РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(19) **RU** (11) **2 373 653** (13) **C2**

(51) МПК
H04L 9/12 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2006112010/09, 13.09.2004**

(24) Дата начала отсчета срока действия патента:
13.09.2004

(30) Конвенционный приоритет:
12.09.2003 SE 0302456-9
12.09.2003 US 60/502,254

(43) Дата публикации заявки: **10.11.2007**

(45) Опубликовано: **20.11.2009** Бюл. № **32**

(56) Список документов, цитированных в отчете о поиске: **WO 0191366 A2, 29.11.2001. RU 2195079 C1, 20.12.2002. WO 0239660 A2, 16.05.2002. JP 2002342233 A, 29.11.2002.**

(85) Дата перевода заявки PCT на национальную фазу: **12.04.2006**

(86) Заявка PCT:
SE 2004/001314 (13.09.2004)

(87) Публикация PCT:
WO 2005/027404 (24.03.2005)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
ДАВИН Петер (SE)

(73) Патентообладатель(и):
СИКЬЮРЕД ИМЭЙЛ ГЕТЕБОРГ АБ (SE)

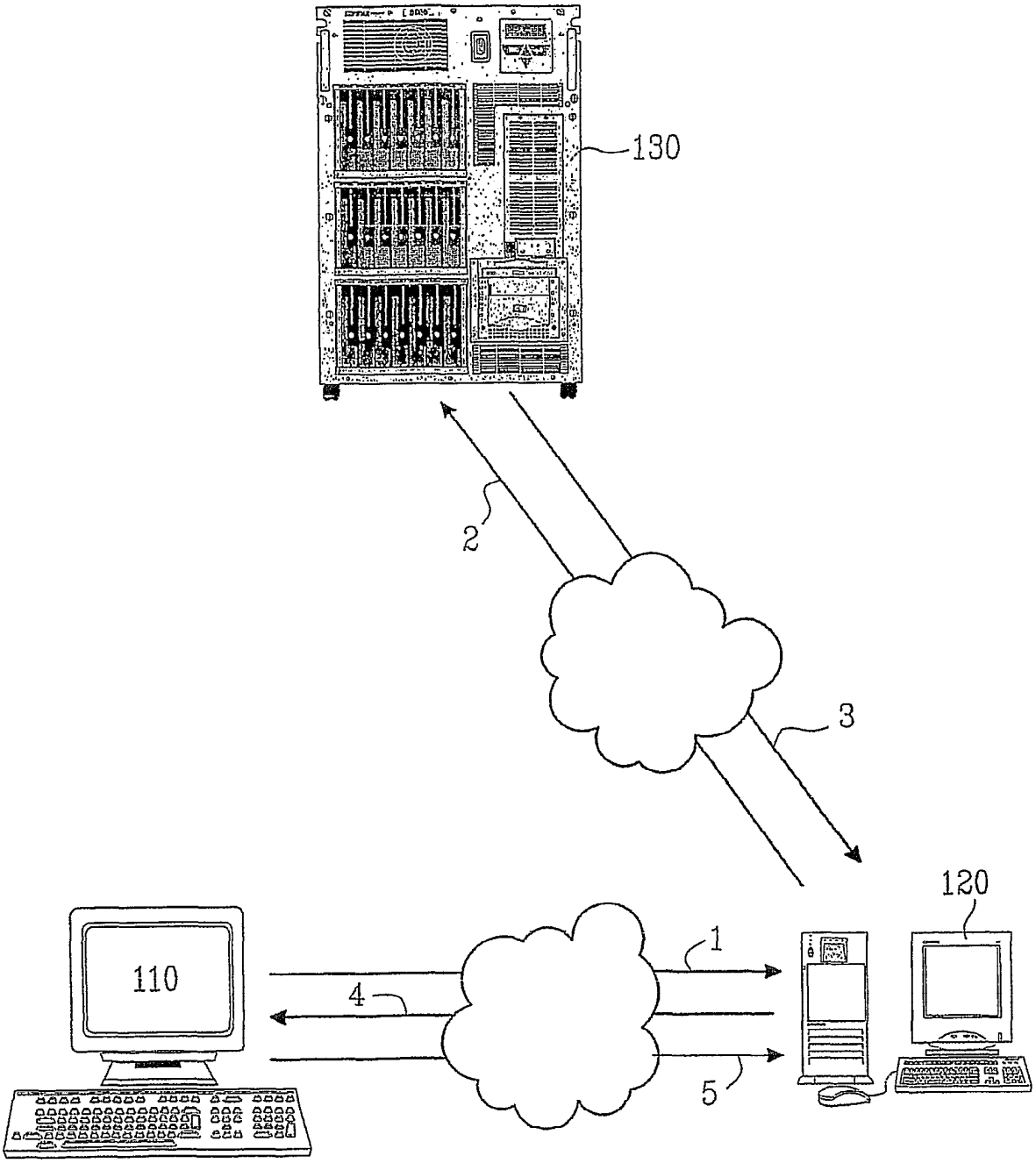
RU 2373653 C2

(54) БЕЗОПАСНОСТЬ СООБЩЕНИЙ

(57) Реферат:

Изобретение относится к области сетей передачи данных, а именно к способам передачи электронных сообщений, предпочтительно электронных писем. Технический результат заключается в обеспечении защиты в системе передачи электронной почты без необходимости повторного использования паролей или персональных ключей. Сущность изобретения заключается в том, что от первого пользователя, имеющего первый терминал, ко второму пользователю, имеющему второй терминал, передают электронное письмо в зашифрованной форме первым терминалом. Зашифрованное электронное письмо шифруют посредством ключа, сформированного первым генератором ключей, использующим начальное число; представляют второму пользователю начальное число для формирования ключа с помощью второго генератора ключа, предусмотренного во втором терминале; предоставляют и сохраняют начальное число во втором терминале;

используют начальное число вторым терминалом для формирования ключа каждый раз, когда принимают зашифрованное электронное письмо от первого пользователя ко второму пользователю; синхронизируют значения счетчика в каждом терминале; и формируют ключ на основе начального числа и значения счетчика в каждом терминале независимо от другого терминала. 3 н. и 22 з.п. ф-лы, 4 ил.



Фиг.1

RU 2373653 C2

RU 2373653 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 373 653** (13) **C2**

(51) Int. Cl.
H04L 9/12 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2006112010/09, 13.09.2004**

(24) Effective date for property rights:
13.09.2004

(30) Priority:
12.09.2003 SE 0302456-9
12.09.2003 US 60/502,254

(43) Application published: **10.11.2007**

(45) Date of publication: **20.11.2009 Bull. 32**

(85) Commencement of national phase: **12.04.2006**

(86) PCT application:
SE 2004/001314 (13.09.2004)

(87) PCT publication:
WO 2005/027404 (24.03.2005)

Mail address:
129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
DAVIN Peter (SE)

(73) Proprietor(s):
SIK'JuRED IMEhJL GETEBORG AB (SE)

RU 2373653 C2

(54) SAFETY OF MESSAGES

(57) Abstract:

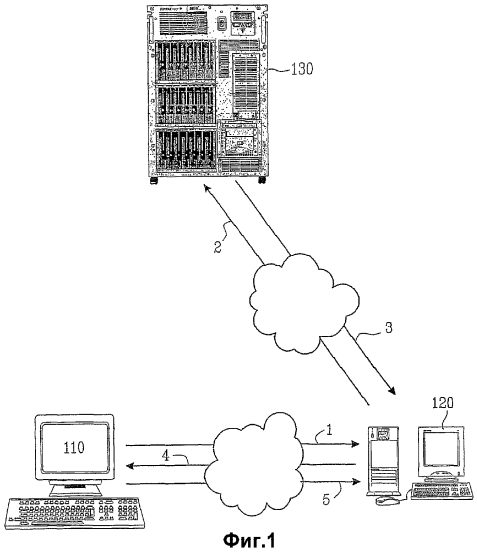
FIELD: communication facilities.

SUBSTANCE: invention elates to field defense data network, particularly to transmission methods of electronic messages, preferentially emails. Essence of invention is that from the first user, allowing the first terminal, to the second user, allowing the second terminal, it is transmitted email in encode form by the first terminal. Encoded email is ciphered by means of key, formed by the first key gun, using seed; provide to the second user seed for formation of key by means of the second key gun, provided in the second terminal; it is provided and saved seed in the second terminal; it is used seed by the second terminal for generation of key each time, when it is received scrambled email from the first user to the second user; synchronise value of metre in each terminal; and is generated key on the basis of seed and value of metre in each terminal, independently of the other terminal.

EFFECT: providing protection in email transmission system without necessity of reuse of passwords or personal keys.

25 cl, 4 dwg

RU 2373653 C2



Фиг.1

RU 2373653 C2

RU 2373653 C2

Область техники, к которой относится изобретение.

Настоящее изобретение относится к способу и системе для безопасной и шифрованной передачи сообщений, в частности электронной почты, в сетях связи.

Уровень техники

В настоящее время все более обычным становится обмен информацией через электронную почту (электронное письмо) как через доступ к Интернету, так и по другим интрасетям. Каждый день миллионы электронных писем отправляют по Интернет, включая многие типы информации. Передача по электронной почте также используется в компаниях и на предприятиях для внутренних и внешних связей. Многие из электронных писем содержат зависимую и секретную информацию.

К сожалению, все электронные письма не находят свое место назначения и могут даже быть приняты ошибочными адресатами. Кроме того, обычно не составляет сложности для неавторизованных лиц взломать серверы или сети доступа и прочитать электронные письма.

Предусмотрен ряд решений для отправки зашифрованных электронных писем: PGP (Pretty Good Privacy - досл. вполне хорошая секретность) (PGP и Pretty Good Privacy являются зарегистрированными торговыми марками корпорации PGP) является одним из приложений, которое используется для отправки зашифрованных электронных писем. Это приложение является подключаемым модулем для программ электронной почты, основанным на использовании открытых ключей. Два пользователя обмениваются открытыми ключами, которые затем могут быть использованы для того, чтобы шифровать и дешифровать электронные письма или другие файлы. Кроме того, когда электронное письмо шифруется и передается с открытым ключом получателя, отправляющая сторона не может получить доступ к электронному письму.

Также возможно предоставить документ и вложить его в электронное письмо и задать пароль получателя для доступа к вложению.

Оба этих решения подразумевают, что каждый раз, когда осуществляется доступ к новому зашифрованному файлу или электронной почте, должен быть использован пароль или персональный ключ. Пароли и персональный ключ могут быть забыты или попасть во владение неавторизованных лиц. Кроме того, тесты показывают, что многие люди, чтобы не забыть пароль/персональный ключ, используют имена родственников, ласкательные имена и т.д., которые могут быть легко угаданы, или даже делают записи.

В интернациональной патентной заявке WO 02/077773 описывается система, способ и компьютерный программный продукт для предоставления программы чтения и ответа зашифрованной электронной почты. Способ распределения и инициализации шифрованной электронной почты включает в себя: получение первым пользователем лицензии для прикладной программы клиентского программного обеспечения электронной почты, имеющей открытое/закрытое шифрование; запрос первым пользователем, чтобы второй пользователь загрузил прикладную программу программного обеспечения чтения/ответа для того, чтобы обменяться зашифрованной электронной почтой между первым и вторым пользователем; загрузку и установку прикладной программы чтения/ответа программного обеспечения вторым пользователем; отправку электронной почты вторым пользователем первому пользователю, включающей в себя внедренный незашифрованный открытый ключ, используя функцию отправки ключа прикладной программы чтения/ответа программного обеспечения; прием электронной почты от

второго пользователя первым пользователем, где незашифрованный открытый ключ внедрен в электронное письмо; ответ первого пользователя посредством отправки второго электронного письма первому пользователю, где прикладная программа чтения/ответа программного обеспечения шифрует сообщение второго электронного письма в зашифрованное сообщение с использованием незашифрованного открытого ключа второго пользователя; прием второго электронного письма вторым пользователем с зашифрованным сообщением как вложением от первого пользователя в прикладную программу электронной почты программного обеспечения третьей стороны, где прикладная программа электронной почты программного обеспечения третьей стороны отличается от прикладной программы чтения/ответа программного обеспечения и прикладной программы электронной почты клиентского программного обеспечения; и открытие вторым пользователем вложения, чтобы выполнить прикладную программу чтения/ответа программного обеспечения, действующую так, чтобы позволить пользователю без клиентского программного обеспечения электронной почты прочитать и ответить на зашифрованное электронное письмо, созданное и отправленное от пользователя, имеющего клиентское программное обеспечение электронной почты.

Опубликованная заявка (США) №2002059529 относится к системе защиты электронной почты для предварительно выбранных пользователей электронной почты, формирующей группу участвующих пользователей, требующую защищенную передачу, содержащей сервер безопасного списка, на который все защищенные электронные письма отправляются членами группы участвующих пользователей, сервер содержит запоминающее устройство для сертификационных данных и ЦП, который сравнивает имена подразумеваемых получателей каждого электронного сообщения с данными в запоминающем устройстве и обрабатывает сообщение, чтобы продвинуть вперед сертифицированную передачу, предусматривающую, что пользователь правильно сертифицирован, как указано данными в запоминающем устройстве. US 2003140235 относится к способу для обмена электронными сообщениями между отправителем с зарегистрированным набором биометрических признаков и получателем с зарегистрированным набором биометрических признаков, способ содержит: a. обмен зарегистрированными наборами биометрических признаков между отправителем и получателем; b. формирование отсканированного вживую набора биометрических признаков отправителя; c. формирование первого разностного ключа, полученного из разницы между отсканированным вживую набором биометрических признаков отправителя и зарегистрированным набором биометрических признаков отправителя; d. шифрование сообщения с помощью первого разностного ключа; e. шифрование упомянутого отсканированного вживую набора биометрических признаков отправителя с помощью ключа шифрования; f. передачу получателю зашифрованного сообщения и упомянутого зашифрованного отсканированного вживую набора биометрических признаков отправителя; g. дешифрование получателем упомянутого зашифрованного отсканированного вживую набора биометрических признаков отправителя; h. регенерацию получателем первого разностного ключа посредством вычисления разницы между упомянутым отсканированным вживую набором биометрических признаков отправителя и зарегистрированным набором биометрических признаков отправителя; и i. дешифрование сообщения посредством использования регенерированного первого разностного ключа.

WO 01/91366 относится к устройству и способу для формирования псевдослучайных

криптографических ключей в криптографических системах связи. Дана общая установка инициализации конфигурационных данных, псевдослучайные криптографические ключи могут быть дублировано сгенерированы различными независимыми псевдослучайными генераторами ключей криптографической системы связи.

WO 02/39660 относится к системе и способу для криптографической связи между множеством пользователей и центральным поставщиком услуг с использованием сгенерированных на своем месте криптографических ключей. Каждый пользователь связывается с центральным поставщиком услуг предпочтительно с использованием пользовательского интерфейса связи, который включает в себя локальный генератор ключей, который, после инициализации с пользовательским собственным индивидуальным начальным значением, генерирует уникальный криптографический ключ. Распределяя различные пользовательские индивидуальные уникальные начальные значения каждому пользователю, каждый пользовательский локальный генератор ключей формирует уникальный набор ключей. Центральный поставщик услуг также владеет локальным генератором ключей и также предпочтительно владеет копией всех индивидуальных начальных значений, назначенных авторизованным пользователям. Центральный поставщик услуг предпочтительно связывается безопасно зашифрованным образом с каждым пользователем с использованием криптографических ключей, сгенерированных из этих пользовательских индивидуальных начальных чисел. Распределение дополнительных значений начальных чисел, общих для более чем одного пользователя, через зашифрованную связь с использованием генераций уникальных индивидуальных криптографических ключей затем позволяет осуществить безопасный условный доступ упомянутым пользователям через шифрование сигнала с использованием генераций ключей, получившихся в результате значения начального числа, общего для предназначенной группы пользователей.

В OTP: Программа одноразового генератора-заполнителя является условно-бесплатной программой, распространяемой через Интернет (http: //www.fourmilab.ch/ontime), для формирования одноразовых заполнителей и парольных списков.

Раскрытие изобретения

Главной целью изучения согласно лучшему варианту осуществления настоящего изобретения является предоставить защищенную систему передачи электронной почты, позволяющую шифрование и дешифрование электронных писем без необходимости повторного использования паролей или персональных ключей. В частности, изобретение касается формирования синхронизированных ключей шифрования, по меньшей мере, в двух удаленных местоположениях для шифрования и дешифрования электронных писем или подобных сообщений.

Другой целью настоящего изобретения является предоставить систему передачи электронной почты, которая может фильтровать нежелательные электронные письма, так называемую несанкционированную рассылку (спам).

Еще другой целью настоящего изобретения является предоставить систему передачи электронной почты, которая способствует покупке программ программного обеспечения безопасной электронной почты.

По этим причинам изобретение согласно лучшему варианту осуществления относится к способу передачи электронного сообщения, предпочтительно электронного письма от первого пользователя, имеющего первый терминал, ко

второму пользователю, имеющему второй терминал, содержит этапы, на которых: передают указанное электронное письмо в зашифрованной форме упомянутым первым терминалом, упомянутое зашифрованное электронное письмо шифруют посредством ключа, сформированного первым генератором ключей, использующим начальное число, предоставляют однажды упомянутому второму пользователю упомянутое начальное число для формирования ключа с помощью второго генератора ключа, предусмотренного в упомянутом втором терминале, предоставляют и сохраняют упомянутое начальное число в упомянутом втором терминале, используют упомянутое начальное число упомянутым вторым терминалом для формирования ключа каждый раз, когда принимают зашифрованное электронное письмо от упомянутого первого пользователя к упомянутому второму пользователю, синхронизируют значение счетчика в каждом терминале; и формируют упомянутый ключ на основе упомянутого начального числа и значения счетчика в каждом терминале независимо от другого терминала.

Наиболее предпочтительно, что начальное число получают только первый раз в момент инициализации. Предпочтительно второе начальное число получают, если первое начальное число является непригодным, например, когда приложение переустанавливают или устанавливают на новый компьютер.

Согласно одному варианту осуществления, когда ряд электронных писем отправляют получателю, получают динамический серийный номер для каждого зашифрованного электронного письма. Динамический серийный номер используется для формирования ключа для соответствующего зашифрованного электронного письма.

Согласно одному варианту осуществления изобретение содержит дополнительные этапы, на которых синхронизируют значение счетчика в каждом терминале и формируют упомянутый ключ на основе упомянутого начального числа и значения счетчика в каждом терминале независимо от другого терминала. Начальное число сохраняется динамическим и сменным образом, по меньшей мере, в одном из терминалов, а предпочтительно во всех терминалах. Значение счетчика формируется в счетчике в каждом терминале, синхронизация значений счетчиков предполагает синхронизацию счетчиков. После первоначальной синхронизации счетчиков терминалы выполняют дополнительные этапы синхронизации только тогда, когда необходимо. Операция формирования ключа на основе начального числа и значения счетчика выполняется посредством алгоритма, сохраненного нединамическим и неизменяемым образом, по меньшей мере, в одном из терминалов.

Согласно одному варианту осуществления изобретение также содержит этап, на котором формируют список доверенных терминалов на основе принятого начального числа и принимают электронные письма только от терминалов, зарегистрированных в упомянутом списке. Таким образом несанкционированная рассылка может быть остановлена.

По причинам безопасности изобретение согласно лучшему варианту осуществления содержит этап, на котором предоставляют упомянутое начальное число упомянутым первым пользователем упомянутому второму пользователю посредством, по меньшей мере, одного из телефонного звонка, факса или письма.

Зашифрованное электронное письмо предусмотрено с вложениями, зашифрованными вместе с электронным письмом.

Изобретение также относится к системе для передачи электронных писем от первого пользователя ко второму пользователю. Система содержит в себе первый

терминал и второй терминал, система дополнительно содержит: средство для передачи упомянутого защищенного электронного письма в форме зашифрованного письма упомянутым первым терминалом, упомянутое зашифрованное электронное письмо шифруется посредством ключа, сформированного первым генератором ключа, использующим начальное число, средство для предоставления один раз упомянутому второму пользователю упомянутого начального числа для формирования ключа с помощью второго генератора ключа, средство для формирования ключа упомянутым вторым терминалом, использующим упомянутое начальное число, каждый раз, когда принимают зашифрованное электронное письмо от упомянутого первого пользователя к упомянутому второму пользователю.

Каждый терминал содержит модуль формирования ключа, который содержит память, в которой хранятся идентичные начальные числа, счетчик, чтобы периодически менять значение счетчика, и вычисляющий терминал, адаптированный для того, чтобы формировать в каждом терминале и независимо от других терминалов, а также ключ на основе оригинального значения и счетное значение, принятое от счетчика. Память для хранения начального числа, по меньшей мере, в одном из терминалов является динамической памятью, размещенной для того, чтобы хранить начальное число динамическим и сменным образом. Терминалы размещены так, чтобы чувствовать, когда они не синхронизированы до конца, чтобы затем восстановить синхронизацию. Вычисляющий модуль, по меньшей мере, одного из терминалов содержит алгоритм вычисления, который хранится нединамическим и неизменным образом и который предпочтительно является осуществленным аппаратно. Один из терминалов является центральным терминалом, содержащим множество начальных чисел для безопасной зашифрованной передачи, предполагающей несколько различных терминалов, имеющих одно оригинальное значение каждый.

Изобретение также относится к компьютерному программному продукту для передачи защищенной электронной почты от первого пользователя, имеющего первый терминал, ко второму пользователю, имеющему второй терминал, продукт содержит код для: шифрования и передачи упомянутой электронной почты из упомянутого первого терминала, формирования ключа с использованием упомянутого первого начального числа в упомянутом первом терминале, получения упомянутого начального числа для формирования ключа с помощью второго генератора ключа в упомянутом втором терминале, хранения упомянутого начального числа в упомянутом втором терминале, формирования ключа упомянутым вторым терминалом, использующим упомянутое сохраненное начальное число, каждый раз, когда принимают зашифрованное электронное письмо от упомянутого первого пользователя к упомянутому второму пользователю.

Изобретение также относится к распространяемому сигналу для передачи защищенной электронной почты от первого пользователя, имеющего первый терминал, ко второму пользователю, имеющему второй терминал, содержащему сигнал, который содержит код для: шифрования и передачи упомянутой электронной почты из упомянутого первого терминала, формирования ключа с использованием упомянутого первого начального числа в упомянутом первом терминале, получения упомянутого начального числа для формирования ключа с помощью второго генератора ключа в упомянутом втором терминале, хранения упомянутого начального числа в упомянутом втором терминале, формирования ключа упомянутым вторым терминалом, использующим упомянутое сохраненное начальное

число, каждый раз, когда принимают зашифрованное электронное письмо от упомянутого первого пользователя к упомянутому второму пользователю.

Изобретение также относится к машиночитаемому носителю, имеющему сохраненные на нем наборы инструкций для передачи защищенной электронной почты от первого пользователя, имеющего первый терминал, ко второму пользователю, имеющему второй терминал, упомянутый набор инструкций содержит код для: шифрования и передачи упомянутой электронной почты из упомянутого первого терминала, формирования ключа с использованием упомянутого первого начального числа в упомянутом первом терминале, получения упомянутого начального числа для формирования ключа с помощью второго генератора ключа в упомянутом втором терминале, хранения упомянутого начального числа в упомянутом втором терминале, формирования ключа упомянутым вторым терминалом, использующим упомянутое сохраненное начальное число, каждый раз, когда принимают зашифрованное электронное письмо от упомянутого первого пользователя к упомянутому второму пользователю. Носитель может быть модулем памяти.

Изобретение также относится к способу продажи набора инструкций для передачи и приема защищенной электронной почты от первого пользователя, имеющего первый терминал, ко второму пользователю, имеющему второй терминал. Способ содержит этапы, на которых: передают упомянутую защищенную электронную почту в зашифрованной упомянутым первым терминалом форме, упомянутая зашифрованная электронная почта шифруется посредством ключа, сформированного первым генератором ключа с использованием начального числа, предоставляют упомянутую защищенную электронную почту с доступным сообщением относительно места производителя, получают из упомянутого места производителя второй набор инструкций для дешифрования упомянутой электронной почты и дебетуют упомянутого второго пользователя для использования упомянутого второго набора инструкций для шифрования новой электронной почты. Наиболее предпочтительно, что способ является компьютеризированным. Выставление счета происходит после заказа или приема упомянутого второго набора инструкций. Второй набор инструкций является кодом доступа к предварительно установленному набору инструкций.

Изобретение также относится к способу фильтрации электронных писем к получателю от первого пользователя, имеющего первый терминал, к получателю, являющемуся вторым пользователем, имеющим второй терминал, упомянутое электронное письмо передают в зашифрованной упомянутым первым терминалом форме, упомянутое зашифрованное электронное письмо шифруют посредством ключа, сформированного первым генератором ключа с использованием начального числа, предоставляют один раз упомянутому второму пользователю упомянутое начальное число для формирования ключа с помощью второго генератора ключа, предусмотренного в упомянутом втором терминале, формируют список доверенных отправителей посредством упомянутого второго терминала на основе отношения отправитель-получатель, сформированного упомянутым начальным числом, и производят действие при приеме электронного письма на основе упомянутого списка. Действие может быть одно из сохранения, удаления или возвращения упомянутого электронного письма.

Краткое описание чертежей

В последующем изобретение будет описано со ссылкой на раскрытые схематические

чертежи, иллюстрирующие предпочтительные варианты осуществления изобретения:

Фиг.1 - блок-схема по этапам связи в сети согласно изобретению,

Фиг.2 - блок-схема, иллюстрирующая компьютерный терминал,

Фиг.3 - блок-схема, иллюстрирующая этапы части изобретения, и

Фиг.4 - блок-схема, иллюстрирующая часть изобретения.

Детальное описание предпочтительных вариантов осуществления изобретения

В своей основе изобретение дает возможность предоставления начального числа инициализации системе как от отправляющей, так и от принимающей стороны, и формирует для каждого электронного письма различные, но в каждом терминале отправителя/получателя одинаковые ключи шифрования, основанные на одном и том же начальном числе без необходимости предоставления начального числа каждый раз, когда передается электронное письмо. Настоящее изобретение согласно предпочтительному варианту изобретения является приложением, реализованным как добавление к программе электронной почты, такой как Microsoft Outlook, Lotus Notes, Outlook Express и т.д. В последующем не ограничивающие примеры даны относительно Microsoft Outlook. Однако понимается, что идеи изобретения могут быть применены к любому приложению/системе передачи данных в целом и приложению/системе передачи электронной почты в частности. Изобретение может, таким образом, быть также применено к передаче SMS и MMS.

Фиг.1 иллюстрирует схематический поток информации между двумя пользователями, использующими компьютерные терминалы для отправки и приема электронных писем. Передающий терминал обозначен как 110, а получатель как 120. Очевидно, что два терминала даны как пример, и изобретение может быть применено на нескольких терминалах. Связь между терминалами ведется через Интернет или интранет с использованием работающего сервера электронной почты, например сервера Exchange Server.

Система изобретения создает защищенный путь для передачи электронной почты. Каждое отношение отправитель/получатель между двумя адресами электронной почты связано уникально (канал). Система управляет каждой парой отправитель/получатель с их собственными конкретными ключами шифрования.

Согласно блок-схеме на фиг.1 пользователь терминала 110 отправляет (1) электронное письмо пользователю принимающего терминала 120. Терминал 110 оснащен приложением согласно настоящему изобретению, которое шифрует электронные письма. В последующем примере отправителю присвоен адрес электронной почты «110@mail.com», а получателю - «120@mail.com». Электронное сообщение шифруется с использованием обычного алгоритма шифрования, такого как SHS-1, Blowfish или подобным, и закрывается ключом шифрования. Если приложение шифрования обнаруживает, что получатель не является одним из доверяемых получателей, т.е. получатель не находится в регистре получателей, обеспеченных приложением дешифрования или паролем дешифрования, приложение запрашивает отправителя, чтобы обеспечить инициирующим паролем или секретом конкретного получателя. Секрет, предоставленный отправителем, например 120xxx, хранится в системе вместе с другой уместной информацией (такой как адрес электронной почты) о получателе. Секрет используется:

- для формирования ключа и инициализации канала, имеющего ключ, например 110120xxx, который используется для передачи электронных писем получателю 120;

- для формирования ключа, например 120110xxx, который используется, когда

принимают электронные письма от 120; и

- формирования уникального ключа шифрования для передачи электронных писем. Формирование ключа описано более подробно далее.

Должно быть указано, что канал в данном документе относится к виртуальному каналу и касается отношения отправитель-получатель, которое применяется в настоящий момент времени.

Если получатель не имеет приложения дешифрования, электронное письмо предоставляется с незашифрованным сообщением получателю о том, что электронное письмо зашифровано и с доступом (2) к поставщику 130 программы, например поставщику услуг Интернета, для того, чтобы получить/загрузить (3) программу дешифрования. Зашифрованное электронное письмо может также быть отправлено как вложение в сообщение (информация) электронного письма. Если ключ отсутствует, т.е. получатель не принял разрешения дешифрования, после установки программы дешифрования получатель инструктируется о том, чтобы получить «секрет» для того, чтобы иметь возможность сформировать ключ для дешифрования электронной почты. Получатель может, например, запросить (4) отправителя о том, чтобы получить (6) секрет для того, чтобы инициировать формирование ключа. Когда часть шифрования установлена и секрет вставлен, зашифрованное электронное письмо может быть дешифровано. Приложение у получателя хранит информацию об отправителе и:

- формирует ключ и инициирует канал, имеющий ключ, например 120110xxx, который используется для передачи электронных писем получателю 110;

- инициирует канал, использующий ключ, например 110120xxx, который используется, когда принимают электронные письма от 120; и

- формирует уникальный ключ шифрования для приема электронных писем от отправителя 110.

Таким образом, создается отношение отправитель-получатель.

На последующих этапах, т.е. когда создается отношение, как отправитель, так и получатель имеют инициированные ключи, нет необходимости для нового обмена секретами или паролями. Приложения отправителя и получателя на каждом терминале будут автоматически идентифицировать и формировать ключ шифрования/дешифрования, например, на основе адреса электронной почты отправителя/получателя.

В следующий раз, когда электронное письмо посылается от 110 к 120, приложение отправителя обнаруживает, что получатель 120 является зарегистрированным и формирует новый уникальный ключ шифрования для электронного письма на основе сформированного канала. Ключ используется для того, чтобы зашифровать сообщение. Вместе с электронным письмом отправляется динамический серийный номер, который идентифицирует порядок электронного письма и используемый ключ.

На месте получателя приложение дешифрования обнаруживает динамический серийный номер ключа шифрования, использованного для шифрования сообщения. Приложение дешифрования формирует ключ на основе динамического серийного номера (и ранее сохраненного секрета) и дешифрует электронное письмо. Если динамический серийный номер не является последовательным, например электронное письмо с меньшим серийным номером принято позже, чем письмо с большим серийным номером, приложение формирует и хранит все ключи до серийного номера, который используется для дешифрования конкретного зашифрованного электронного письма. Все сохраненные ключи могут затем быть использованы для дешифрования

непоследовательных электронных писем. Ключи хранятся зашифрованными в модуле памяти/хранения и могут быть уничтожены после дешифрования соответствующего зашифрованного электронного письма. Таким образом, изобретение может также позволить дешифрование электронных писем гораздо позже, а также в режиме оффлайн.

Отправляющая сторона или приложение электронной почты может снабжать сообщение параметрами настройки, которые будут заставлять принимающую сторону или приложение электронной почты предпринимать определенное действие. Например, отправляющая сторона может потребовать, чтобы принятое сообщение хранилось определенным образом, например, как зашифрованное, в противном случае не сохранялось совсем. Это гарантирует то, что отправляющая сторона уверена, что сообщения хранятся в местоположении получателя таким образом, что нет данного неавторизованного доступа к сообщениям. Возможны другие возможные инструкции, и вышеупомянутый пример приведен только для иллюстративных целей и не ограничивает изобретение, например отправляющая сторона может потребовать немедленное удаление сообщения электронной почты после просмотра и для максимальной безопасности может не позволить ему быть сохраненным каким-либо способом.

Каждый терминал 210, например обычный ПК, схематически иллюстрированный на фиг. 2, содержит в себе центральный процессор 240, ROM (постоянное запоминающее устройство) 250, RAM (оперативное запоминающее устройство) 260 и модуль 270 хранения программы. ROM содержит набор инструкций, например, для функциональности терминала. RAM хранит инструкции из прикладных программ. Модуль хранения программы включает в себя прикладные программы, такие как приложение электронной почты, приложения шифрования и дешифрования и т.д.

Приложение 280 формирования ключей содержит в модуле хранения или RAM идентичные оригинальные значения SID, так называемые начальные числа, предпочтительно динамическим и взаимозаменяемым образом. Хранение оригинальных значений предпочтительно производится вместе с предварительной инициализацией приложения и полезно может быть выполнено через защищенный канал, например, посредством зашифрованного сообщения или телефонного звонка и т.п. Возможно, однако, что нет необходимости передавать оригинальные значения физически, а вместо этого пользователи связанных модулей могут сами ввести предварительно согласованное значение. Кроме того, оригинальные значения могут быть обменяны, когда необходимо, но альтернативно одинаковые оригинальные значения используются во время всего срока службы модуля формирования ключей. В этом случае оригинальные значения не нужно сохранять в динамической памяти, а вместо этого может быть использована постоянная память.

Кроме того, приложение формирования ключей управляет счетчиком 281, чтобы периодически менять значение X счетчика, а вычислительный модуль/приложение 282 адаптирован для того, чтобы формировать в каждом и во всех модулях независимо от других модулей ключ на основе оригинального значения, а значение счетчика выдается счетчиком.

Тем не менее полезно, чтобы счетчик и вычислительный модуль могли быть интегрированы в одном и том же модуле, который полезно может быть процессором (CPU). Осциллятор 283 или генератор тактовых импульсов, который также может быть интегрирован в процессор, может полезно управлять счетчиком. Предпочтительно используется генератор тактовых импульсов в реальном

времени CPU. Кроме того, счетчик увеличивается пошагово, посредством чего становится легче держать терминалы в фазе друг с другом (синхронизированными).

Предусмотрено, что одинаковые оригинальные значения хранятся в памяти и что счетчики синхронизированы так, чтобы предоставлять одинаковое значение счетчика, идентичные ключи могут быть сформированы в нескольких приложениях формирования ключей независимо друг от друга, т.е. в каждом терминале, запускающем приложение.

Эти ключи могут затем быть использованы для шифрования или целей авторизации между терминалами.

Более того, модули формирования ключей предпочтительно адаптированы так, чтобы опознавать, синхронизированы ли они или нет, и в случае когда они не синхронизированы, осуществлять синхронизацию. Опознавание может быть выполнено средствами конкретного теста синхронизации, который выполняется перед формированием ключей.

Альтернативно, необходимость синхронизации может, однако, быть идентифицирована, когда используются разные ключи, и только после этого может быть осуществлено восстановление синхронизации. Синхронизация может быть выполнена, например, посредством обмена значениями счетчика между модулями.

Согласно одному примеру вычислительный модуль содержит алгоритм F вычисления, который хэширует оригинальное значение (начальное число), настоящий ключ и значение счетчика как входные параметры. После этого значение счетчика увеличивается числом, т.е. count=count+1. Этот алгоритм вычисления предпочтительно осуществлен аппаратно в вычислительном модуле или альтернативно он хранится в нединамической и неизменяемой памяти. Алгоритм вычисления предпочтительно формирует 160-битный ключ, но, разумеется, также возможны ключи других длин. Каждый раз формирователю ключей дается команда выработать новый ключ после того, как формируется новое псевдослучайное 160-битное слово, которое вычисляется на основе «начального числа» и значения счетчика.

Приложение формирования ключей может дополнительно содержать часть интерфейса, служащую для того, чтобы разрешить связь между модулем связи и модулем формирования ключей. Предпочтительно эта связь содержит распространение инструкций модулю формирования ключей для того, чтобы сформировать ключ, и распространение, таким образом, сформированного ключа назад к модулю связи.

Модуль формирования ключей может быть осуществлен аппаратно и выполнен в форме интегрированной схемы, таким образом делая его более трудным для несанкционированного вмешательства. Схема может затем быть добавлена и использоваться по существу вместе с любым типом связывающегося модуля. Например, возможно использовать модуль формирования ключей в соответствии с изобретением вместе с приложениями электронной почты.

Приложения формирования ключей в соответствии с изобретением могут быть использованы или для соединения точка-точка, или для авторизации, т.е. между двумя терминалами, или между центральным модулем, сервером электронной почты, или несколькими пользователями, клиентами. Такой центральный модуль предпочтительно содержит множество разных приложений формирования ключей, один для каждого клиента/пользователя/терминала в связи с центральным модулем. Альтернативно модуль ключей может содержать несколько разных оригинальных значений, в каждом случае команда модулю формирования ключей сформировать

ключ также содержит информацию, принимая во внимание которую может быть использовано оригинальное значение. Также возможно для нескольких модулей, что связь с центральным модулем для того, чтобы иметь модули формирования идентичных ключей, разрешает им связываться с одним и тем же модулем формирования ключей в центральном модуле.

Далее описывается зашифрованная передача или аутентификация с помощью вышеописанной системы. На первом этапе электронное письмо создают и шифруют с ключом, сформированным приложением формирования ключей в одном из терминалов. Электронное письмо может содержать одно или несколько вложений, например, в форме файла обработанного текста, файла изображения, JAVA-апплетов или любых других цифровых данных. Таким образом, электронное письмо согласно изобретениям относится к сообщению с или без вложения. Электронное письмо передают принимающему терминалу, и получатель опрашивается, чтобы получить значение инициации, так называемый секрет или начальное число. Вводя секрет в приложение дешифрования получателя, инициализируются терминалы для дальнейшей взаимосвязи, в процессе которой они предоставлены с идентичными оригинальными значениями и предпочтительно также синхронизированы. Система теперь готова для использования, а в следующий раз, который может произойти по прошествии произвольного периода времени после инициализации, и, по меньшей мере, один из терминалов идентифицирует себя с другим. Идентификации достигают, когда другой терминал определяет, известна ли данная идентичность и имеет ли он соответствующее приложение формирования ключей, т.е. приложение формирования ключей как определенное выше и с соответствующим оригинальным значением. Если это как раз такой случай, процесс переходит к следующему этапу, иначе процесс прерывается.

Вычисленные ключи затем используют, чтобы выполнить шифрование/дешифрование/аутентификацию. Должно быть понятно, однако, что шифрованная передача и аутентификация, конечно, могут быть выполнены одновременно и в одном и том же процессе. Шифрование и аутентификация могут быть выполнены, по существу, с помощью любого алгоритма шифрования, который использует ключи, например, как известный DES и RC6, Bluefish и т.д.

Другое преимущество изобретения в том, что приложение может быть использовано как фильтр для блокировки нежелательных электронных писем. Сегодня сотни и тысячи рекламных электронных писем отправляют получателям. В Outlook, например, есть функция, называемая «ненужная почта», которая на основе списка имен или некоторых параметров отправляет принятые электронные письма в папку ненужной почты. Эта функция, однако, не работает, когда имена отправителей и содержимое ненужных электронных писем изменяются. Изобретение уделяет внимание этой проблеме следующим образом.

Как упоминалось выше со ссылкой к фиг.3, принимающий терминал или сервер, содержащий список пар отправитель-получатель, проверяет 300 полученный адрес в списке и сравнивает 310 адрес отправителя с сохраненными адресами. Если электронное письмо может быть дешифровано, т.е. адрес отправителя находится в списке, электронное письмо дешифруют 320 и передают получателю. Если электронное письмо не может быть дешифровано, т.е. адрес отправителя не находится в списке, электронное письмо или удаляют в хранилище ненужной почты, или возвращают 330 отправителю. Сообщение может быть вложено в возвращаемое электронное письмо, например, уведомляющее отправителя нежелательных

электронных писем, что нужна программа шифрования для того, чтобы отправлять электронные письма предназначенному получателю. Конечно, электронное письмо может быть отправлено отправителем, который не находится в списке, но желателен. По этой причине система может хранить 340 копию электронного письма или только уведомить получателя так, что отправитель может быть уведомлен, чтобы установить приложение шифрования и получить секрет от получателя. Очевидно, что функция фильтрации/блокирования является опциональным применением.

Как упоминалось выше, изобретение также позволяет приобретение всего приложения или частей приложения простым способом.

График на фиг. 4 иллюстрирует автоматическую систему 400 приобретения. Получатель 401 принимает информационное электронное письмо, в которое вложено зашифрованное электронное письмо, чтобы получить программу дешифрования. Предпочтительно программа дешифрования предусмотрена бесплатной или условно бесплатной. Однако программа шифрования должна быть приобретена. Когда программа дешифрования загружается, также загружается программа шифрования, но не может быть использована до тех пор, пока не предоставлен лицензионный номер, пароль или подобное. По этой причине покупатель направляется по адресу 410 приобретения, например, в Интернете, откуда может быть получена лицензия. Сайт приобретения может потребовать специальную информацию о стране, языке и т.д. покупателя для того, чтобы могла быть получена правильная версия. Затем покупатель перенаправляется на сайт 420 заказа для предоставления информации о сделке. Плательщик может выполнить операцию известным образом, например, заплатив кредитной картой, банковской операцией, наложенным платежом и т.д. В зависимости от способа операции делается очистка 430 или управление 440. Если операция принята, сайт 420 приобретения отправляет информацию на регистрацию 450 и команду отделу 460 доставки. Отдел доставки отправляет либо программный пакет, либо лицензионный номер, либо какую-либо другую информацию, необходимую для (установки и) запуска программы шифрования. Отделение доставки может доставить программный пакет/лицензионную информацию. Если программа предварительно установлена, пароль/лицензионный номер может быть доставлен (зашифрованным) электронным письмом или загружен с сайта.

Также возможно предоставить электронное письмо от отправителя, информирующее получателя о необходимости получить приложение дешифрования/шифрования, со ссылкой на сайт, включая в себя предварительно оплаченную загрузку программы, также включающую в себя секрет для того, чтобы дешифровать электронное письмо. Однако в этом случае получатель может получить пароль или другие возможности доступа к программе.

Также возможно предоставить серверное размещение, через которое проходят зашифрованные электронные письма, например, посредством туннелирования адресов. В этом случае каждое электронное письмо может быть оплачено отдельно (так называемый тикер), таким образом без необходимости приобретения программы(программ).

Вышеупомянутые примеры относятся к сети, где пользователи используют два терминала для доступа к электронным письмам. Изобретение может также быть применено в случаях, где пользователи используют разные терминалы. В этом случае программа шифрования/дешифрования и начальное число могут быть предоставлены как мобильное приложение, например, в форме вставленного аппаратного средства

(например, USB-ключа), сохраненного на носителе информации, таком как CD и т.д. Таким образом, каждый раз должно быть предусмотрено использование ключа/хранилища приложения электронной почты такое, что приложение шифрования/дешифрования может быть выполнено из него.

В сети, например в организации или на предприятии, сервер управляет клиентами в IP-сети. Клиентам нужно только создать один защищенный канал электронной почты с сервером обслуживания, и этот сервер затем управляет защищенными соединениями с другими пользователями в сети. Каждый пользователь снабжается уникальным паролем для того, чтобы иметь доступ к сообщениям электронной почты и отправлять сообщения электронной почты согласно настоящему изобретению. Кроме того, администратор сети может быть снабжен мастер-паролем, который разрешает администратору доступ к сообщениям и администрировать учетные записи. Для того чтобы еще больше повысить безопасность, возможно потребовать, чтобы администратор использовал аппаратный модуль, формирующий уникальный последовательный номер, который используется для целей аутентификации. Этот уникальный последовательный номер управляется в противоположность другому модулю аппаратного и программного обеспечения, расположенного, например, в центральном сервере, базирующийся на сервере модуль формирует последовательный номер, который является идентичным со сформированным модулем администраторов, если есть правильный аппаратный модуль, и они синхронизируются друг с другом. Если они не являются идентичными, две системы будут пытаться синхронизироваться друг с другом определенное количество раз.

Такой аппаратный модуль для использования администратором может быть снабжен, например, но не ограничиваться этим, аппаратными подключаемыми устройствами, использующими USB (универсальная последовательная шина), RS232, RS485, Ethernet, Firewire, Bluetooth, Centronics, SecureDigital, PCMCIA, PC-Card или похожие стандарты соединяемости аппаратных средств. Также возможно взамен аппаратного модуля использовать программный модуль, расположенный либо на административном ПК, либо на рабочей станции, либо на подобном вычислительном устройстве, или на компьютерном запоминающем устройстве, соединяемом с сетью или соединяемым с устройством, соединенным с администрируемой сетью.

Также возможно предоставить систему с возможностями сжатия для сжатия зашифрованных электронных писем. Любой традиционный способ сжатия может быть использован.

Опционально зашифрованные и/или дешифрованные электронные письма могут быть сохранены в дешифрованной или зашифрованной форме. В этом случае предпочтительно, что электронные письма шифруются с использованием пароля. По причинам безопасности, особенно в компаниях, должен быть персональный пароль или один мастер-ключ (сетевой администратор).

Изобретение не ограничено вариантами осуществления, описанными и иллюстрированными. Изобретение может быть модифицировано в рамках прилагаемой формулы изобретения несколькими способами в зависимости от приложений, потребностей и нужд.

Формула изобретения

1. Способ инициирующей передачи электронного сообщения, предпочтительно электронного письма, от первого пользователя, имеющего первый терминал, ко второму пользователю, имеющему второй терминал, способ содержит этапы, на

которых:

управляют списком для идентификации второго пользователя,

принимают ключ шифрования от первого пользователя,

устанавливают виртуальный канал на основании идентификации первого и второго пользователей,

отправляют первое зашифрованное сообщение, зашифрованное с помощью ключа, от первого терминала ко второму терминалу, и

предоставляют второму пользователю ключ шифрования.

2. Способ по п.1, который также содержит этапы, на которых:

передают электронное сообщение в зашифрованной форме первым терминалом, зашифрованное электронное сообщение зашифровано посредством ключа, сформированного первым генератором ключей с использованием начального числа,

предоставляют один раз второму пользователю начальное число для формирования ключа с помощью второго генератора ключей, предусмотренного во втором терминале,

предоставляют и сохраняют начальное число во втором терминале,

используют начальное число посредством второго терминала для формирования ключа каждый раз, когда принимается зашифрованное электронное сообщение от первого пользователя ко второму пользователю;

синхронизируют значение счетчика в каждом терминале; и

формируют ключ на основе начального числа и значения счетчика в каждом терминале независимо от другого терминала, и

получают динамический серийный номер для каждого зашифрованного электронного сообщения, используемый для формирования ключа для соответствующего зашифрованного сообщения.

3. Способ по п.1, в котором уникальный идентификатор является адресом электронной почты.

4. Способ по п.2, в котором начальное число получают только первый раз во время инициализации.

5. Способ по п.2, в котором второе начальное число получают, если начальное число является непригодным.

6. Способ по п.2, в котором начальное число сохраняют динамическим и сменным образом, по меньшей мере, в одном из терминалов, а предпочтительно во всех терминалах.

7. Способ по п.1 или 6, в котором значение счетчика формируют в счетчике в каждом терминале, синхронизация значений счетчиков предполагает синхронизацию счетчиков.

8. Способ по п.1, в котором, вслед за начальной синхронизацией счетчиков, терминалы выполняют также этапы синхронизации, только когда необходимо.

9. Способ по п.1, в котором операцию формирования ключа на основе начального числа и значения счетчика выполняют посредством алгоритма вычисления, сохраненного нединамическим и неизменяемым образом, по меньшей мере, в одном из терминалов.

10. Способ по п.2, который содержит этап, на котором формируют список доверенных терминалов на основе принятого начального числа.

11. Способ по п.10, который содержит этап, на котором принимают электронные письма только от зарегистрированных в упомянутом списке.

12. Способ по п.1, который содержит этап, на котором предоставляют начальное

число первым пользователем второму пользователю посредством, по меньшей мере, одного из телефонного звонка, факса или письма.

13. Способ по п.1, в котором зашифрованное электронное сообщение предоставляют с вложениями, зашифрованными вместе с электронным письмом.

14. Способ по п.1, в котором передающая сторона снабжает сообщение параметрами настройки, которые заставляют принимающую сторону выполнить определенное действие.

15. Способ по п.1, в котором сетевого администратора снабжают мастер-паролем, который разрешает администратору доступ к сообщениям и администрированию учетных записей.

16. Способ по п.15, в котором администратору предоставляют аппаратный модуль, формирующий уникальный последовательный номер, который используется для целей аутентификации.

17. Система для передачи электронного сообщения, предпочтительно электронного письма, от первого пользователя, использующего первый терминал, ко второму пользователю, использующему второй терминал, система содержит:

устройство для управления списком для идентификации второго пользователя, сохраненным в модуле памяти,

устройство ввода для приема ключа шифрования от первого пользователя,

устройство для установления виртуального канала на основании идентификации первого и второго пользователей,

устройство связи для отправления первого зашифрованного сообщения, зашифрованного с помощью ключа, от первого терминала ко второму терминалу, и

устройство для предоставления второму пользователю ключа шифрования.

18. Система по п.17, которая также содержит:

средство для передачи защищенного электронного письма в форме зашифрованной почты посредством первого терминала, зашифрованную электронную почту шифруют посредством ключа, сформированного посредством первого генератора ключей с использованием начального числа,

средство для обеспечения один раз второго пользователя начальным числом для формирования ключа с помощью второго генератора ключей,

средство для предоставления и средства для хранения начального числа во втором терминале,

средство для формирования ключа каждый раз, когда принимают зашифрованное электронное письмо от первого пользователя ко второму пользователю посредством второго терминала с использованием начального числа;

каждый терминал содержит в себе модуль формирования ключей, модуль формирования ключей содержит память, в которой хранятся идентичные начальные числа, счетчик, чтобы периодически менять значение счетчика, и вычислительный терминал, адаптированный для того, чтобы формировать в каждом терминале и независимо от других терминалов ключ на основе оригинального значения и значения счетчика, выданного из счетчика, причем терминалы выполнены с возможностью опознавать, когда они не синхронизованы, и затем сбрасывать синхронизацию; и

средство для получения динамического серийного номера для каждого зашифрованного электронного сообщения, используемого для формирования ключа для соответствующего зашифрованного сообщения.

19. Система по п.18, в которой память для хранения начального числа, по меньшей мере, в одном из терминалов является динамической памятью, размещенной, чтобы

хранить начальное число динамическим и сменным образом.

20. Система по п.17, в которой вычисляющий модуль, по меньшей мере, одного из терминалов содержит алгоритм вычисления, который хранится нединамическим и неизменным образом, и который предпочтительно является осуществленным аппаратно.

21. Система по п.17, в которой один из терминалов является центральным терминалом, содержащим множество начальных чисел для безопасной зашифрованной передачи, предполагающей несколько разных терминалов, имеющих одно оригинальное значение каждый.

22. Система по п.17, которая содержит первый модуль для формирования уникальной последовательности номеров, который управляется в отношении ко второму модулю, расположенному в системе, который формирует последовательный номер, который является идентичным сформированному первым модулем, и, если это правильный модуль, они синхронизируются друг с другом.

23. Машиночитаемый носитель, имеющий сохраненные на нем наборы инструкций для передачи защищенной электронной почты от первого пользователя, имеющего первый терминал, ко второму пользователю, имеющему второй терминал, набор инструкций содержит код для:

управления списком для идентификации второго пользователя;

приема ключа шифрования от первого пользователя;

установления виртуального канала на основании идентификации первого и второго пользователей,

отправки первого зашифрованного сообщения, зашифрованного с помощью ключа, от первого терминала ко второму терминалу, и

предоставления второму пользователю ключа шифрования.

24. Носитель по п.23, который также содержит инструкции для:

шифрования и передачи электронного письма из первого терминала,

формирования ключа с использованием первого начального числа в первом терминале,

получения начального числа для формирования ключа с помощью второго генератора ключей во втором терминале,

хранения начального числа во втором терминале,

формирования ключа каждый раз, когда принимают зашифрованное электронное письмо от первого пользователя ко второму пользователю, вторым терминалом с использованием сохраненного начального числа;

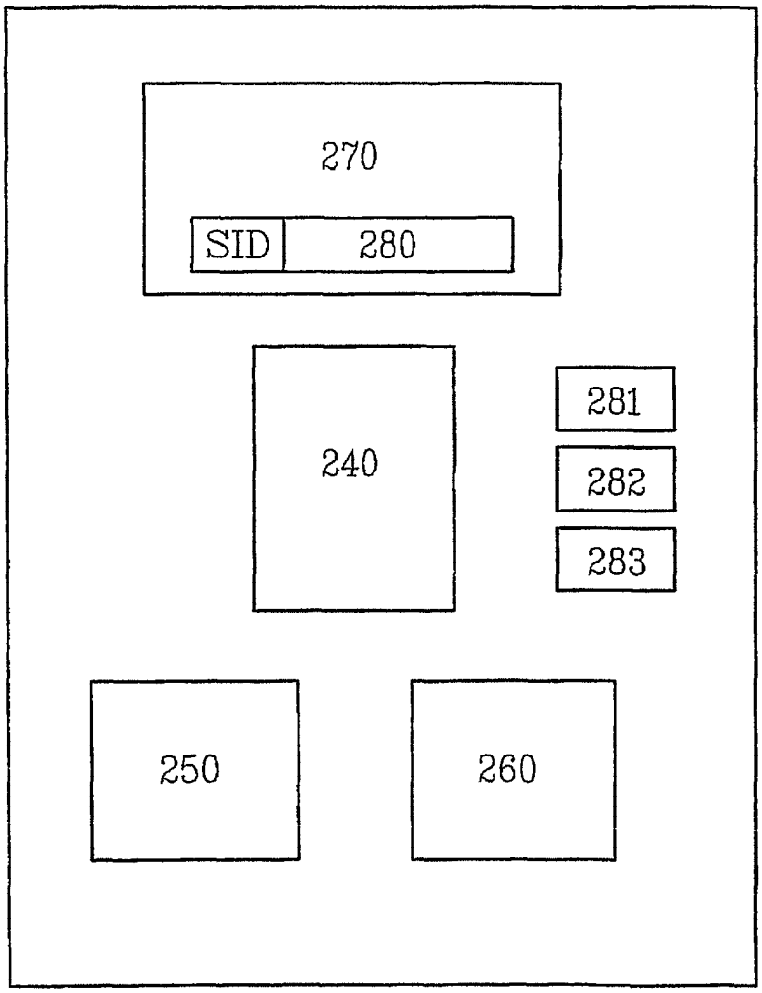
получения динамического серийного номера для каждого зашифрованного электронного сообщения, используемого для формирования ключа для соответствующего зашифрованного сообщения;

формирования ключа для соответствующего зашифрованного электронного письма с использованием динамического серийного номера;

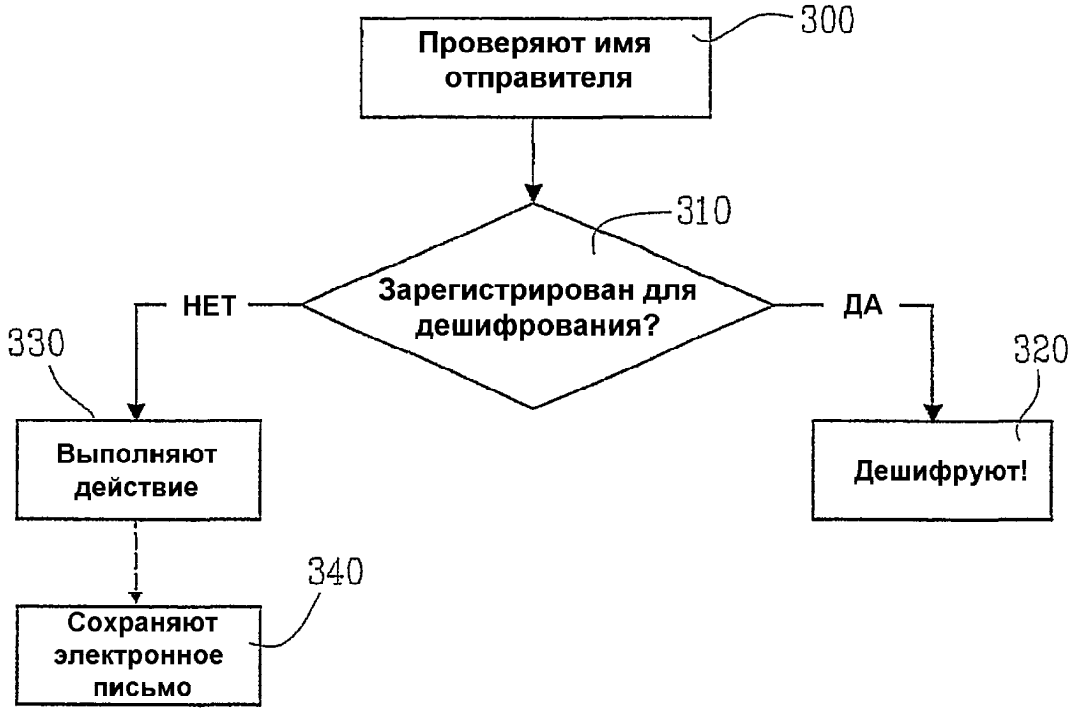
синхронизации значения счетчика в каждом терминале; и

формирования ключа на основе начального числа и значения счетчика в каждом терминале независимо от другого терминала.

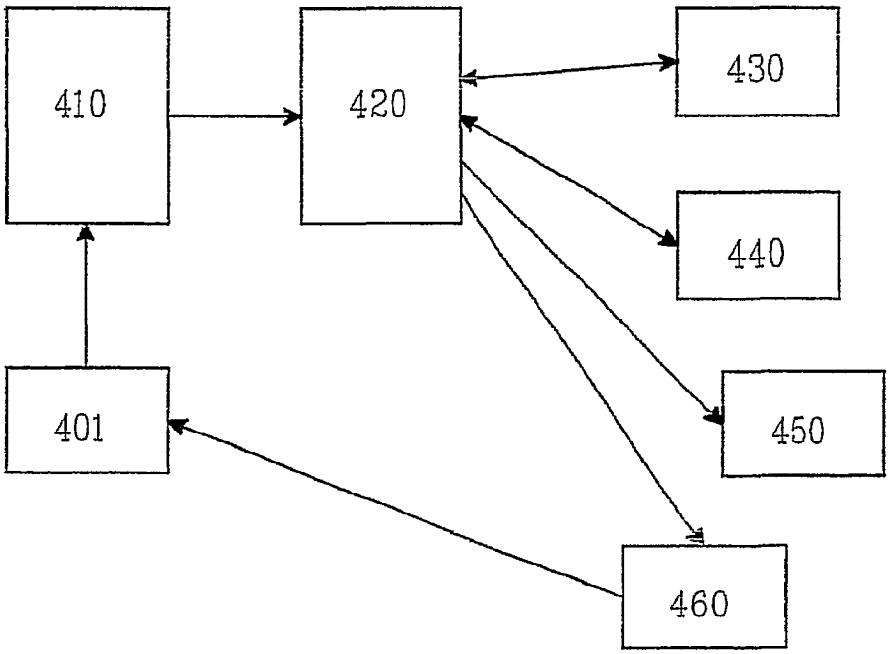
25. Носитель по п.24, который является модулем памяти.


270
SID
280
240
281
282
283
250
260

Фиг.2


Проверяют имя отправителя
300
310
Зарегистрирован для дешифрования?
НЕТ
ДА
330
320
Выполняют действие
Дешифруют!
340
Сохраняют электронное письмо

Фиг.3



Фиг.4