

# RuBackup

Система резервного копирования и восстановления данных

Утилита RBCRYPT



Версия 1.0

2019

## Оглавление

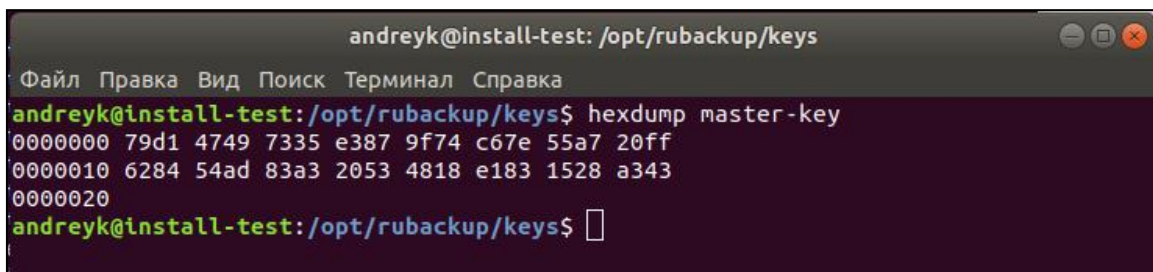
Введение.....	3
Использование RBCRYPT.....	5
Описание всех опций RBCRYPT.....	6
Copyrights.....	7

# 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:



```
andreyk@install-test: /opt/rubackup/keys
Файл Правка Вид Поиск Терминал Справка
andreyk@install-test:/opt/rubackup/keys$ hexdump master-key
00000000 79d1 4749 7335 e387 9f74 c67e 55a7 20ff
00000010 6284 54ad 83a3 2053 4818 e183 1528 a343
00000020
andreyk@install-test:/opt/rubackup/keys$
```

# Алгоритмы преобразования, реализованные в RBCRYPT

Наименование 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)

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

# Copyrights

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

Copyright (c) 2015-2016, kerukuro

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.

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 OWNER 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) 2012, Intel Corporation

;

; All rights reserved.

;

; Redistribution and use in source and binary forms, with or without

; modification, are permitted provided that the following conditions are

; met:

;

; \* Redistributions of source code must retain the above copyright

; notice, this list of conditions and the following disclaimer.

;

; \* 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.

;

; \* Neither the name of the Intel Corporation nor the names of its  
; contributors may be used to endorse or promote products derived from  
; this software without specific prior written permission.  
;  
;  
; THIS SOFTWARE IS PROVIDED BY INTEL CORPORATION "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 INTEL CORPORATION 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) 2014 Project Nayuki

#

# (MIT License)

# Permission is hereby granted, free of charge, to any person obtaining a copy of  
# this software and associated documentation files (the "Software"), to deal in  
# the Software without restriction, including without limitation the rights to  
# use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of  
# the Software, and to permit persons to whom the Software is furnished to do so,  
# subject to the following conditions:

# - The above copyright notice and this permission notice shall be included in  
# all copies or substantial portions of the Software.

# - The Software is provided "as is", without warranty of any kind, express or  
# implied, including but not limited to the warranties of merchantability,  
# fitness for a particular purpose and noninfringement. In no event shall the  
# authors or copyright holders be liable for any claim, damages or other  
# liability, whether in an action of contract, tort or otherwise, arising from,  
# out of or in connection with the Software or the use or other dealings in the  
# Software.

Copyright (c) 2013, Alexey Degtyarev.

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.

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.

\*  
\* THIS SOFTWARE IS PROVIDED BY THE AUTHOR 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 AUTHOR 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.

\*  
\* This file was originally written by Colin Percival as part of the Tarsnap  
\* online backup system.

\*/

%  
% In addition to these licenses, cppcrypto contains public-domain or non-copyrighted code written by:  
%  
% Wei Dai  
% Jean-Philippe Aumasson  
% Samuel Neves  
% Shawn Kirst  
% Peter Schwabe  
% Günther A. Roland  
% Martin Schläffer  
% Krystian Matusiewicz  
% Daniel J. Bernstein  
% vampire77  
% Guido Bertoni  
% Joan Daemen  
% Michaël Peeters  
% Gilles Van Assche  
% Hongjun Wu  
% Maxim Locktyukhin  
% Ronen Zohar  
% Romain Dolbeau  
% Andrew Moon  
% Vladimir Sedach