Автор:
25.09.14 09:27 -

Увидел свет выпуск свободной кри Sodium 1.0.0, совместимой на уровне API NaCl (Networking and Cry
распространяется

В отличие от NaCl в Sodium решены проблемы с переносимостью кода на разные программные и Ruby Python

По сравнению с OpenSSL, Sodium и NaCl предоставляют существенно более простой API, а такж

API Sodium включает следующие возможности:

- Операции шифрования с использованием аутентифицированных открытых и симметричны
- Создание и проверка цифровых подписей по открытым и симметричным ключам. Позволяе
- Операции хэширования, позволяющие сформировать слепок от сообщения, имеющий фикс
- Средства для формир DoS-атак SipHash-2-4
- Безопасный генератор псевдослучайных чисел, пригодный для использования в криптогра

1. Главная ссылка к новости (https://github.com/jedisct1/libsodium/re...)
2. OpenNews: Проект Tox развивает свободную альтернативу Skype
3. OpenNews: Представлен новый защищённый SSH-сервер TinySSH
4. OpenNews: Компания Google представила BoringSSL, форк OpenSSL
5. OpenNews: Первый выпуск LibreSSL, форка OpenSSL от проекта OpenBSD

Тип: Программы
Ключевые слова: sodium , crypt , ssl , (
найти похожие документы

1.1 , Anonim , 12:39, 25/09/2014 [ответить] [
смотреть все
к модератору

Автор:
25.09.14 09:27 -

+
–
Bitrig еще жив?

1.2 , anonymous , 13:13, 25/09/2014 [ответить] [смотреть все] [к модератору] + / –
список алгоритмов на оф. сайте отсутствует

2.3 , Аноним , 13:26, 25/09/2014 [^] [ответить смотреть все к модератору + –
сводный - может быть весь текст скрыт на каждую функциональность [показать] используе...

3.6 , anonymous , 14:35, 25/09/2014 [^] [ответить смотреть все к модератору + –
Сильно урезанный набор алгоритмов - OpenSSL для хомячков.

4.9 , ryzhov_al , 15:31, 25/09/2014 [^] [ответить смотреть все к модератору + –
Это просто nacl, допиленная для использования с dnscrypt-proxy.

4.10 , Аноним , 15:43, 25/09/2014 [^] [ответить] [смотреть все] [к модератору] + / –
Я так понимаю, что принцип был не все алгоритмы одинаково полезны, как и не все...
весь текст скрыт
[показать]

1.4 , pda

, 13:58, 25/09/2014 [
ответить
] [
смотреть все
] [
к модератору
]
+
/
–
> и непредсказуемым результатом операции

Ммм... Выхлоп /dev/random в качестве хеш-функции для словарей...
(На самом деле, я знаю, что имелось ввиду. Но как написано! :)

1.8 , Аноним , 14:46, 25/09/2014 [ответить] [смотреть все] [к модератору] + / –
Монструозный больно Tweetnacl лучше и от системы тоже мало зависит ...
весь текст скрыт
[
показать
]
Ваш комментарий

Read more http://www.opennet.ru/opennews/art.shtml?num=40674