RuBackup

Система резервного копирования и восстановления данных

Утилита RBCRYPT

Версия 1.0 2019

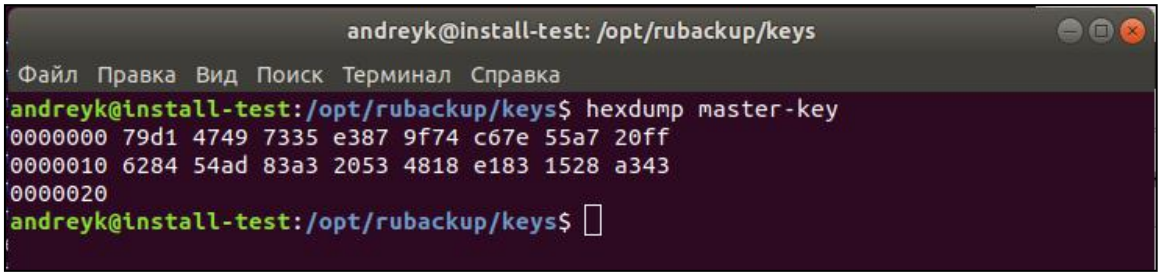
Оглавление

Введение

Утилита командной строки RBCRYPT используется для защитного преобразования файлов. RBCRYPT используется на стороне клиента RuBackup. Для защитного преобразования используется секретный ключ, задаваемый пользователем.

[!!! Важно] Секретный ключ необходимо хранить в месте, недоступным никому, кроме тех, кто должен иметь возможность произвести обратное преобразование файла. Утеря ключа делает невозможным обратное преобразование файла.

Секретный ключ рекомендуется распечатать при помощи утилиты hexdump, так как он может содержать неотображаемые на экране символы:



Алгоритмы преобразования, реализованные в RBCRYPT

Наименовние алгоритма	**Поддерживаемая rbcrypt длина ключа, бит**	**Примечание**
Anubis	128, 256	
Aria	128, 256	
CAST6	128, 256	
Camellia	128, 256	
Kalyna	128, 256, 512	Украинский национальный стандарт ДСТУ 7624:2014
Kuznyechik	256	Российский национальный стандарт ГОСТ Р 34.12-2015
MARS	128, 256	
Rijndael	128, 256	Advanced Encryption Standard (AES)
Serpent	128, 256	
Simon	128	
SM4	128	Chinese national standard for Wireless LAN
Speck	128, 256	
Threefish	256, 512, 1024	
Twofish	128, 256	

Использование RBCRYPT

Пользователь RuBackup может самостоятельно проводить защитное преобразование файлов, используя утилиту командной строки RBCRYPT.

Для работы утилиты необходимо создать файл с секретным ключом. Длина ключа должна соответствовать выбранному алгоритму преобразования (см.”Алгоритмы защитного преобразования, реализованные в RBCRYPT). По умолчанию длина ключа составляет 256 бит или 32 байта. Соответственно, файл ключа должен иметь длину 32 байта.

Режим защитного преобразования файла:

\# *rbcrypt -a kuzneyechik -c file-to-crypt.tgz -o crypted-file.tgz.cr -k .\key -r*

Данная команда произведет преобразование файла file-to-crypt.tgz ключом, который содержится в файле key, удалит файл file-to-crypt.tgz и создаст файл crypted-file.tgz.cr

Алгоритм преобразования в данном случае выбран ГОСТ Р 34.12-2015, длина ключа - 256 бит.

Режим обратного преобразования файла:

\# *rbcrypt -a kuzneyechik -x crypted-file.tgz.cr -o decrypted-file.tgz -k .\key -r*

Данная команда производит обратное преобразование файла crypted-file.tgz.cr ключом, который содержится в файле key, удалит файл crypted-file.tgz.cr и создаст файл decrypted-file.tgz

Описание всех опций RBCRYPT

-h справка

-v режим расширенной информации о работе утилиты

-a алгоритм преобразования, можно выбрать следующие варианты: anubis, aria, cast6, camellia, kalyna, kuznyechik или GOST_R_34_12_2015, mars, rijndael или AES, serpent, simon, sm4, speck, treefish, twofish

-1 выбрать длину ключа 128 бит (если алгоритм поддерживает эту длину ключа)

-2 выбрать длину ключа 256 бит (значение по умолчанию)

-5 выбрать длину ключа 512 бит (если алгоритм поддерживает эту длину ключа, если нет - то будет использован ключ максимально длинный из поддерживаемых)

-0 выбрать длину ключа 1024 бит (если алгоритм поддерживает эту длину ключа, если нет - то будет использован ключ максимально длинный из поддерживаемых)

-k файл с секретным ключом (ключ должен располагаться в первой строке файла)

-b размер блока данных при работе утилиты (размер по умолчанию 16384 байта, максимальный размер блока данных 1048576)

-o файл вывода

-c файл, для которого требуется произвести преобразование (нельзя эту опцию совмещать с опцией -x)

-x файл, для которого требуется произвести обратное преобразование (нельзя эту опцию совмещать с опцией -c)

-r удалять входящий файл (заданный опциями -c или -x)

Copyrights

Утилита RBCRYPT разработана Andrey Kuznetsov © 2019 с использованием библиотеки cppcrypto http://cppcrypto.sourceforge.net/

list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

;
;Copyright (c) 2007 Robert W. Waite <winstonwaite@gmail.com>
;
;Permission to use, copy, modify, and distribute this software for any
;purpose with or without fee is hereby granted, provided that the above
;copyright notice and this permission notice appear in all copies.
;
;THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
;WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
;MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
;ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
;WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
;ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
;OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

/*-
 * Copyright 2009 Colin Percival
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *   notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *   notice, this list of conditions and the following disclaimer in the
 *   documentation and/or other materials provided with the distribution.