(19) Евразийское патентное ведомство

(11) 043334 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.05.15

(21) Номер заявки
201990412

(22) Дата подачи заявки
2016.07.29

(51) Int. Cl. ***H04L 9/06*** (2006.01)

(54) ШИФРОВАЛЬНОЕ УСТРОЙСТВО И СПОСОБ ШИФРОВАНИЯ

(43) **2019.06.28**
(86) **PCT/IB2016/001215**
(87) **WO 2018/020286 2018.02.01**

(71)(73) Заявитель и патентовладелец:
ПЕРМАНЕНТ ПРАЙВЕСИ ЛТД. (GB)

(72) Изобретатель:
Юэнь Пак Кай (CN)

(74) Представитель:
Медведев В.Н. (RU)

(56) Cristopher Ian ET AL.: "FLAXOR: A Symmetric-Key Block Cipher Plug-in using USB Mass Storage Device for Extracted Block Storage", JUPITER: 1st ITE Research Colloquium, 28 March 2008 (2008-03-28), XP55357760, Retrieved from the Internet: URL:http://flaxor.ianuy.com/Flaxor-ExtendedAbstract-10Pages.pdf [retrieved on 2017-03-22] the whole document

US-A1-2003161467

(57) Предложено устройство шифровальной приставки, которое имеет память и процессор, соединенный с памятью. Первый буфер обмена выполняется на процессоре и загружает поток нешифрованного текста. Шифровальная машина выполняется на процессоре, принимает поток нешифрованного текста и шифрует поток нешифрованного текста для создания зашифрованного потока. Цифратор выполняется на процессоре и цифрует зашифрованный поток для создания оцифрованного зашифрованного потока. Второй буфер обмена выполняется на процессоре и выгружает оцифрованный зашифрованный поток. Шифровальная машина также может дешифровать зашифрованный поток для создания потока нешифрованного текста и выгружать поток нешифрованного текста в первый буфер обмена.

043334 B1

043334 B1

Область техники, к которой относится изобретение

Устройство относится к шифрованию и, в частности, к шифрованию между разными блоками памяти, облачными платформами, операционными системами и другими продуктами.

Описание уровня техники

Многие шифровальные машины или системы, например, описанные в патентах США №№ 7,751,565 и 8,595,508, могут осуществлять функциональное шифрование/дешифрование и создавать полномасштабное кодирование или полную секцию шифрованного текста или потока шифрованного текста. Эти полномасштабные потоки шифра во многих случаях нечитаемы, неотображаемы, их нелегко передавать, и иногда трудно объединять с другими устройствами и продуктами. В современной среде интернета, облачной среде и интегрируемой среде, полномасштабное кодирование составляет основной недостаток шифровальных машин и шифровальных систем, влияющий на их применения в глобальном масштабе.

Сущность изобретения

В первом аспекте, устройство шифровальной приставки включает в себя память и процессор, соединенный с памятью. Первый буфер обмена выполняется на процессоре и загружает поток нешифрованного текста. Шифровальная машина выполняется на процессоре и принимает поток нешифрованного текста и шифрует поток нешифрованного текста для создания зашифрованного потока. Шифровальная машина также может дешифровать зашифрованный поток для создания потока нешифрованного текста и выгружать поток нешифрованного текста в первый буфер обмена.

Во втором аспекте, цифратор выполняется на процессоре и цифрует зашифрованный поток для создания оцифрованного зашифрованного потока. Цифратор цифрует зашифрованный поток согласно режиму, например, отсутствия оцифровки, оцифровки по основанию 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в виде файла (флага).

В третьем аспекте, второй буфер обмена выполняется на процессоре и выгружает оцифрованный зашифрованный поток.

В четвертом аспекте, устройство шифровальной приставки также может включать в себя децифратор, выполняющийся на процессоре, который загружает оцифрованный поток шифрования из второго буфера обмена и децифрует оцифрованный поток шифрования для создания зашифрованного потока. Затем децифратор может подавать зашифрованный поток в шифровальную машину.

В пятом аспекте, децифратор децифрует оцифрованный поток шифрования согласно режиму, например, отсутствия децифровки, основания 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в виде файла (флага).

В шестом аспекте, устройством шифровальной приставки может быть аппаратный ключ-заглушка, который может вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище или телевизионная приставка.

В седьмом аспекте, устройством шифровальной приставки может быть USB-устройство, которое может вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище или телевизионная приставка.

В восьмом аспекте, устройство шифровальной приставки может включать в себя беспроводную связь, например, Wi-Fi или Bluetooth.

В девятом аспекте, устройством шифровальной приставки может быть любое устройство или платформа связи, которая может отображать, сохранять или обмениваться данными в том числе, но без ограничения, мобильный телефон, телефон ISDN, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище, смартфон, экран дисплея, телефонная станция, планшет, компьютер, радиостанция или облако, унифицированная связь, любая форма услуг связи в масштабах предприятия, мгновенный обмен сообщениями (беседа), информация присутствия, речь (включая IP-телефонию), признаки мобильности (включающие в себя расширение мобильности и единственный диапазон чисел), аудио, веб- и видеоконференцсвязь, сближение стационарной и мобильной связи (FMC), совместное использование рабочего стола, совместное использование данных (в том числе, подключенные к сети электронные интерактивные лекционные доски), управление вызовами, распознавание речи, любая форма услуг связи, унифицированный обмен сообщениями (объединенные голосовая почта, электронная почта, SMS и факс), любой набор продуктов, который обеспечивает согласованный унифицированные пользовательский интерфейс и пользовательское восприятие между множественными устройствами и типами медиа, все формы связи, которые осуществляются через сеть для включения других форм связи, например, телевидения интернет-протокола (IPTV) и передачи цифрового идентификационного комплекта, любая объединенная часть развертывания сетевой связи, которая может направляться как связь между отдельными устройствами или широковещательная связь от одного устройства ко многим, связь, позволяющая индивидууму отправлять сообщение на одном носителе, и принимать ту же передачу на другом носителе (например, можно принимать сообщение голосовой почты и выбирать осуществлять

доступ к нему посредством электронной почты или сотового телефона. Если отправитель находится в сети согласно информации присутствия и в настоящее время принимает вызовы, ответ может отправляться непосредственно через текстовую беседу (чат) или видео-вызов. В противном случае, он может отправляться как сообщение вне реального времени, к которому можно обращаться через различные среды), многорежимную связь, речевой доступ и персональный помощник, конференцсвязь (аудио, веб и видео), инструментарий обеспечения групповых работ, мобильность, интеграцию бизнес-процессов (BPI) и программное обеспечение для обеспечения интеграция бизнес-процессов.

В 10-м аспекте, устройство шифровальной приставки может включать в себя специализированную беспроводную связь и множество беспроводных адаптеров, которые могут вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище и телевизионную приставку. Использование устройства шифровальной приставки может ограничиваться пользователем одного из беспроводных адаптеров.

В 11-м аспекте, устройство шифровальной приставки может имитироваться аппаратным эмулятором, например, эмулятором, выполняющимся на компьютере.

В 12-м аспекте, способ защитного шифрования с использованием устройство шифровальной приставки включает в себя первую операцию вставки устройства шифровальной приставки в компьютер. Затем способ защитного шифрования осуществляет вторую операцию выполнения приложения на компьютере. Затем способ защитного шифрования осуществляет третью операцию загрузки потока нешифрованного текста из приложения в первый буфер обмена. Затем способ защитного шифрования осуществляет четвертую операцию шифрования потока нешифрованного текста для создания зашифрованного потока. Затем способ защитного шифрования осуществляет пятую операцию оцифровки зашифрованного потока для создания оцифрованного зашифрованного потока. Затем способ защитного шифрования осуществляет шестую операцию выгрузки оцифрованного зашифрованного потока во второй буфер обмена.

В 13-м аспекте, приложение может быть электронной таблицей, текстовым окном, электронной почтой, текстовым процессором, пользовательской беседой или презентацией.

В 14-м аспекте, способ защитного шифрования может дополнительно включать в себя седьмую операцию оцифровки зашифрованного потока согласно режиму, например, отсутствия оцифровки, оцифровки по основанию 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в виде файла (флага).

В 15-м аспекте, способ защитного шифрования может дополнительно включать в себя восьмую операцию загрузки оцифрованного потока шифрования из второго буфера обмена. Способ защитного шифрования может дополнительно включать в себя девятую операцию децифровки оцифрованного потока шифрования для создания зашифрованного потока и подачи зашифрованного потока в шифровальную машину. Способ защитного шифрования может дополнительно включать в себя 10-ю операцию дешифрования зашифрованного потока для создания потока нешифрованного текста и выгрузки потока нешифрованного текста в первый буфер обмена.

В 16-м аспекте, способ защитного шифрования может дополнительно включать в себя 11-ю операцию децифровки оцифрованного потока шифрования согласно режиму, например, отсутствия децифровки, основания 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в виде файла (флага).

В 17-м аспекте, способ защитного шифрования может дополнительно включать в себя 12-ю операцию имитации устройства шифровальной приставки с использованием аппаратного эмулятора.

Вышеперечисленные и другие признаки и преимущества настоящего изобретения, а также структура и операция различных вариантов осуществления настоящего изобретения, подробно описаны ниже со ссылкой на прилагаемые чертежи.

Краткое описание чертежей

Прилагаемые чертежи, которые включены сюда и образуют часть описания изобретения, иллюстрируют различные варианты осуществления настоящего изобретения и, совместно с описанием, дополнительно служат для объяснения принципов и для обеспечения специалисту в данной области техники возможности использовать изобретение. В чертежах, аналогичные ссылочные позиции указывают идентичные или функционально сходные элементы. Более полное понимание и многие из сопутствующих преимуществ легко получить, обратившись к нижеследующему подробному описанию, рассматриваемому в связи с прилагаемыми чертежами, где

фиг. 1 - устройство шифровальной приставки согласно первому варианту осуществления;

фиг. 2 - устройство шифровальной приставки согласно второму варианту осуществления;

фиг. 3 - единая шифровальная приставка в виде аппаратного ключа-заглушки и USB-устройства для использования согласно варианту осуществления;

фиг. 4 - беспроводная шифровальная приставка для использования согласно варианту осуществления;

фиг. 5 - беспроводной концентратор шифрования с множественными беспроводными адаптерами для использования согласно варианту осуществления;

фиг. 6 - шифровальная приставка для использования согласно варианту осуществления;

фиг. 7 - кликабельная вкладка под названием "ppExcel30" для использования согласно варианту осуществления;

фиг. 8 - процесс шифрования ячеек MS Excel с помощью ppExcel для использования согласно варианту осуществления;

фиг. 9 - процесс шифрования ячеек MS Excel с помощью ppExcel для использования согласно варианту осуществления;

фиг. 10 - шифровальная приставка, вставленная в машину для использования согласно варианту осуществления;

фиг. 11 - универсальный шифратор текста с использованием шифровальной приставки для использования согласно варианту осуществления;

фиг. 12 - процесс шифрования для использования согласно варианту осуществления;

фиг. 13 - процесс шифрования для использования согласно варианту осуществления;

фиг. 14 - процесс дешифрования для использования согласно варианту осуществления;

фиг. 15 - процесс дешифрования для использования согласно варианту осуществления;

фиг. 16 - процесс отправки зашифрованного сообщения в программу беседы в реальном времени для использования согласно варианту осуществления;

фиг. 17 - процесс отправки зашифрованного сообщения в программу беседы в реальном времени для использования согласно варианту осуществления;

фиг. 18 - процесс дешифрования зашифрованного сообщения, принятого от программы беседы в реальном времени для использования согласно варианту осуществления;

фиг. 19 - процесс дешифрования зашифрованного сообщения, принятого от программы беседы в реальном времени для использования согласно варианту осуществления;

фиг. 20 - устройство шифровальной приставки согласно третьему варианту осуществления;

фиг. 21 - способ защитного шифрования согласно четвертому варианту осуществления.

Подробное описание предпочтительных вариантов осуществления

Первый вариант осуществления устройства 100 шифровальной приставки показан на фиг. 1. Первый модуль 122 буфера обмена, второй модуль 140 буфера обмена и цифратор/децифратор 128 добавлены в шифровальную машину для преодоления недостатка шифровальной машины и обеспечения ее совместимости и доступности для всех разных блоков памяти, облачных платформ, операционных систем и возможности связи с другими продуктами.

Для перемещения или совместимости со всеми разными блоками памяти, операционными системами и т.д., используется особая структура памяти (аппаратная память) "буфер обмена". Буфер обмена (или кэш-память буфера обмена) является особой памятью во всех устройствах, в том числе компьютерах, мобильных телефонах и планшетах. Буфер обмена сам по себе не может решить все проблемы несовместимости; необходим также "модуль цифратора/децифратора" 136 (236 на фиг. 2).

В устройстве 100 шифровальной приставки, показанном на фиг. 1, первый буфер 122 обмена выполняется на процессоре и загружает поток 116 нешифрованного текста с использованием буфера обмена 126 загрузки.

Шифровальная машина выполняется на процессоре и принимает поток 116 нешифрованного текста и шифрует поток 116 нешифрованного текста для создания потока шифрованного текста или зашифрованный поток 110. Шифровальная машина также может дешифровать зашифрованный поток 110 для создания потока 116 нешифрованного текста и выгружать поток 116 нешифрованного текста в первый буфер 122 обмена с использованием буфера обмена 124 выгрузки.

Цифратор/децифратор 128 выполняется на процессоре и цифрует (преобразовывает в цифровой вид) зашифрованный поток 110 для создания оцифрованного зашифрованного потока 138. Цифратор/децифратор 128 цифрует зашифрованный поток 110 согласно режиму 132, такому как, например, отсутствие оцифровки, оцифровка по основанию 64, шестнадцатеричные числа без пробелов, спаренные шестнадцатеричные числа с пробелами, задаваемый пользователем режим или сохранение в качестве файла (флага).

Второй буфер 140 обмена выполняется на процессоре и выгружает оцифрованный зашифрованный поток 138 с использованием буфера обмена 134 выгрузки.

Цифратор/децифратор 128, выполняющийся на процессоре, также может загружать оцифрованный поток 138 шифрования из второго 140 буфера обмена с использованием буфера обмена 142 загрузки и децифровать оцифрованный поток 138 шифрования для создания зашифрованного потока 110. Затем цифратор/децифратор 128 может подавать зашифрованный поток 110 в шифровальную машину.

Цифратор/децифратор 128 децифрует (обратно преобразовывает из цифровой формы) оцифрованный поток 138 шифрования согласно режиму 132, например, отсутствия децифровки, основания 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в качестве файла (флага).

Устройством 100 шифровальной приставки может быть аппаратный ключ-заглушка, который может вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон,

планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище или телевизионная приставка.

Устройством 100 шифровальной приставки может быть USB-устройство, которое может вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище или телевизионная приставка.

Устройство 100 шифровальной приставки может включать в себя беспроводную связь, например, Wi-Fi или Bluetooth.

Устройством 100 шифровальной приставки может быть мобильный телефон, телефон ISDN, Skype, Viber, Whatsapp, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище, смартфон, экран дисплея, телефонная станция, планшет, компьютер, радиостанция или облако.

Устройство 100 шифровальной приставки может включать в себя специализированную беспроводную связь и множество беспроводных адаптеров, которые могут вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище и телевизионную приставку. Использование устройства 100 шифровальной приставки может ограничиваться пользователем одного из беспроводных адаптеров.

Устройство 100 шифровальной приставки может имитироваться аппаратным эмулятором, например, эмулятором, выполняющимся на компьютере.

Генератор 103 первого потока шифра генерирует и синхронизирует первый поток шифра с использованием нешифрованной текстовой информации 116 и первого ключа 118. Генератор 101 второго потока шифра генерирует и синхронизирует второй поток шифра с использованием второго ключа 106 и функции 104 рандомизации для рандомизации с последующей синхронизацией потока 102 управляемого нешифрованного текста. Оператор 120 исключающей дизъюнкции, действующий на первом и втором синхронизированных потоках шифра, получает поток 110 шифрованного текста.

Генератор 103 первого потока шифра включает в себя блок 114 шифрования блочным шифром, который генерирует и синхронизирует первый синхронизированный поток шифра после ввода нешифрованной текстовой информации 116 и первого ключа 118. Устройство 114 шифрования блочным шифром генерирует первый поток шифра и первый блок 112 синхронизации синхронизирует первый поток шифра.

Генератор 101 второго потока шифра включает в себя генератор случайных функций, который рандомизирует, и затем синхронизирует, поток 102 управляемого нешифрованного текста после ввода второго ключа 106 и потока 102 управляемого нешифрованного текста, и выводит второй синхронизированный поток шифра. Генератор случайных функций включает в себя устройство 104 генератора случайных функций для рандомизации потока управляемого нешифрованного текста и второй блок 108 (208 на фиг. 2) синхронизации для синхронизации рандомизированного второго потока шифра.

Второй вариант осуществления устройства 200 шифровальной приставки показан на фиг. 2.

В устройстве 200 шифровальной приставки показанный на фиг. 2, первый буфер обмена 222 выполняется на процессоре и загружает поток 216 нешифрованного текста с использованием буфера обмена 226 загрузки.

Шифровальная машина выполняется на процессоре и принимает поток 216 нешифрованного текста и шифрует поток 216 нешифрованного текста для создания потока шифрованного текста или зашифрованный поток 210. Шифровальная машина также может дешифровать зашифрованный поток 210 для создания потока 216 нешифрованного текста и выгружать поток 216 нешифрованного текста в первый буфер обмена 222 с использованием буфера обмена 224 выгрузки.

Цифратор/децифратор 228 выполняется на процессоре и цифрует зашифрованный поток 210 для создания оцифрованного зашифрованного потока 238. Цифратор/децифратор 228 цифрует зашифрованный поток 210 согласно режиму 232, например, отсутствия оцифровки, оцифровки по основанию 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в виде файла (флага).

Второй буфер обмена 240 выполняется на процессоре и выгружает оцифрованный зашифрованный поток 238 с использованием буфера обмена 234 выгрузки.

Цифратор/децифратор 228, выполняющийся на процессоре, также может загружать оцифрованный поток 238 шифрования из второго буфера обмена 240 с использованием буфера обмена 242 загрузки и децифровать оцифрованный поток 238 шифрования для создания зашифрованного потока 210. Затем цифратор/децифратор 228 может подавать зашифрованный поток 210 в шифровальную машину.

Цифратор/децифратор 228 децифрует оцифрованный поток 238 шифрования согласно режиму 232, например, отсутствия децифровки, основания 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в виде файла (флага).

Устройством 200 шифровальной приставки может быть заглушка, которая может вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интел-

лектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище или телевизионная приставка.

Устройством 200 шифровальной приставки может быть USB-устройство, которое может вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище или телевизионная приставка.

Устройство 200 шифровальной приставки может включать в себя беспроводную связь, например, Wi-Fi или Bluetooth.

Устройством 200 шифровальной приставки может быть мобильный телефон, телефон ISDN, Skype, Viber, Whatsapp, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище, смартфон, экран дисплея, телефонная станция, планшет, компьютер, радиостанция или облако.

Устройство 200 шифровальной приставки может включать в себя специализированную беспроводную связь и множество беспроводных адаптеров, которые могут вставляться в компьютер, например, персональный компьютер, портативный компьютер, смартфон, планшет, интеллектуальный телевизор, дисковый накопитель интеллектуальной сети, центральное хранилище и телевизионную приставку. Использование устройства 200 шифровальной приставки может ограничиваться пользователем одного из беспроводных адаптеров.

Устройство 200 шифровальной приставки может имитироваться аппаратным эмулятором, например, эмулятором, выполняющимся на компьютере.

Генерируется второй синхронизированный поток шифра. Могут использоваться управляемый нешифрованный текст 202, который совпадает с управляемым нешифрованным текстом 102, показанным на фиг. 14, случайная функция 200, которая совпадает со случайной функцией 104, и второй ключ 206, который совпадает с вторым ключом. Управляемый нешифрованный текст 202 и случайная функция 104 обычно передаются отдельно от передающего агента к принимающему агенту, и второй ключ 106, в общем случае, уже известен принимающему агенту.

На фиг. 3 показаны единая шифровальная приставка в виде аппаратного ключа-заглушки и USB-устройства 310 для использования согласно варианту осуществления. Единая шифровальная приставка в виде аппаратного ключа-заглушки и USB-устройства 310 называется "шифровальной приставкой" и может использоваться с PC, портативными компьютерами, смартфонами, (айфонами и телефонами Android) и интеллектуальными планшетами, например, айпадами.

Шифровальная приставка будет содержать шифровальную машину с вышеописанными цифратором/децифратором и буфером обмена.

Единая шифровальная приставка в виде аппаратного ключа-заглушки и USB-устройства 310 могут вставляться в PC 302, портативный компьютер 308 или смартфон и/или планшет 304 и 306 и обеспечивать прямое шифрование/дешифрование для одного пользователя.

На фиг. 4 показана беспроводная (WiFi или Bluetooth) шифровальная приставка 410 для использования согласно варианту осуществления. Чтобы больше людей использовали шифровальную приставку, беспроводная шифровальная приставка 410 будет содержать шифровальную машину, цифратор/децифратор и модули буфера обмена совместно с беспроводными модулями (WiFi или Bluetooth). Это устройство позволяет большому количеству людей одновременно использовать шифровальную приставку. Беспроводная шифровальная приставка 410 может использоваться с PC 402, портативным компьютером 408 или смартфоном и/или планшетом 404 и 406.

На фиг. 5 показан беспроводной концентратор шифрования с множественными беспроводными адаптерами 512 для использования согласно варианту осуществления. Чтобы больше людей использовали шифровальную приставку, беспроводной концентратор 512 шифрования будет содержать шифровальную машину, цифратор/децифратор, модули буфера обмена совместно с беспроводными модулями (WiFi или Bluetooth). Это устройство позволяет большому количеству людей одновременно использовать шифровальную приставку. Беспроводной концентратор 512 шифрования может использоваться с PC 502, портативным компьютером 508 или смартфоном и/или планшетом 504 и 506.

Беспроводной USB-адаптер 510 содержит беспроводную передачу, соответствующую беспроводному концентратору 512 шифрования, и позволяет большому количеству людей одновременно использовать беспроводной концентратор 512 шифрования. Беспроводной USB-адаптер 510 содержит беспроводные специализированные модули, соответствующие концентратору 512 шифрования.

Пользователи могут покупать один беспроводной концентратор 512 шифрования и множественные беспроводные адаптеры 510. Каждый адаптер 510 может вставляться непосредственно в PC 502, портативный компьютер 508 или смартфон и/или планшет 504 и 506. Только пользователи адаптера 510 могут использовать шифрование/дешифрование, обеспеченное беспроводным концентратором 512 шифрования.

На фиг. 6 показана шифровальная приставка 610, вставленная в устройство, например, PC 602. Когда шифровальная приставка 610 вставляется в устройство, например, PC 602, несколько приложений может загружаться и устанавливаться автоматически или вручную.

В одном варианте осуществления, ppExcel, которой интегрирует Microsoft Excel и шифровальную

приставку 610, полностью внедрен в MS Excel для обеспечения шифрования/дешифрования на ячейках MS Excel независимо от типа ячейки.

Хорошо известно, что сложности с форматом ячеек MS Excel, например, числовые ячейки, текстовые ячейки и формульные ячейки, образующие основную трудность для любой шифровальной машины для обеспечения успешного защитного шифрования. Эти разные типы ячеек несовместимы друг с другом, но взаимосвязаны. При изменении одного типа ячеек, например, формульных ячеек, с помощью шифрования, все остальные зависимые ячейки, например, числовые ячейки, непосредственно изменят статус на "трудный". По этой причине, предполагается, что никакая традиционная шифровальная машина не может обеспечивать успешное шифрование на ячейках Excel независимо от их типов. С помощью цифратора и модуля буфера обмена, шифровальная приставка 610 может обеспечивать решение этой проблемы.

Когда шифровальная приставка 610 вставляется в устройство, например, PC 602, шифровальная приставка 610 будет устанавливать кликабельную вкладку 702 под названием "ppExcel30", как показано на фиг. 7. При кликаньи по этой вкладке ppExcel30, в программном обеспечении MS Excel появится несколько функциональных кнопок 704.

Функциональные кнопки 704, обеспеченные ppExcel, можно использовать для шифрования и дешифрования на выбранных ячейках, всем листе и всей рабочей книге Excel независимо от типов ячеек. Предполагается, что ppExcel является первым шифратором для обеспечения успешного шифрования ячеек для MS Excel в этом стиле.

Следующий процесс описывает основное шифрование ppExcel на ячейках MS Excel.

1. Выделить выбранные исходные ячейки в Excel, которые нужно зашифровать.

2. Нажать кнопку "Enc/Dec Selected Cells" (шифровать/дешифровать выбранные ячейки).

3. ppExcel будет копировать все выбранные ячейки и отправлять их на шифровальную приставку одну за другой.

4. После шифрования шифровальной приставкой, содержимое ячейки будет отправляться в буфер обмена.

5. Затем ppExcel будет вставлять зашифрованное содержимое ячейки из буфера обмена обратно в исходное положение ячейки.

Следующий процесс описывает основное дешифрование ppExcel на ячейках MS Excel со ссылкой на фиг. 7.

1. Выделить выбранные зашифрованные ячейки в MS Excel, которые нужно дешифровать.

2. Нажать кнопку "Enc/Dec Selected Cells".

3. ppExcel будет копировать все выбранные зашифрованные ячейки и отправлять их на шифровальную приставку одну за другой. Поскольку они зашифрованы ppExcel (в формате оцифрованного потока шифрованного текста), шифровальная приставка будет осуществлять дешифрование автоматически.

4. После дешифрования шифровальной приставкой, исходная ячейка будет отправляться в буфер обмена.

5. Затем ppExcel будет вставлять ячейку из буфера обмена обратно в исходное положение ячейки.

Процесс шифрования ячеек MS Excel с помощью ppExcel показан на фиг. 8 и 9.

1. Сначала пометить (или выделить) ячейки которые нужно зашифровать 802, из MS Excel.

2. Кликнуть по кнопке 904 "Enc/Dec Selected Cells".

3. Выбранные исходные ячейки MS Excel 802 будут заменены зашифрованными ячейками 902.

С использованием аналогичной конструкции также устанавливаются следующие связанные прототипы.

1. ppOutlook, которой интегрирует MS Outlook и шифровальную приставку.

2. ppWord, которой интегрирует MS Word и шифровальную приставку.

3. ppPowerPoint, которой интегрирует MS PowerPoint и шифровальную приставку.

В другом варианте осуществления, показанном на фиг. 10 и 11, PPM, который является универсальным шифратором текста, использующим шифровальную приставку 1004, может использовать шифровальную приставку 1004 для шифрования/дешифрования любого текста из любых других программ.

В силу сложностей всех разных программ на разных платформах (или операционных системах), которые создают тексты, традиционным шифровальным машинам нелегко построить универсальный шифратор, который может шифровать/дешифровать тексты для всех них. С помощью цифратора и модулей буфера обмена, шифровальная приставка 1004 устанавливает универсальный шифратор под названием PPM (Professional Protection for Messages) для шифрования/дешифрования любого текста из любых других программ.

Когда шифровальная приставка 1004 вставлена в машину 1002, как показано на фиг. 10, шифровальная приставка 1004 будет загружать и устанавливать программу под названием "PPM" 1102, которая показана на фиг. 11. PPM 1102 является универсальным шифратором текста для любой программы, связанной с текстом. Любое изменение текста в окне исходного сообщения (ORIGINAL MESSAGE) будет инициировать автоматическое шифрование, и результаты шифрования появятся в окне зашифрованного сообщения (ENCRYPTED MESSAGE). Любое изменение текста в окне зашифрованного сообщения

(ENCRYPTED MESSAGE) будет инициировать автоматическое дешифрование, и результаты дешифрования появятся в окне исходного сообщения (ORIGINAL MESSAGE).

Кнопки, обеспеченные PPM, можно использовать для шифрования и дешифрования на любом тексте из любой программы.

При впечатывании фрагмента текста в окно исходного сообщения (ORIGINAL MESSAGE), он будет шифроваться автоматически, и зашифрованное сообщение появится в окне зашифрованного сообщения (ENCRYPTED MESSAGE).

Возможны следующие кнопки:

Msg Copy - копировать текст из окна исходного сообщения (ORIGINAL MESSAGE) в буфер обмена,

Msg Paste - загрузить текст из буфера обмена в окно исходного сообщения (ORIGINAL MESSAGE). (Auto-Encrypt) Это будет инициировать автоматическое шифрование, и результаты дешифрования появляются в окне зашифрованного сообщения (ENCRYPTED MESSAGE) (используется режим оцифровки=3),

Enc Copy - копировать зашифрованный текст из окна зашифрованного сообщения (ENCRYPTED MESSAGE) в буфер обмена,

Enc Paste - загрузить зашифрованный текст из буфера обмена в окно зашифрованного сообщения (ENCRYPTED MESSAGE). Зашифрованный текст будет дешифроваться автоматически и появляться в окне исходного сообщения (ORIGINAL MESSAGE). Это также может именоваться Auto-Decrypt.

Процесс шифрования PPM будет описан со ссылкой на фиг. 12 и 13.

1. Выделить выбранный текст 1202 например "This is my secret" и нажать сочетание клавиш Control-C в любой программе, связанной с текстом (при этом выбранный текст будет отправляться в буфер обмена).

2. Нажать кнопку "Msg Paste" PPM (PPM будет копировать текст из буфера обмена и вставлять его в окно исходного сообщения (ORIGINAL MESSAGE)).

3. Текст в окне 1302 исходного сообщения будет шифроваться автоматически и напрямую.

4. Зашифрованный текст появится в окне 1304 зашифрованного сообщения как

"f3 0e c2 ab e2 ef 71 4a e1 70 67 81 53 95 28 02 12

e1 5a cf 5a 3b 27 cf 73 90 93 68 df 3a 74 f5 5c f4 ff c2 6c 14

dc fd"

Спаренные шестнадцатеричные числа с пробелами (или режим оцифровки =3).

Дешифрование PPM будет описано со ссылкой на фиг. 14 и 15.

1. Выделить любой зашифрованный PPM текст 1402 и нажать сочетание клавиш Control-C, при этом выбранный текст будет отправляться в буфер обмена.

2. Нажать кнопку "Enc Paste" PPM, PPM вставит текст из буфера обмена в окно 1504 зашифрованного сообщения.

3. Текст в окне 1504 зашифрованного сообщения также будет дешифроваться автоматически.

4. Дешифрованный текст появится в окне 1502 исходного сообщения.

Отправка зашифрованного сообщения в программу беседы в реальном времени под названием LINE будет описана со ссылкой на фиг. 16 и 17.

Предположим, пользователь хочет вести защищенную беседу в реальном времени с пользователем под именем "Buckingham" с использованием популярного программного обеспечения для ведения беседы под названием LINE, установленном на машине. К машине также присоединена шифровальная приставка.

Защищенная беседа в реальном времени может осуществляться посредством следующих процедур.

1. Предположим, на машине пользователя установлены PPM и популярное программное обеспечение для ведения беседы LINE.

2. Напечатать сообщение в окне 1602 исходного сообщения PPM, например, "Meet Me At 2pm Tomorrow".

3. Одновременно с печатью сообщения в окне 1602 исходного сообщения, соответствующее зашифрованное сообщение

"1b 67 f2 de 0a 86 41 3f 52 9b c6 8f 2a 70 6c 0b 6c

b0 ac d1 35 65 01 8d 1e

65 d0 6b 31 50 d6 87 41 f6 22 70 cb 3e 1f fb"

будет появляться в окне 1604 зашифрованного сообщения.

4. Нажать кнопку "Enc Copy", чтобы отправить зашифрованное сообщение в буфер обмена.

5. Вставить зашифрованное сообщение из буфера обмена в область 1702 печати LINE и нажать клавишу "возврат", чтобы отправить зашифрованное сообщение в область беседы LINE.

6. Зашифрованное сообщение появляется в области беседы LINE.

Дешифрование зашифрованного сообщения из программы беседы в реальном времени под названием LINE будет описано со ссылкой на фиг. 18 и 19.

Предположим, получено зашифрованное PPM сообщение

"ff ad d6 f5 ee 4c 65 14 1d 73 0b b9 e5 db 9f 27 bf

4b 11 a1 33 39 20 ab 34 18 72

63 a2 d0 b3 ef c2 e3 fa fb 7b e9 81"

из LINE. Для его дешифрования можно использовать следующую процедуру.

1. Выделить зашифрованное сообщение из области 1802 беседы LINE.

2. Нажать сочетание клавиш Control-C, чтобы отправить зашифрованное сообщение в буфер обмена.

3. Нажать кнопку "Enc Paste" в PPM.

4. Зашифрованное сообщение будет скопировано из буфера обмена в окно 1904 зашифрованного сообщения PPM. Одновременно зашифрованное сообщение будет автоматически дешифроваться PPM.

5. Результаты дешифрования, например,

"OK. At the spot-772 as usual"

будут отображаться в окне 1902 исходного сообщения PPM. Можно прочитать исходное сообщение и действовать по своему усмотрению.

В третьем варианте осуществления, показанном на фиг. 20, устройство 2000 шифровальной приставки включает в себя память 2002 и процессор 2004, соединенный с памятью 2002.

В четвертом варианте осуществления, показанном на фиг. 21, способ защитного шифрования с использованием устройство шифровальной приставки включает в себя первую операцию 2102 вставки устройства шифровальной приставки в компьютер. Затем способ защитного шифрования осуществляет вторую операцию 2104 выполнения приложения на компьютере. Затем способ защитного шифрования осуществляет третью операцию 2106 загрузки потока нешифрованного текста из приложения в первый буфер обмена. Затем способ защитного шифрования осуществляет четвертую операцию 2108 шифрования потока нешифрованного текста для создания зашифрованного потока. Затем способ защитного шифрования осуществляет пятую операцию 2110 оцифровки зашифрованного потока для создания оцифрованного зашифрованного потока. Затем способ защитного шифрования осуществляет шестую операцию 2112 выгрузки оцифрованного зашифрованного потока во второй буфер обмена.

Приложение может быть электронной таблицей, текстовым окном, электронной почтой, текстовым процессором, пользовательской беседой или презентацией.

Способ защитного шифрования может дополнительно включать в себя седьмую операцию оцифровки зашифрованного потока согласно режиму, например, отсутствия оцифровки, оцифровки по основанию 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в виде файла (флага).

Способ защитного шифрования может дополнительно включать в себя восьмую операцию загрузки оцифрованного потока шифрования из второго буфера обмена. Способ защитного шифрования может дополнительно включать в себя девятую операцию децифровки оцифрованного потока шифрования для создания зашифрованного потока и подачи зашифрованного потока в шифровальную машину. Способ защитного шифрования может дополнительно включать в себя 10-ю операцию дешифрования зашифрованного потока для создания потока нешифрованного текста и выгрузки потока нешифрованного текста в первый буфер обмена.

Способ защитного шифрования может дополнительно включать в себя 11-ю операцию децифровки оцифрованного потока шифрования согласно режиму, например, отсутствия децифровки, основания 64, шестнадцатеричных чисел без пробелов, спаренных шестнадцатеричных чисел с пробелами, задаваемого пользователем режима или сохранения в качестве файла (флага).

Способ защитного шифрования может дополнительно включать в себя 12-ю операцию имитации устройства шифровальной приставки с использованием аппаратного эмулятора.

Варианты осуществления можно реализовать в вычислительном оборудовании (вычислительном устройстве) и/или программном обеспечении, например (в неограничительном примере) любом компьютере, который может сохранять, извлекать, обрабатывать и/или выводить данные и/или осуществлять связь с другими компьютерами. Полученные результаты могут отображаться на дисплее вычислительного оборудования. Программа/программное обеспечение, реализующая/ее варианты осуществления, может записываться на компьютерно-считываемых средах, содержащих компьютерно-считываемые носители записи. Программа/программное обеспечение, реализующая/ее варианты осуществления, также может передаваться по средам передачи данных. Примеры компьютерно-считываемых носителей записи включают в себя магнитное записывающее устройство, оптический диск, магнито-оптический диск и/или полупроводниковую память (например, RAM, ROM и т.д.). Примеры магнитного записывающего устройства включают в себя устройство жесткого диска (HDD), гибкий диск (FD) и магнитную ленту (MT). Примеры оптического диска включают в себя DVD (цифровой универсальный диск), DVD-RAM, CD-ROM (компакт-диск однократной записи), и CD-R (перезаписываемый)/RW. Пример сред передачи данных включает в себя сигнал несущей волны.

Дополнительно, согласно аспекту вариантов осуществления, могут обеспечиваться любые комбинации описанных признаков, функций и/или операций.

Многие признаки и преимущества вариантов осуществления явствуют из подробного описания

изобретения и, таким образом, нижеследующая формула изобретения призвана охватывать все подобные признаки и преимущества вариантов осуществления, которые укладываются в их истинную сущность и объем. Дополнительно, поскольку многочисленные модификации и изменения очевидны специалистам в данной области техники, нежелательно ограничивать варианты осуществления изобретения конкретными проиллюстрированными и описанными конструкцией и операцией, и, соответственно, допустимы все пригодные модификации и эквиваленты, укладывающиеся в его объем.

Выше были описаны принципы, варианты осуществления и режимы работы настоящего изобретения. Однако не следует считать, что изобретение ограничивается вышеописанными конкретными вариантами осуществления, поскольку их следует рассматривать как иллюстративные и неограничительные. Очевидно, что специалисты в данной области техники могут предложить вариации этих вариантов осуществления, не выходя за рамки объема настоящего изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Шифровальное устройство (100), содержащее

память; и

процессор, соединенный с памятью и выполненный с возможностью реализации:

первого буфера (122) обмена, выполненного с возможностью загружать поток (116) нешифрованного текста в первом формате из приложения на компьютере;

шифровальной машины, выполненной с возможностью принимать поток (116) нешифрованного текста и шифровать поток (116) нешифрованного текста для создания зашифрованного потока (110);

цифратора (128), выполненного с возможностью цифровать зашифрованный поток (110) согласно режиму для создания оцифрованной формы зашифрованного потока (138), причем оцифрованная форма зашифрованного потока согласно упомянутому режиму - во втором формате, который является совместимо отображаемым посредством упомянутого приложения на компьютере, чтобы отображаться посредством компьютера; и

второго буфера (140) обмена, выполненного с возможностью выгружать оцифрованный зашифрованный поток (138) во втором формате.

2. Шифровальное устройство (100) по п.1, в котором упомянутый режим - это режим, выбираемый из группы режимов, включающих в себя

оцифровку по основанию 64,

шестнадцатеричные числа без пробелов,

спаренные шестнадцатеричные числа с пробелами и

задаваемый пользователем режим.

3. Шифровальное устройство (100) по п.2, в котором

процессор дополнительно выполнен с возможностью реализации децифратора (128), выполненного с возможностью загружать оцифрованную форму зашифрованного потока (138) из второго буфера (140) обмена и децифровать оцифрованную форму зашифрованного потока (138) во втором формате для создания зашифрованного потока (110) и подавать зашифрованный поток (110) в шифровальную машину; и

шифровальная машина дополнительно выполнена с возможностью дешифровать зашифрованный поток (110) для создания потока (116) нешифрованного текста в первом формате и выгружать поток (116) нешифрованного текста в первый буфер (122) обмена.

4. Шифровальное устройство (100) по п.3, в котором децифратор (128) децифрует оцифрованную форму зашифрованного потока (138) для создания зашифрованного потока согласно упомянутому режиму (132).

5. Шифровальное устройство (100) по п.1, при этом шифровальное устройство (100) представляет собой аппаратный ключ-заглушку, который может вставляться в упомянутый компьютер, причем компьютер представляет собой любое одно из персонального компьютера, портативного компьютера, смартфона, планшета, интеллектуального телевизора, дискового накопителя интеллектуальной сети, центрального хранилища и телевизионной приставки.

6. Шифровальное устройство (100) по п.1, при этом шифровальное устройство (100) представляет собой USB-устройство, которое может вставляться в упомянутый компьютер, причем компьютер представляет собой любое одно из персонального компьютера, портативного компьютера, смартфона, планшета, интеллектуального телевизора, дискового накопителя интеллектуальной сети, центрального хранилища и телевизионной приставки.

7. Шифровальное устройство (100) по п.1, в котором упомянутые загрузка и выгрузка осуществляются посредством беспроводной связи, включающей в себя любое одно из Wi-Fi и Bluetooth.

8. Шифровальное устройство (100) по п.1, дополнительно содержащее специализированный интерфейс беспроводной связи и множество беспроводных адаптеров, которые могут вставляться в упомянутый компьютер, причем компьютер представляет собой любое одно из персонального компьютера, портативного компьютера, смартфона, планшета, интеллектуального телевизора, дискового накопителя интеллектуальной сети, центрального хранилища и телевизионной приставки.

9. Шифровальное устройство (100) по п.8, в котором процессор выполнен с возможностью ограничивать использование шифровального устройства (100) пользователем одного из беспроводных адаптеров.

10. Шифровальное устройство (100) по п.1, при этом использование шифровального устройства (100) имитируется аппаратным эмулятором.

11. Шифровальное устройство (100) по п.1, при этом шифровальное устройство (100) имитируется в мобильном телефоне, телефоне ISDN, интеллектуальном телевизоре, дисковом накопителе интеллектуальной сети, центральном хранилище, смартфоне, экране дисплея, телефонной станции, планшете, компьютере, радиостанции, облачной платформе или в платформе связи.

12. Шифровальное устройство (100) по п.1, в котором упомянутый режим дополнительно включает в себя режим сохранения в виде файла, с вариантом установленного флага.

13. Шифровальное устройство (100) по п.1, в котором

первый буфер обмена содержит буфер обмена выгрузки и буфер обмена загрузки, при этом первый буфер обмена выполняется в процессоре для загрузки потока нешифрованного текста в первом формате из упомянутого приложения в буфер (126) обмена загрузки из состава первого буфера обмена;

второй буфер обмена содержит буфер обмена выгрузки и буфер обмена загрузки, при этом второй буфер обмена выполняется в процессоре для выгрузки оцифрованного зашифрованного потока с использованием буфера обмена выгрузки из состава второго буфера обмена,

при этом в упомянутом приложении установлена кликабельная вкладка, причем кликабельная вкладка, при выполнении клика по ней, обеспечивает по меньшей мере одну кнопку из кнопки шифрования и кнопки дешифрования из числа кнопок в упомянутом приложении, при этом поток нешифрованного текста является выбираемым содержимым в местоположении в упомянутом приложении,

причем кликабельная вкладка выполнена с возможностью:

при нажатии на кнопку шифрования, копировать выбранное содержимое и отправлять выбранное содержимое в буфер обмена загрузки из состава первого буфера обмена;

шифровать выбранное содержимое с использованием шифровальной машины для создания зашифрованного выбранного содержимого;

цифровать зашифрованное выбранное содержимое с использованием цифратора для создания зашифрованного и оцифрованного выбранного содержимого, при этом зашифрованное и оцифрованное выбранное содержимое отправляется в буфер обмена выгрузки из состава второго буфера обмена; и

вставлять зашифрованное и оцифрованное выбранное содержимое в упомянутое местоположение в приложении из второго буфера обмена с использованием буфера обмена выгрузки из состава второго буфера обмена.

14. Шифровальное устройство (100) по п.13, в котором упомянутым приложением является приложение электронной таблицы, и упомянутое местоположение в приложении включает в себя ячейку в электронной таблице приложения электронной таблицы.

15. Способ защитного шифрования посредством шифровального устройства (100), вставляемого в компьютер, при этом способ содержит этапы, на которых, посредством процессора, подключенного к памяти

загружают поток (116) нешифрованного текста в первом формате из приложения, исполняющегося на компьютере, в первый буфер (122) обмена;

шифруют поток (116) нешифрованного текста для создания зашифрованного потока (110);

цифруют зашифрованный поток (110) согласно режиму для создания оцифрованной формы зашифрованного потока (138), причем оцифрованная форма зашифрованного потока - во втором формате, который является совместимо отображаемым посредством упомянутого приложения на компьютере, чтобы отображаться посредством компьютера; и

выгружают оцифрованный зашифрованный поток (138) во втором формате во второй буфер (140) обмена.

16. Способ защитного шифрования по п.15, в котором первый формат - это формат, соответствующий приложению из числа приложений, включающих в себя электронную таблицу, текстовое окно, электронную почту, текстовый процессор, пользовательскую беседу и презентацию.

17. Способ защитного шифрования по п.15, в котором упомянутый режим (132) выбирается из группы режимов, включающих в себя

оцифровку по основанию 64,

шестнадцатеричные числа без пробелов,

спаренные шестнадцатеричные числа с пробелами,

задаваемый пользователем режим и

сохранение в виде файла (флага).

18. Способ защитного шифрования по п.17, дополнительно содержащий этапы, на которых посредством процессора

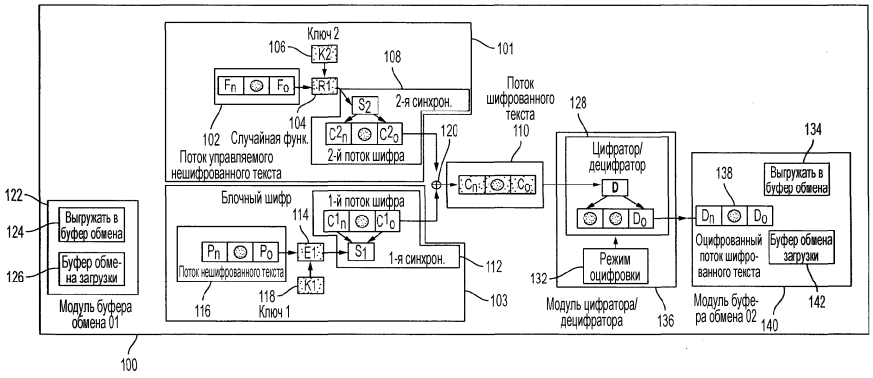
загружают оцифрованную форму зашифрованного потока (138) из второго буфера (140) обмена и децифруют оцифрованную форму зашифрованного потока (138) во втором формате согласно упомянутому режиму для создания зашифрованного потока (110) и подают зашифрованный поток (110) в шиф-

ровальную машину; и

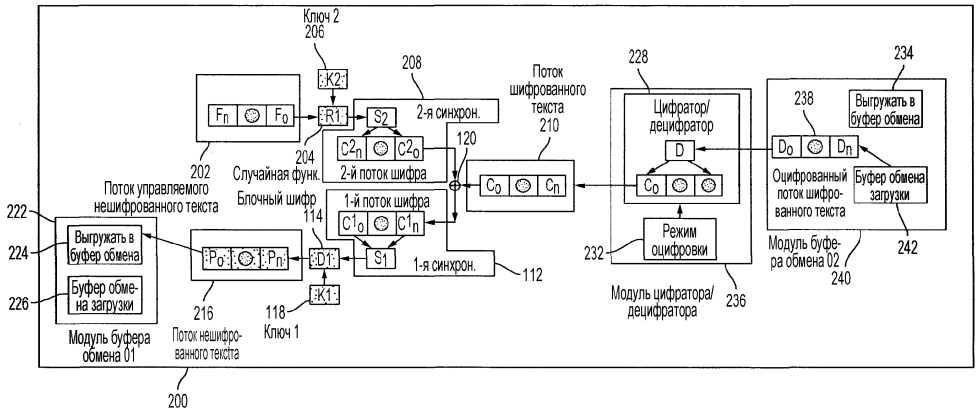
дешифруют зашифрованный поток (110) для создания потока (116) нешифрованного текста в первом формате и выгружают поток (116) нешифрованного текста в первый буфер (122) обмена.

19. Способ защитного шифрования по п.18, в котором упомянутая децифровка для создания зашифрованного потока осуществляется согласно упомянутому режиму (132).

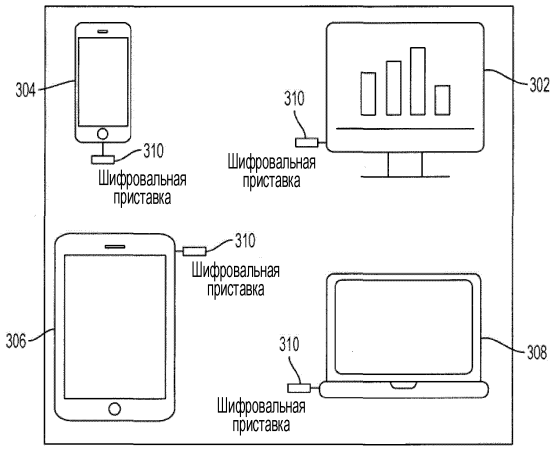
20. Способ защитного шифрования по п.15, дополнительно содержащий этап, на котором имитируют шифровальное устройство (100) в компьютере с использованием аппаратного эмулятора.



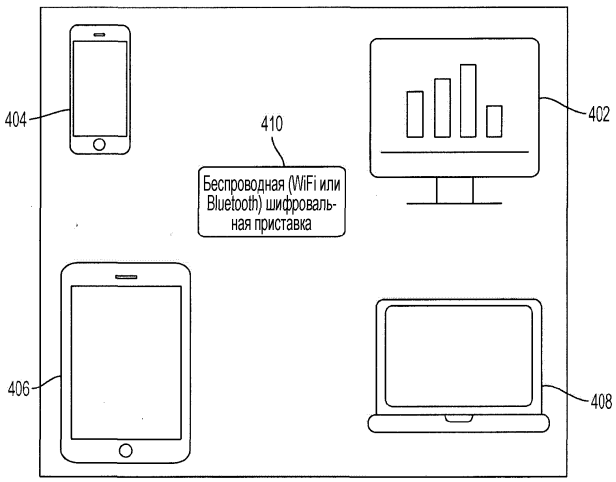
Фиг. 1



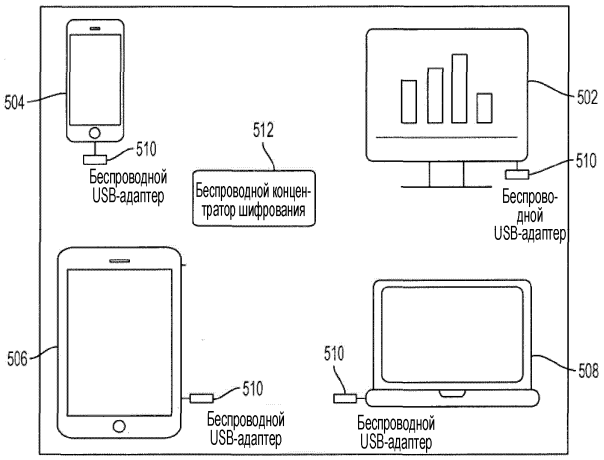
Фиг. 2



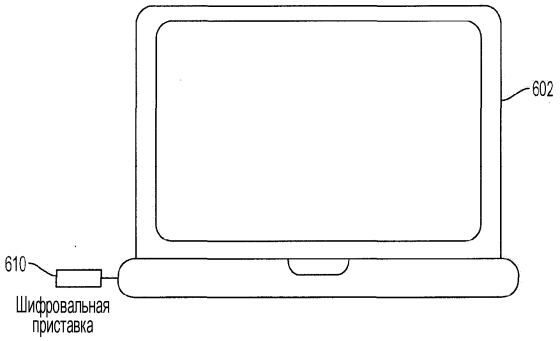
Фиг. 3



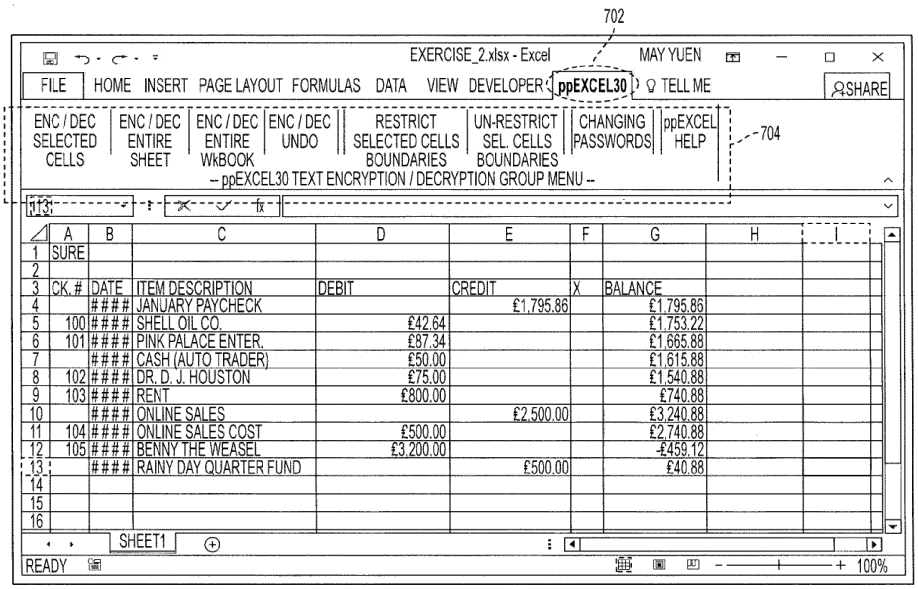
Фиг. 4



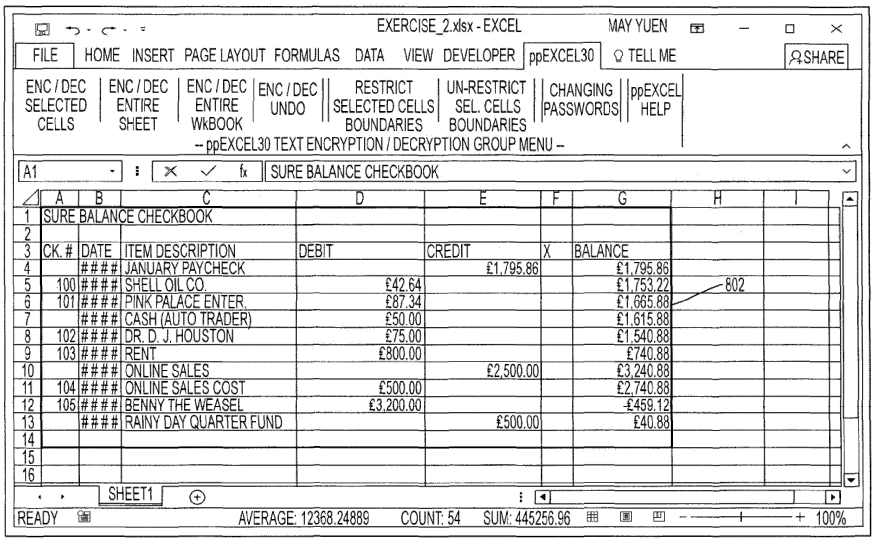
Фиг. 5



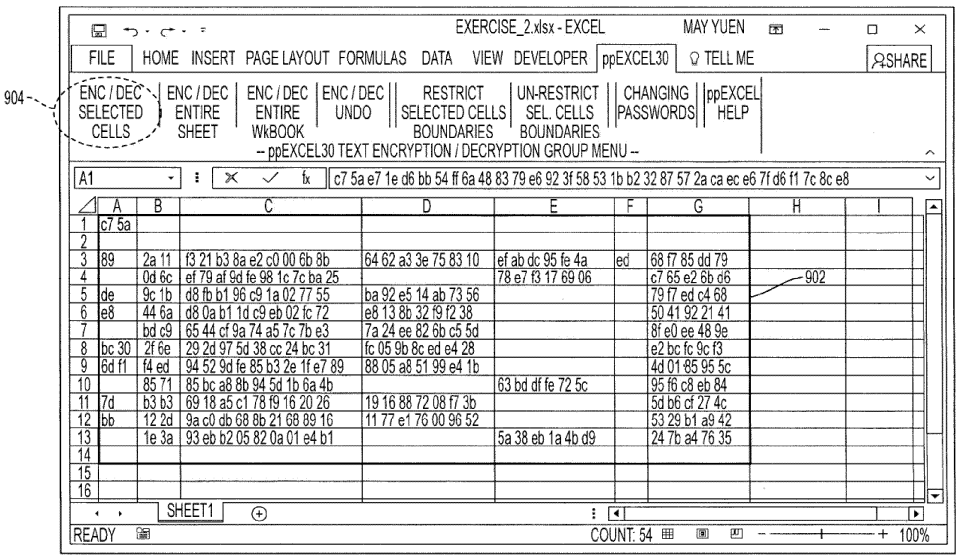
Фиг. 6



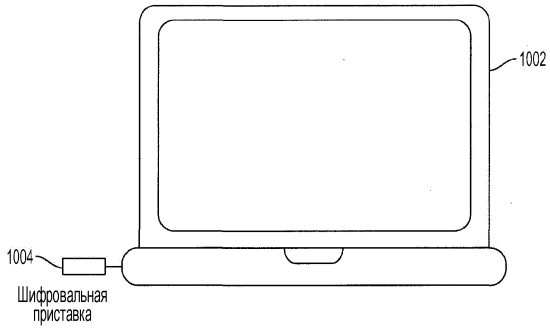
Фиг. 7



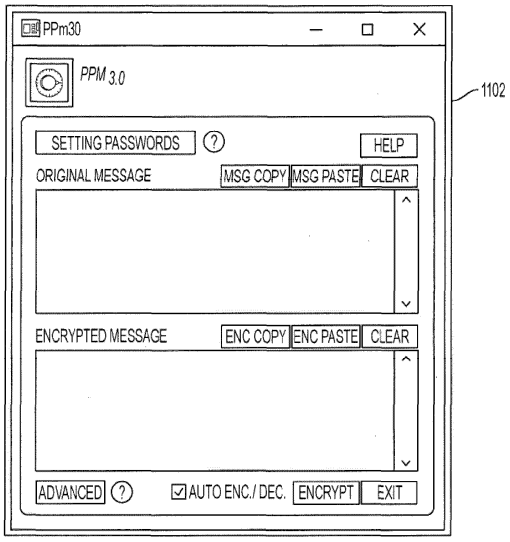
Фиг. 8



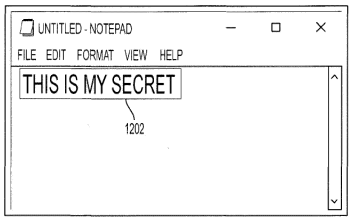
Фиг. 9



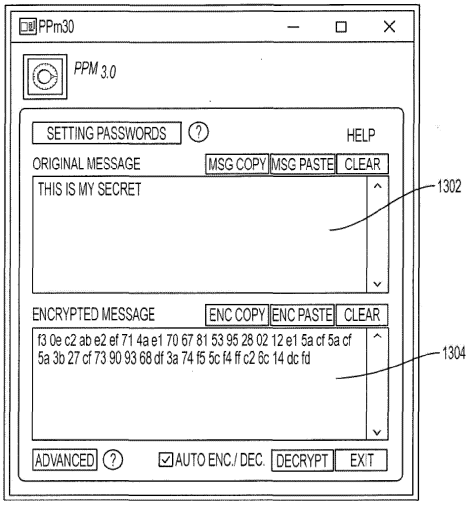
Фиг. 10



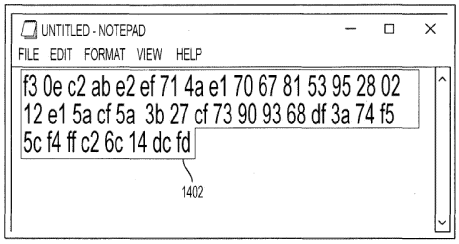
Фиг. 11



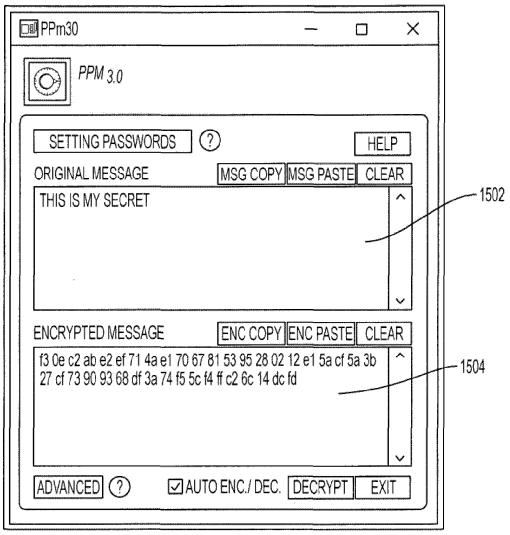
Фиг. 12



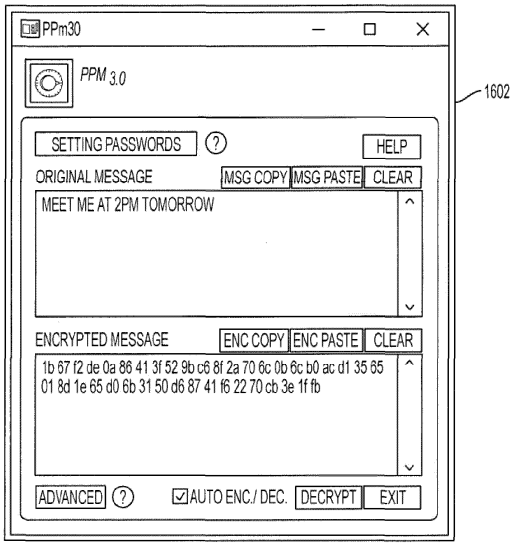
Фиг. 13



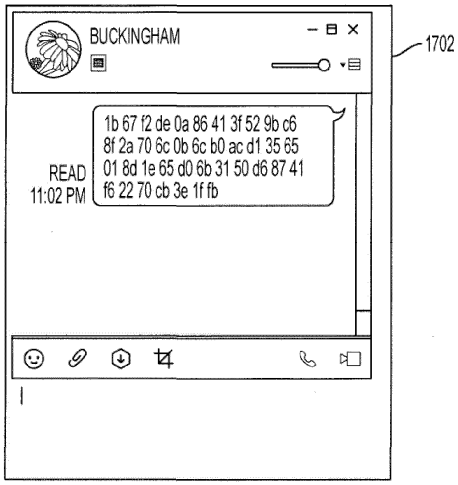
Фиг. 14



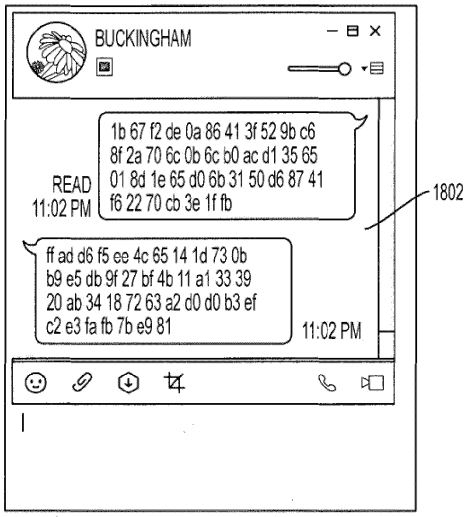
Фиг. 15



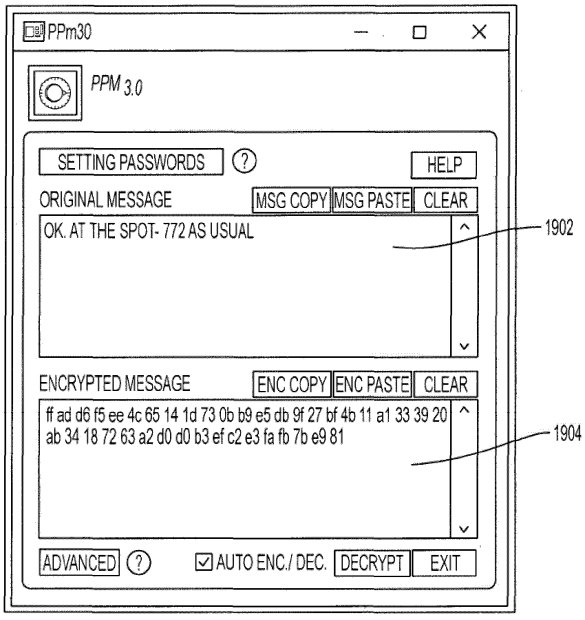
Фиг. 16



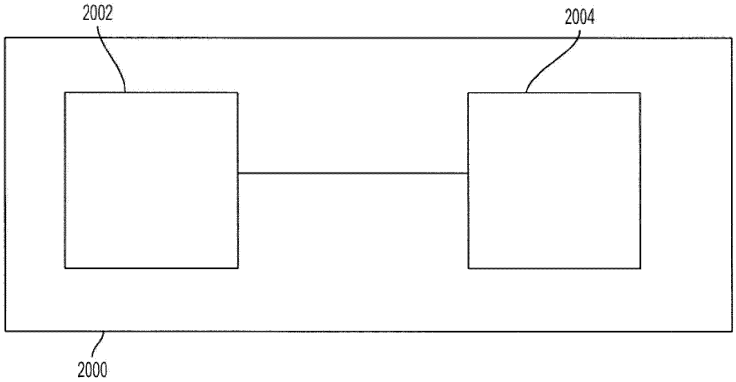
Фиг. 17



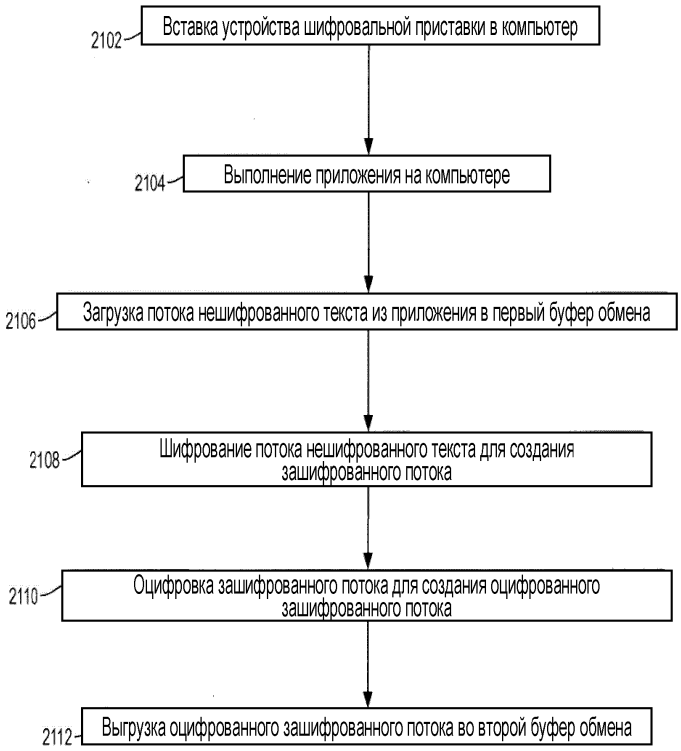
Фиг. 18



Фиг. 19



Фиг. 20



Фиг. 21

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2