

### **Предмет изобретения**

Настоящее изобретение, как следует из его названия, относится к способу шифрования на основе обычного алгоритма DES (стандарт шифрования данных, от англ. "Data Encryption Standard"), который позволяет аппаратными средствами зашифровывать пакеты данных, передаваемые между подключенными к сети пользователями или узлами такой сети.

Предлагаемый в изобретении способ характеризуется тем, что для повышения безопасности системы генерируют случайные ключи, каждый пакет данных зашифровывают новым, совершенно случайным ключом, что позволяет повысить безопасность обмена данными между узлами или устройствами системы связи, в которой используется не отвечающая требованиям безопасности передающая среда, за счет применения предлагаемого в изобретении способа вместо алгоритма DES.

### **Предпосылки создания изобретения**

В большей части систем связи необходимо осуществлять процесс шифрования информации для ее защиты от перехвата и/или изменения данных лицами вне таких систем.

Среди алгоритмов шифрования следует особо отметить DES (стандарт шифрования данных), признанный в качестве стандарта и применяемый правительством США начиная с 1977 г.

DES представляет собой алгоритм шифрования 64-разрядных блоков или пакетов данных при помощи 56-разрядного ключа, для чего осуществляют операции перестановки и подстановки, которые можно легко реализовать как аппаратными, так и программными средствами. Кроме того, этот алгоритм также является симметричным, поскольку как для зашифрования, так и для расшифрования данных применяется один и тот же ключ.

Такой алгоритм является открытым и подробно описан во множестве статей и исследований по криптографии, а 15 января 1977 г. он был признан в качестве международного стандарта Национальным бюро стандартов США, что следует из опубликованного в этой связи документа FIBS PUB 46.

Из уровня техники также известны другие алгоритмы шифрования, обеспечивающие более высокую степень защиты и безопасности данных, такие как стандарт тройного шифрования данных TDES (от англ. "Triple DES") или передовой стандарт шифрования AES (от англ. "Advanced Encryption Standard"). Стандарт TDES является вариантом DES, который заключается в том, что информацию последовательно трижды зашифровывают посредством алгоритма DES и трех различных ключей. В то же время в передовом стандарте шифрования применяют ключи, состоящие из 128, 192 и до 256 разрядов, что обеспечивает лучшее сочетание безопасности и скорости, чем в алгоритме DES.

Чтобы расшифровать сообщение, зашифрованное при помощи любого из названных алгоритмов, необходим криптоанализ перебором ключей. Подсчитано, что в случае стандарта DES для этого требуется  $2^{56}$  попыток, а в случае стандарта TDES их число достигает  $2^{112}$ .

Преимущество предлагаемого в изобретении способа заключается в том, что в использующей этот способ системе связи уровень безопасности, равноценный тому, что обеспечивается алгоритмом с более высокой степенью защиты (таким как TDES или AES), достигается менее сложными средствами, аналогичными применяемым в алгоритме DES. Для этого процесс создания ключей сделан совершенно случайным, а ключи, используемые для каждого пакета данных и каждого пользователя, обязательно должны быть разными. Таким образом, чтобы расшифровать перехваченную несанкционированным способом информацию, зашифрованную в соответствии с предлагаемым в изобретении способом, весь процесс криптоанализа пришлось бы повторять для каждого переданного пакета методом проб и ошибок, и полученной при этом информацией было бы невозможно воспользоваться для расшифрования следующего пакета, что обеспечивает надежную и эффективную защиту системы.

### **Сущность изобретения**

Для решения задач изобретения и преодоления перечисленных выше недостатков предлагается способ шифрования на основе алгоритма DES для применения в системах связи, в которых предусмотрена передача пакетов данных между подключенными к сети устройствами. Предлагаемый в изобретении способ отличается тем, что при передаче для каждого пакета данных, подлежащего шифрованию посредством алгоритма DES, генерируют случайные ключи на основе реального сигнала, к которому примешан шум, выбранный из белого и окрашенного шума. Такой пакет данных зашифровывают посредством алгоритма DES и случайного ключа, сгенерированного для этого пакета данных. Случайный ключ, в свою очередь, также зашифровывают посредством алгоритма шифрования с более высокой по сравнению с DES степенью защиты и безопасности, а полученный результат, т.е. зашифрованный ключ, вводят в заголовок передаваемого пакета данных.

На принимающей стороне предлагаемый в изобретении способ характеризуется тем, что при приеме зашифрованный ключ извлекают из заголовка принятого пакета и расшифровывают зашифрованный ключ посредством того же алгоритма шифрования с более высокой по сравнению с DES степенью защиты и безопасности, что использовался при передаче. Таким образом снова получают случайный ключ, который был создан для передаваемого пакета. Далее принятый пакет расшифровывают при помощи полученного случайного ключа, в результате чего снова получают переданную исходную информацию.

Кроме того, алгоритмом шифрования с более высокой по сравнению с DES степенью защиты и безопасности, в свою очередь, для каждого пользователя используется по меньшей мере один или не-

сколько ключей шифрования, причем эти ключи являются для каждого пользователя при передаче и приеме случайными и своими (т.е. различными для разных пользователей).

Для физической реализации способа предусмотрено, что ключ или ключи, необходимые для зашифрования случайного ключа и генерирования зашифрованного ключа пакета данных, известны отправителю и получателю и хранятся в памяти переменной емкости, зависящей от числа единиц пользовательских устройств. Аналогичным образом, ключи, необходимые при приеме для расшифрования зашифрованного ключа, также известны отправителю и получателю и хранятся в памяти переменной емкости, зависящей от числа единиц пользовательских устройств.

Таким образом, благодаря применению описанного способа вместо алгоритма DES повышается степень безопасности системы, при этом его сложность аналогична сложности шифрования на основе алгоритма DES, который применяется в системах связи.

#### **Краткое описание чертежей**

На фиг. 1 схематически представлена блок-схема возможного примера реализации предлагаемого в изобретении способа при передаче зашифрованных пакетов данных,

на фиг. 2 - блок-схема возможного примера реализации предлагаемого в изобретении способа при приеме зашифрованных пакетов данных,

на фиг. 3 - генератор случайных ключей, образованный сдвиговым регистром и случайным входным сигналом и подходящий для использования в варианте осуществления предлагаемого в изобретении способа для генерирования случайных ключей.

#### **Описание варианта осуществления изобретения**

Далее описан пример осуществления изобретения со ссылкой на цифровые позиции, приведенные на чертежах.

Как указано выше в разделе "Предпосылки создания изобретения", задача, положенная в основу настоящего изобретения, заключается в повышении безопасности алгоритма DES до уровня, сравнимого с безопасностью более сложных систем шифрования, таких как стандарт тройного шифрования данных (TDES) или передовой стандарт шифрования (AES), но при условии сохранения сложности шифрования, аналогичной сложности алгоритма DES.

В данном примере посредством алгоритма TDES осуществляют шифрование ключа, используемого в процессе шифрования пакета данных по алгоритму DES. Для шифрования при помощи названного алгоритма TDES необходимы три ключа.

Для этого в системе связи, в которой применяется предлагаемый в изобретении способ, используют генератор 5 случайных ключей (фиг. 1), структура которого показана на фиг. 3 и который образован сдвиговым регистром 25 с количеством битов, необходимым для генерирования ключа, в алгоритме DES составляющим 64 бита. Входной сигнал 24, поступающий в такой сдвиговый регистр, содержит бит сигнала 22, к которому примешан белый или цветной шум, обычно искажающий сигналы, передаваемые по реальному каналу связи. Поскольку сигнал 22 искажен шумом, после преобразования этого сигнала в двоичную форму при помощи, например, аналого-цифрового преобразователя 23, его младшие биты будут совершенно случайными, так что, если в каждом цикле синхронизации брать один из таких битов в качестве входного сигнала и сдвигать содержимое регистра, следуя числу циклов, равному ширине сдвигового регистра, все биты регистра будут случайными, а содержимое такого регистра можно использовать в качестве случайного ключа 6 для зашифрования реального передаваемого пакета данных, что дополнительно описано ниже. Описанный процесс генерирования ключей повторяют применительно к каждому передаваемому пакету данных, при этом все генерируемые ключи 6 являются совершенно случайными и не зависят друг от друга.

На фиг. 1 показана блок-схема примера общего функционирования элементов, при помощи которых реализован предлагаемый в изобретении способ при передаче данных в системе связи.

При передаче поступающий пакет 1 данных подвергают анализу в управляющем модуле 2 с целью извлечения из его заголовка соответствующей информации 3 о пользователе, которому пакет предназначен. После распознавания получателя из памяти 4 извлекают три ключа 7, соответствующих этому получателю.

Названные три ключа 7 используют в процессе применения алгоритма TDES 8, который в настоящем изобретении используют для зашифрования случайного ключа 6, созданного генератором 5 случайных ключей. Кроме того, эти три ключа, в свою очередь, генерируются для каждого пользователя случайным образом. В результате получают зашифрованный ключ 9.

Перед тем как зашифровать случайный ключ 6, его используют в модуле 10 для зашифрования данных пакета посредством алгоритма DES с получением пакета 11 данных, зашифрованного для его передачи. Чтобы декодировать пакет при приеме, потребовалось бы передать случайный ключ 6, но вместо этого модуль 10 после шифрования данных вводит зашифрованный ключ 9 в заголовок пакета 11. Таким образом, чтобы иметь возможность расшифровать пакет на приемной стороне, потребуется расшифровать зашифрованный ключ.

На фиг. 2 показана блок-схема примера общего функционирования элементов, при помощи которых реализован предлагаемый в изобретении способ при приеме данных в системе связи.

На приемной стороне операции выполняют в обратном порядке, хотя с учетом симметричности алгоритмов DES и TDES может применяться схема, аналогичная описанной выше применительно к передаче.

В данном случае управляющий модуль 13 извлекает из поступившего пакета 12 данных информацию 14 о пользователе, передавшем такой пакет, и зашифрованный ключ 9. Зашифрованный ключ 9 является случайным для каждого пакета ключом 6, который при передаче был зашифрован по алгоритму TDES с использованием трех ключей 7, известных получателю.

Зашифрованный ключ 9 расшифровывают в модуле 18 посредством алгоритма TDES и трех ключей 7. Эти три ключа извлекают из памяти 15, заноса в нее информацию 14 о пользователе-отправителе. После расшифрования зашифрованного ключа 9 получают ключ 6, который был использован для зашифрования данных при передаче.

После расшифрования этого ключа 6 в модуле 20 расшифровывают данные посредством алгоритма DES, успешно получая исходные данные 1.

#### ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ шифрования на основе алгоритма DES для применения в системах связи, в которых предусмотрена передача пакетов данных между подключенными к сети устройствами, отличающийся тем, что при передаче для каждого пакета данных, подлежащего зашифрованию посредством алгоритма DES, генерируют случайные ключи (6) на основе реального сигнала, к которому примешан шум, выбранный из белого и окрашенного шума, зашифровывают пакет данных посредством алгоритма DES и случайного ключа (6), сгенерированного для этого пакета данных, зашифровывают случайный ключ (6) посредством алгоритма шифрования с более высокой по сравнению с DES (8) степенью защиты и безопасности и вводят зашифрованный ключ (9) в заголовок передаваемого пакета данных.

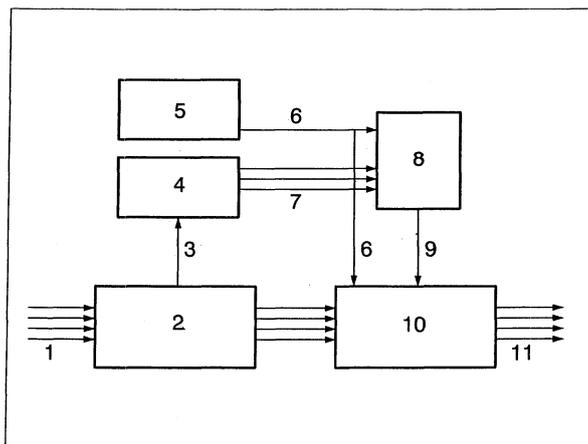
2. Способ по п.1, отличающийся тем, что при приеме зашифрованный случайный ключ (9) извлекают из заголовка принятого пакета, расшифровывают зашифрованный случайный ключ (9) посредством того же алгоритма шифрования с более высокой по сравнению с DES (18) степенью защиты и безопасности, что использовался при передаче, с получением случайного ключа (6) и посредством полученного случайного ключа (6) расшифровывают принятый пакет.

3. Способ по п.1 или 2, отличающийся тем, что алгоритмом шифрования с более высокой по сравнению с DES степенью защиты и безопасности, в свою очередь, используется по меньшей мере один ключ (7) шифрования, свой для каждого пользователя.

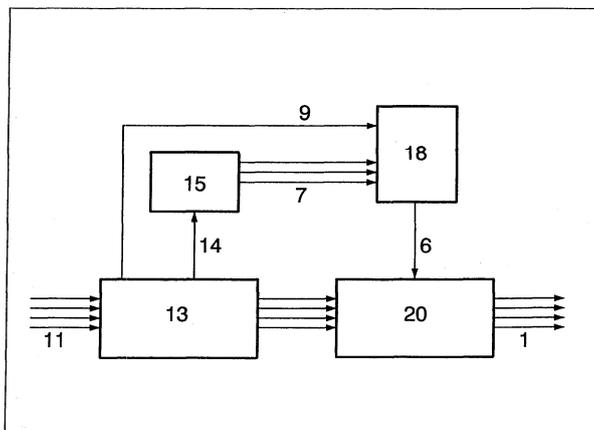
4. Способ по п.3, отличающийся тем, что по меньшей мере один ключ (7) шифрования, необходимый для зашифрования ключа шифрования данных посредством более безопасного алгоритма шифрования, является для каждого пользователя при передаче и приеме случайным и своим.

5. Способ по п.1, отличающийся тем, что по меньшей мере один ключ (7), необходимый для зашифрования случайного ключа (6) и генерирования зашифрованного ключа (9) пакета данных, известен отправителю и получателю и при передаче хранится в памяти (4) переменной емкости, зависящей от числа пользовательских устройств.

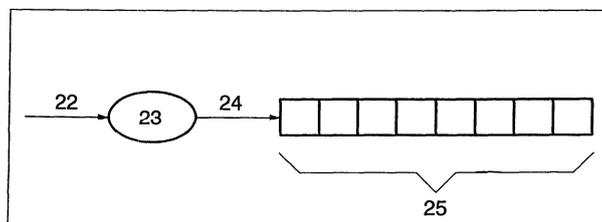
6. Способ по п.2 или 3, отличающийся тем, что по меньшей мере один ключ (7), необходимый для расшифрования случайного ключа (9) и генерирования расшифрованного ключа (6) пакета данных, известен отправителю и получателю и при приеме хранится в памяти (15) переменной емкости, зависящей от числа пользовательских устройств.



Фиг. 1



Фиг. 2



Фиг. 3

