin{pmatrix}1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11.\ 12,\ 13,\ 14,\ 15,\ 16\\ 2,\ 3,\ 4,\ 8,\ 1,\ 10,\ 6,\ 12,\ 5,\ 11,\ 7,\ 16,\ 9,\ 13,\ 14,\ 15\end{pmatrix}$$

На рис. 1b можно выделить 2 циклические перестановки: первая – продвижение против часовой стрелки приграничных клеток и продвижение по часовой стрелке центральных клеток таблицы. Сопоставление нижних строк перестановок π_1 и π_2 задает правила замены чисел малого квадрата при выполнении перестановки π_2. Действительно 1 меняется на 2, 2 – на 3, ..., 11 – а 7, ..., 16 – на 15. Проведя такую замену чисел во всех малых квадратах, получим большой квадрат, который будет обладать свойствами S-квадрата.

Программная реализация рассматриваемой перестановки состоит из двух простых шагов:

1) Сформируем вектор V размерностью n так, чтобы i-я компонента этого вектора равнялась числу, на которое следует менять число i;

2) Используя вектор V, выполним перестановки во всех малых квадратах исходного S-квадрата.

Оценка снизу для количества возможных S-таблиц порядка $n=k^2$ равна факториалу n. Очевидно, можно построить набор базисных перестановок, позволяющих получить любую наперед заданную S-таблицу.

Рассмотрим вариант динамической генерации ключей с использованием S-таблицы порядка $n=16$. Для этой таблицы создадим базисный набор перестановок из 8-ми функций и легенду их применения из 64-х элементов. Под легендой понимается простое перечисление в определенном порядке выбранных базисных перестановок. Зададимся некоторой S-таблицей и сопоставим ей такую же по размерам таблицу из равномерно распределенных в диапазоне 0...255 случайных чисел. Пользуясь этой таблицей можно сформировать, как минимум, 32 различных ключа, для алгоритма шифрования AES.

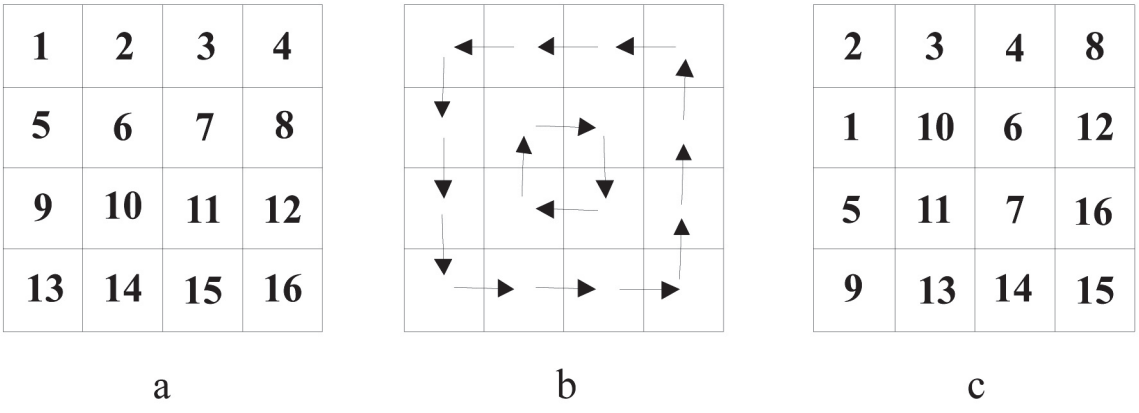

Рис. 1. Пример перестановки элементов малого квадрата для k = 4, n = 16.

Стартовая *S*-таблица, соответствующая ей таблица случайных чисел, легенда и идентификационная информация шифрующего устройства и устройств, с которыми связь санкционирована являются секретными. Перечисленная информация записывается в память процессора и недоступна ни пользователю, ни тем более, гипотетическому «злоумышленнику».

Любой сеанс передачи данных начинается с посылки случайно выбранного числа из диапазона 0...63 от инициатора обмена информацией к получателю. Передаваемое случайное число сопровождается зашифрованной идентификационной информацией отправителя. Отправление шифруется с использованием выбранной по случайному числу перестановке из легенды. Получатель, используя полученное случайное число, расшифровывает переданный блок информации, проверяет идентификационную информацию и, если эта информация достоверна, то продолжает сеанс обмена информацией.

Авторами проводилось моделирование процесса шифрования/дешифрования с использованием персонального компьютера с 4-х ядерным процессором Core i7 и канала передачи данных Ethernet. Для клиента и сервера использовались многопоточные программы. В одном из потоков производилась передача (прием) данных, а в другом генерация ключей и шифрование. Кроме того, проводился эксперимент с шифрованием данных и их передачей по каналу беспроводной связи. Схема эксперимента приведена на рис. 2. Обработка данных проводилась с использованием контроллера MK20DX256VLH7 и коммуникационного Wi-Fi контроллера ESP8266. Проводимый в течение суток эксперимент показал высокую надежность функционирования закрытого канала связи и бессбойную работу алгоритма защиты данных.

4. Заключение

Представленный в статье алгоритм динамического формирования закрытых ключей, позволяет расширить возможности стандарта AES и практически исключить вероятность потери, хищения или фальсификации медицинских и других данных при передаче их по открытым линиям связи. Более того, реализация описанного программно-аппаратного алгоритма не исключает, при необходимости, возможность сохранения протокольных операций (выполненных предварительно) с медицинскими данными, которые требуют действующие сегодня в телемедицине стандарты HL7 v.3.0 и DICOM.

Отметим, что скорость передачи данных (v = 20 Кбайт/сек), получена в макетных экспериментах с контроллером на базе процессора MK20DX256VLH7. Использование более быстрого процессора со встроенной аппаратной функцией шифрования AES и функцией аппаратной генерации случайных чисел несомненно позволит существенно улучшить этот показатель. Такие процессоры уже существуют, например, серия STM32F4xx. Моделирование шифрования с использованием ПЭВМ с 4-х ядерным процессором Core i7, при использовании многопоточного программирования показало, что при обмене шифрованной информацией между двумя подобными ПЭВМ можно в реальном времени передавать полноформатный видеосигнал. Таким образом, отсутствие предварительных вычислений и программная простота матричных преобразований, обеспечивающая достаточно большую скорость шифрования информационного потока при сохранении высокой криптостойкости, позволяет утверждать, что предлагаемый алгоритм защиты данных может быть эффективно использован не только в телемедицинских сетях, но и в открытых каналах коммуникационного управления иных технических приложений.

Исследования проводились с соблюдением национальных норм биоэтики и положений Хельсинкской декларации (в редакции 2013 г.). Авторы статьи — Ю. М. Пенкин, В. Г. Кучеренко, А. Г. Литвинов, Г. И. Хара — подтверждают, что у них нет конфликта интересов.

Литература

1. Марценюк В. П., Клымук Н. Я., Гвоздецкая И. С. Проблема защиты телемедицинской информации: нормативно-правовые и организационные аспекты из опыта республики Польша. *Медична інформатика та інженерія*. 2016, № 3, сс. 44–55.
2. Майоров О. Ю., Білов Л. Б., Нєженський С. А. Інформаційні системи охорони здоров'я (госпітальні інформаційні системи) — дань моді чи необхідність (техніко-економічне обгрунтування упровадження програмного комплексу «С-Госпіталь®»). *ISSN 1812-7231. Клиническая информатика и телемедицина*. 2004, Т. 1, Вип. 1., сс. 1–12.
3. Мінцер О. П., Болгов М. Ю. Інформаційне відображення лікувально- діагностичного процесу на рівні логіки роботи з даними. *Український журнал телемедицини та медичної телематики*. 2007, Т. 5, № 2, сс. 128–138.
4. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних. К., Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009, 716 с.
5. Дубчак Л. О. Нечітка система захисту інформації в телемедицині. Системи обробки інформації. 2015, Вип. 8, сс. 97–101.
6. Венбо Мао. Современная криптография: теория и практика. Москва, Санкт-Петербург, Киев, 2005., Изд. дом Вильямс, с. 763.
7. Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры. Санкт-Петербург, 2002., изд-во БХВ-Петербург, 496 с.

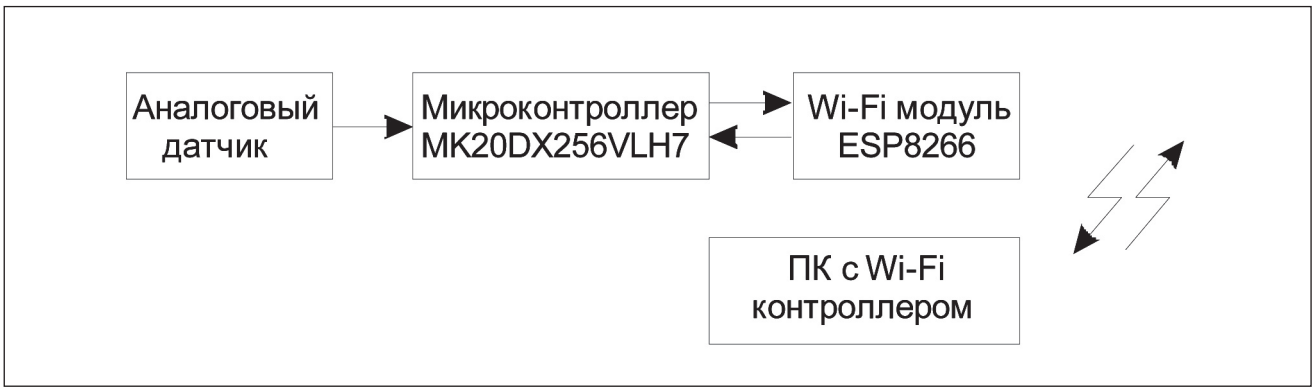

Рис. 2. Эксперимент по созданию закрытого канала связи в открытой компьютерной сети.

Застосування програмно-апаратних засобів захисту інформації в телемедицині

Ю. М. Пєнкін, В. Г. Кучеренко, О. Г. Литвинов, Г. І. Хара
Національний фармацевтичний університет, Харків, Україна

Резюме

Вступ. Для забезпечення цілісності даних за умови їх передачі в системах телемедицини у даний час використовуються два стандарти з протокольним типом захисту. Проте в комунікаційних мережах інших призначень широко використовуються більш ефективні і більш криптостійкі реалізації програмно-апаратного стандарту AES. У статті обговорено можливість застосування в рамках цього стандарту методу динамічної генерації ключів, що є закритими для користувачів, який може бути використано для захисту даних в телемедичних мережах.

Мета роботи. Модифікація алгоритму AES для захисту телемедичних даних у відкритих комп'ютерних мережах. Дослідження одного з можливих варіантів динамічної генерації ключа шифрування, що є закритим для кінцевих користувачів. Програмна та апаратна реалізація на практиці алгоритму, що досліджується.

Об'єкт і методи. Аналіз операцій у вигляді нелінійних перестановок елементів квадратних матриць і побудова множини перестановок із заданими властивостями. Моделювання алгоритмів, які запропоновано, з використанням персональних комп'ютерів (C ++ Microsoft Visual Studio). Побудова закритого каналу зв'язку у відкритій комп'ютерної мережі за допомогою застосування мікроконтролера типу MK20DX256VLH7 спільно з Wi-Fi модулем ESP8026).

Результати. Побудовано комп'ютерну модель запропонованого алгоритму і досліджено її можливості щодо захисту переданих у відкритій мережі даних. Створена програмно-апаратна реалізація алгоритму передачі даних в бездротовій мережі на засаді мікроконтролерів.

Ключові слова: захист даних; криптоалгоритм; метод динамічної генерації ключа; телемедичні системи.

Hardware and software tools application for information protection in telemedicine

Yu. M. Penkin, V. G. Kucherenko, A. G. Litvinov, G. I. Khara
National University of Pharmacy, Kharkov, Ukraine
e-mail: geoivn11@gmail.com

Abstract

Introduction. To provide the integrity of data while it transmission in telemedicine systems, two standards with a protocol type of protection are currently used. However, more effective and more crypto-stable software and hardware implementations of AES standard are widely used in communication networks of other assignments. The within this standard possibility of using the method of dynamic generation of closed for users keys, which can be used to protect data in telemedicine networks, is considered in the paper.

Objective. AES algorithm modification to protect telemedicine data transmitted in open computer networks. Study one of the possible options for dynamic generation of the encryption key, which is closed to the end-user. Practical software and hardware implementation of the investigated algorithm.

Object and methods. Operations analysis of nonlinear permutations of square matrices elements, and construction of a set of permutations with given properties. Simulation of proposed algorithms using personal computers (C ++ Microsoft Visual Studio). Construction of a closed communication channel in an open computer network with the help of the MK20DX256VLH7-type microcontroller in conjunction with the ESP8026 Wi-Fi module.

Results. A computer model of the proposed algorithm is constructed and its possibilities for data protection in an open network have been studied. The software and hardware implementation of the data transfer algorithm in a wireless network based on microcontrollers has been created.

Key words: Data protection; Cryptoalgorithm; Method of dynamic key generation; Telemedicine systems.

ISSN 1812-7231 Klin.inform.telemed. Volume 12, Issue 13, 2017, Pages 113–118
http://kit-journal.com.ua/en/index_en.html

References (7)

References

1. Martsenyuk V. P., Klymuk N. Ya., Gvozdetska I. S. The problem of protection of telemedical information: regulatory and legal and organizational aspects from the experience of the Republic of Poland. *Medichna informatika ta ingenerija* [Medical informatics and engineering]. 2016, iss. 3, pp. 44–55. (In Rus.).
2. Mayorov O. Yu., Belov L. B., Niezhens'kii S. A. Health information systems (hospital information system) — atribute to fashion or necessity (feasibility study for the implementation of the program complex «C-Hospital®». *Klinicheskaya informatika i telemeditsina* [Clinical informatics and telemedicine]. 2004, vol. 1, iss. 1, pp. 1–12. (In Rus.).
3. Mintser O. P., Bolgov M. Yu. The information display on the logic level of data handling diagnostic and treatment process. *Ukraïns'kii zhurnal telemeditsini ta medichnoi telematiki* [Ukrainian journal of telemedicine and medical telematics). 2007, vol. 5, iss. 2, pp.128–138. (In Ukr.).
4. Yudin O. K., Korchenko O. G., Konakhovich G. F.. *Zakhist informatsii v merezhakh peredachi danikh* [Protection of information in data networks]. the textbook. Kyiv, INTERSERVIS Publ. 2009, 716 p.(In Ukr.).
5. Dubchak L. O. *Nechitka systema zaxystu informaciyi v telemedycyni.* [Fuzzy information security system in telemedicine]. *Systemy obrobky informaciyi.* [Information processing systems]. 2015, iss. 8. pp. 97–101. (In Ukr.).
6. Wenbo Mao. *Sovremennaja kriptografija: teorija i praktika.* [Modern cryptography: theory and practice]. Moskva, Sankt-Peterburg, Kiev, 2005., Vil'jams Publ. 763 p. (In Rus.).
7. Moldovjan A. A., Moldovjan N. A., Guc N. D., Izotov B. V. *Kriptografija: skorostnye shifry* [Cryptography: high-speed ciphers]. St. Petersburg, Publ. House BXV-Petersburg, 2002, 496 p. (In Rus.).

Переписка

к. ф.-м. н. **Г. И. Хара**
Национальный фармацевтический университет
кафедра фармакоинформатики
ул. А. Невского, 18, Харьков, 61140, Украина
тел.: +380 (57) 771 81 52
эл. почта: geoivn11@gmail.com