РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 266 621** (13) **C1**

(51) МПК[7] **H 04 L 9/00, H 04 K 1/06**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2004108917/09, 29.03.2004**

(24) Дата начала действия патента: **29.03.2004**

(45) Опубликовано: **20.12.2005 Бюл. № 35**

(56) Список документов, цитированных в отчете о поиске: **Стандарт СССР ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования, Москва, ГК СССР по стандартам 1989 г. RU 2212108 C2, 10.09.2003. RU 2199826 C2, 27.02.2003. RU 2186466 C2, 27.07.2002. US 5594797 A1, 14.01.1997. US 6259791 A1, 10.07.2001.**

Адрес для переписки:
119607, Москва, ул. Раменки, 14, корп.1, кв.33, С.А.Осмоловского

(72) Автор(ы):
Осмоловский С.А. (RU)

(73) Патентообладатель(ли):
Осмоловский Станислав Антонович (RU)

(54) СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ В РАДИО И ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

(57) Реферат:

Изобретение относится к системам криптографической защиты информации в радио и локальной вычислительной сети. Техническим результатом является обеспечение шифрования информации на индивидуальных для каждой пары абонентов ключах при быстрой реализации криптографического преобразования. Технический результат достигается тем, что способ защиты информации в радио и локальной вычислительной сети с разграничением доступа к абонентам сети характеризуется шифрованием текстовой части пакета с индивидуальными для каждой пары абонентов ключами с помощью двухпараметрического шифрующего преобразования $v_i=F(u_i,\xi_i)$ и дешифрующего преобразования $u_i=F^{-1}(v_i,\xi_i)$ на основе случайной таблицы замены $T_к$ длиной 2^l знаков, где l - длина элемента алфавита, u_i - преобразуемая при шифровании комбинация, v_i - результат шифрования, ξ_i - параметр преобразования, для шифрования очередной информационной комбинации u_i, передаваемой от абонента с номером t к абоненту с номером g, находят в таблице $T_к$ исходное значение u_i, вычисляют разность значений адресов абонентов $\Delta=g-t$ по модулю 2^l, маскируют значение Δ с помощью случайно заполненной таблицы маскирования $T_м$, для чего считывают из таблицы $T_м$ по адресу Δ результат маскирования $\Delta_м$, используют значение $\Delta_м$ как параметр преобразования ξ_i шифруемого знака u_i, при этом шифрующее преобразование знака выполняют с помощью таблицы $T_к$ и дополнительной таблицы адресов T_a, в которой в строке с адресом u_i хранится адрес комбинации u_i в таблице $T_к$, определяют адрес комбинации u_i, вычисляют адрес результата преобразования как сумму по модулю 2^l адреса комбинации u_i и величины $\Delta_м$ и считывают результат преобразования v_i по вычисленному адресу из таблицы $T_к$, дешифрующее преобразование знака выполняют с помощью таблицы $T_к$ и дополнительной таблицы адресов T_a, в которой в строке с адресом v_i хранится адрес комбинации v_i в таблице $T_к$, определяют адрес комбинации v_i, вычисляют адрес результата преобразования u_i, как разность по модулю 2^l адреса комбинации v_i и величины $\Delta_м$ и считывают результат преобразования u_i по вычисленному адресу из таблицы $T_к$. 4 з.п. ф-лы.

RU 2266621 C1

RU 2266621 C1

RUSSIAN FEDERATION

(19) **RU** (11) **2 266 621** (13) **C1**

(51) Int. Cl.[7] **H 04 L 9/00, H 04 K 1/06**

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2004108917/09, 29.03.2004**

(24) Effective date for property rights: **29.03.2004**

(45) Date of publication: **20.12.2005 Bull. 35**

Mail address:
119607, Moskva, ul. Ramenki, 14, korp.1, kv.33, S.A.Osmolovskogo

(72) Inventor(s):
Osmolovskij S.A. (RU)

(73) Proprietor(s):
Osmolovskij Stanislav Antonovich (RU)

(54) METHOD FOR DATA PROTECTION IN RADIO AND LOCAL COMPUTER NETWORK

(57) Abstract:

FIELD: cryptographic data protection in radio and local computer networks.

SUBSTANCE: data protection method in radio and local computer networks with limitations on access to network clients, is characterized by encryption of text portion of packet with keys, individual for each pair of clients by means of two-parameter encrypting transformation $v_i=F(u_i,\xi_i)$ and decrypting transformation $u_i=F_{-1}(v_i,\xi_i)$ on basis of random replacement table T_k having length of 2^l symbols, where l - length of alphabet element, u_i - combination, transformed during encryption, v_i - encryption result, ξ_i - transformation parameter, for encryption of next information combination u_i, transferred from client with number t to client with number g, source value u_i is found in table T_k, difference of values of addresses of clients $\Delta=g-t$ is calculated by module 2^l, value Δ is masked by randomly filled masking table T_m, for which purpose from table T_m at address Δ result of masking Δ_M is read, value Δ_M is used as transformation parameter ξ_i of symbol u_i subjected to encryption, while encrypting transformation of symbol is performed using table T_k and additional addresses table T_a, in which in row with address u_i address of combination u_i in table T_k is stored, address of combination u_i is determined, address of transformation result is calculated as sum by module 2^l of address of combination u_i and value Δ_M and transformation result v_i is read by calculated address from table T_k, decrypting transformation of symbol is performed using table T_k and additional addresses table T_a, in which in a row with address v_i an address of combination v_i in table T_k is stored, address of combination v_i is determined, address of transformation result u_i is determined as difference by module 2^l of combination address v_i and value Δ_M and transformation result u_i is read by calculated address from table T_k.

EFFECT: encryption of information by keys, individual for each pair of clients, with fast realization of cryptographic transformation.

5 cl

RU 2266621 C1

RU 2266621 C1

Изобретение относится к техническим средствам защиты информации в радио и локальной вычислительной сети и может применяться при построении программных, аппаратных и программно-аппаратных средств криптографической защиты информации и разграничения доступа к информации в высокоскоростных сетях. В таких сетях сочетаются жесткие требования к реализации защиты по следующим причинам:

- необходимо обеспечить очень высокие скорости обмена, которые постоянно увеличиваются и способ защиты не должен сдерживать необходимое повышение физической скорости передачи;
- необходимо осуществлять защиту информации между данным и любыми другими абонентами сети на индивидуальных ключах;
- необходимо обеспечить сочетание большого объема ключа с простой реализацией использования ключа в процессе обмена.

Известны способы шифрования информации, основанные на использовании криптографического преобразования информации с помощью случайных таблиц замены. Первый из известных способов такого шифрования, называемый полибианский квадрат, предполагает использование таблицы, в которой случайным образом записаны значения букв используемого алфавита. Значение шифруемой буквы используется как адрес, по которому считывается из таблицы записанная там буква, которая является результатом криптографического преобразования. С позиций современной криптографии такое преобразование не изменяет вероятности появления отдельных букв в шифруемом тексте, а лишь меняет соотношение вероятностей отдельных букв в криптограмме. Если буква «а», в соответствии с таблицей замены переходит в букву «т», то вероятность появления в исходном тексте буквы «а» будет равна вероятности появления в криптограмме буквы «т». Известно, что анализ статистики отдельных букв в тексте криптограммы дает возможность для дешифрования теста противником. Подобные таблицы замены, как одно параметрическая операция криптографического преобразования используется в различных криптографических алгоритмах, в том числе в отечественном стандарте шифрования ГОСТ 28147-89, в качестве одной из операции усложнения преобразования.

В соответствии с изобретением в способе шифрующего преобразования предполагается строить шифрование как двухпараметрическую операцию, где результат шифрующего преобразования зависит как от значения исходного шифруемой комбинации u_i длиной L бит (в простейшем случае это буква или байт, в более общем - это q-ичный символ или блок, содержащий несколько байт) и квазислучайного параметра преобразования ξ_i, длиной не менее L бит - $F(u_i,\xi_i)$. Для реализации способа строится кодовая таблица $T_к$ объемом 2^l, где l - длина шифруемой последовательности (блока), а величина $2^l=N$ - определяет размер алфавита обрабатываемых знаков. В таблицу $T_к$ до начала шифрования записывают без повторения случайным образом все возможные значения обрабатываемых в процессе шифрования знаков длиной l бит. Процесс заполнения может осуществляться одним из двух способов. В соответствии с первым в таблицу заносятся последовательно в порядке возрастания числа с 0 до 2^l-1. Затем производится случайная перестановка записанных в таблицу значений без введения новых или исключения имеющихся значений букв. Число таких возможных перестановок равно $(2^l)!$. Например, при l=8 число перестановок $(2^8)!$ превышает 10^{300}. Такая математическая интерпретация формирования таблицы $T_к$ дает представление о числе вариантов заполнения таблицы, но не дает конкретного варианта реализации заполнения. Практическое заполнение таблицы $T_к$ осуществляют предварительно с помощью следующих операций. С помощью датчика случайных чисел (ДСЧ) вырабатывают первое значение знака, которое записывают в первую строку таблицы $T_к$ с номером 0, полученное от ДСЧ второе значение знака сравнивают с ранее записанным первым знаком, при их несовпадении второе значение записывают во вторую ячейку таблицы с номером 1, в противном случае значение второго знака, полученного от ДСЧ, отбрасывается, вырабатывается третье значение знака, сравниваемое затем с записанным в таблице значением, для заполнения очередной строки таблицы $T_к$ с номером i (i имеет значение

от 1 до 2^l-1) получают очередное значение знака от ДСЧ, сравнивают полученное значение с каждым из i-1 значением записанных в таблицу знаков, в случае несовпадения ни с одним из знаков этот знак записывается в строку с номером i, при совпадении с одним из ранее записанным в таблицу знаков полученное от ДСЧ значение отбрасывается и процесс заполнения таблицы повторяется до полного ее заполнения.

Предлагаемый способ защиты информации в радио и локальной вычислительной сети с разграничением доступа к абонентам сети основан на шифровании и дешифровании текстовой части пакета с индивидуальными для каждой пары абонентов ключами с помощью двухпараметрического шифрующего преобразования $v_i=F(u_i,\xi_i)$ и дешифрующего преобразования $u_i=F^{-1}(v_i,\xi_i)$ на основе случайной таблицы замены $T_к$ длиной 2^l знаков, где l - длина элемента алфавита, u_i - преобразуемая при шифровании комбинация, v_i - результат шифрования, ξ_i - параметр преобразования.

Для шифрования очередной информационной комбинации u_i, передаваемой от абонента с номером t к абоненту с номером g, находят в таблице $T_к$ исходное значение u_i, вычисляют разность значений адресов абонентов $\Delta=g-t$ по модулю 2^l, маскируют значение Δ с помощью случайно заполненной таблицы маскирования $T_м$, для чего считывают из таблицы $T_м$ по адресу Δ результат маскирования $\Delta_м$, используют значение $\Delta_м$ как параметр преобразования ξ_i шифруемого знака u_i, при этом шифрующее преобразование знака выполняют с помощью таблицы $T_к$ и дополнительной таблицы адресов T_a, в которой в строке с адресом u_i хранится адрес комбинации u_i в таблице $T_к$, определяют адрес комбинации u_i, вычисляют адрес результата преобразования как сумму по модулю 2^l адреса комбинации u_i и величины $\Delta_м$ и считывают результат преобразования v_i по вычисленному адресу из таблицы $T_к$, дешифрующее преобразование знака выполняют с помощью таблицы $T_к$ и дополнительной таблицы адресов T_a, в которой в строке с адресом v_i хранится адрес комбинации v_i в таблице $T_к$, определяют адрес комбинации v_i, вычисляют адрес результата преобразования u_i как разность по модулю 2^l адреса комбинации v_i и величины $\Delta_м$ и считывают результат преобразования u_i по вычисленному адресу из таблицы $T_к$.

При этом результат шифрования v_i исходной комбинации u_i при значении параметра преобразования $\Delta_м$ с использованием таблиц $T_к$ и T_a вырабатывают как значение комбинации, хранящейся в строке $A(v_i)$ таблицы $T_к$, адрес которой определяют как $A(v_i)=A(u_i)+\Delta_м$ по модулю числа N, где N - размер алфавита, совпадающий с числом строк таблиц $T_к$ и T_a.

Результат дешифрования u_i ранее зашифрованной комбинации v_i при значении параметра преобразования $\Delta_м$ с использованием таблиц $T_к$ и T_a вырабатывают как значение комбинации, хранящейся в строке $A(u_i)$ таблицы $T_к$, адрес которой определяют как $A(u_i)=A(v_i)-\Delta_м$ по модулю числа N, где N - размер алфавита, совпадающий с числом строк таблиц $T_к$ и T_a.

Случайное заполнение таблиц $T_к$ и $T_м$ неповторяющимися значениями чисел является ключом для шифрования и дешифрования.

Для передачи информации в широковещательном режиме всем абонентам сети используют маскированное с помощью таблицы $T_м$ значение параметра $\Delta=0$.

Заявленный способ обеспечивает шифрование информации на индивидуальных для каждой пары абонентов ключах при быстрой реализации криптографического преобразования; при этом сочетается большой объем ключа (две таблицы со случайным заполнением по 256 байт в каждой при байтовом преобразовании) с простой реализацией использования ключа в процессе обмена.

Описанный способ обладает следующими преимуществами:

- высокая скорость обработки информации;
- обеспечение после шифрования квазислучайной последовательности сигналов, независимо от статистики отдельных букв в исходном тексте;
- сложное преобразование, не имеющее никакого другого формального описания, кроме

описания заполнения кодовой таблицы $T_к$;

- возможность рассматривать начальное заполнение таблицы как ключ шифрования.

Источники информации

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: ГК СССР по стандартам, 1989.

2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 1999.

3. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. - СПб.: БХВ-Петербург, 2001.

4. Московский университет и развитие криптографии в России. Материалы конференции в МГУ 17-18 2002 г. - М.: МЦНМО, 2003. - 287 с.

Формула изобретения

1. Способ защиты информации в радио и локальной вычислительной сети с разграничением доступа к абонентам сети, характеризуемый шифрованием текстовой части пакета с индивидуальными для каждой пары абонентов ключами с помощью двухпараметрического шифрующего преобразования $v_i=F(u_i,\xi_i)$ и дешифрующего преобразования $u_i=F^{-1}(v_i,\xi_i)$ на основе случайной таблицы замены $T_к$ длиной 2^l знаков, где l - длина элемента алфавита, u_i - преобразуемая при шифровании комбинация, v_i - результат шифрования, ξ_i - параметр преобразования, для шифрования очередной информационной комбинации u_i, передаваемой от абонента с номером t к абоненту с номером g, находят в таблице $T_к$ исходное значение u_i, вычисляют разность значений адресов абонентов $\Delta=g-t$ по модулю 2^l, маскируют значение Δ с помощью случайно заполненной таблицы маскирования $T_м$, для чего считывают из таблицы $T_м$ по адресу Δ результат маскирования $\Delta_м$, используют значение $\Delta_м$ как параметр преобразования ξ_i шифруемого знака u_i, при этом шифрующее преобразование знака выполняют с помощью таблицы $T_к$ и дополнительной таблицы адресов T_a, в которой в строке с адресом u_i хранится адрес комбинации u_i в таблице $T_к$, определяют адрес комбинации u_i, вычисляют адрес результата преобразования как сумму по модулю 2^l адреса комбинации u_i и величины $\Delta_м$ и считывают результат преобразования v_i по вычисленному адресу из таблицы $T_к$, дешифрующее преобразование знака выполняют с помощью таблицы $T_к$ и дополнительной таблицы адресов T_a, в которой в строке с адресом v_i хранится адрес комбинации v_i в таблице $T_к$, определяют адрес комбинации v_i, вычисляют адрес результата преобразования u_i как разность по модулю 2^l адреса комбинации v_i и величины $\Delta_м$ и считывают результат преобразования u_i по вычисленному адресу из таблицы $T_к$.

2. Способ по п.1, отличающийся тем, что результат шифрования v_i исходной комбинации u_i при значении параметра преобразования $\Delta_м$ с использованием таблиц $T_к$ и T_a вырабатывают как значение комбинации, хранящейся в строке $A(u_i)$ таблицы $T_к$, адрес которой определяют как $A(v_i)=A(u_i)+\Delta_м$ по модулю числа N, где N - размер алфавита, совпадающий с числом строк таблиц $T_к$ и T_a.

3. Способ по п.1, отличающийся тем, что результат дешифрования и ранее зашифрованной комбинации v_i при значении параметра преобразования $\Delta_м$ с использованием таблиц $T_к$ и T_a вырабатывают как значение комбинации, хранящейся в строке $A(u_i)$ таблицы $T_к$, адрес которой определяют как $A(u_i)=A(v_i)-\Delta_м$ по модулю числа N, где N - размер алфавита, совпадающий с числом строк таблиц $T_к$ и T_a.

4. Способ по п.1, отличающийся тем, что случайное заполнение таблиц $T_к$ и $T_м$ неповторяющимся значением чисел является ключом для шифрования и дешифрования.

5. Способ по п.1, 2, отличающийся тем, что для передачи информации в широковещательном режиме всем абонентам сети используют маскированное с помощью

таблицы $T_м$ значение параметра Δ=0.