

❧ КРИПТОГРАФИЯ ❧
КОТОРАЯ ПРОСТО РАБОТАЕТ

АРТЁМ ПОПЦОВ

2017-02-12

СОДЕРЖАНИЕ.

- ❶ ПОСТАНОВКА ЗАДАЧИ.
- ❷ ВЫБОР ИНСТРУМЕНТА.
- ❸ ДОСТУПНЫЕ ИНСТРУМЕНТЫ.
- ❹ GNU PRIVACY GUARD.
- ❺ OFF-THE-RECORD MESSAGING.

ПОСТАНОВКА ЗАДАЧИ.

Шерлок
Холмс



Доктор
Ватсон



☞ Необходимо обеспечить три параметра:

- Конфиденциальность
- Целостность
- Аутентификацию

РЕАЛЬНОСТЬ.

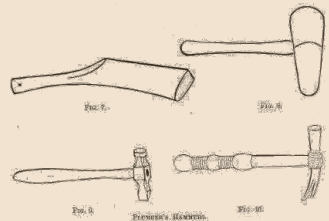


ВЫБОР ИНСТРУМЕНТА.

“Криптография – единственный набор инструментов для обеспечения безопасности в интернете, который у нас есть. Мы открываем наш ящик с инструментами и всё, что мы имеем – криптомолоток.” – Ян Голдберг

Характеристики хорошего инструмента:

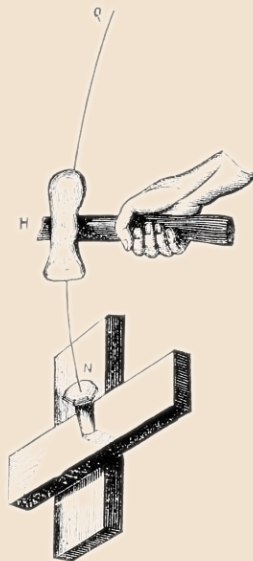
- Удобство использования (англ. *usability*)
- Доступность (англ. *deployability*)
- Эффективность (англ. *effectiveness*)
- Надёжность (англ. *robustness*)



УДОБСТВО ИСПОЛЬЗОВАНИЯ.

☞ Инструмент должен быть удобен для использования.

- Необходим понятный интерфейс, упрощающий корректное использование инструмента.
- В идеале, инструмент должен оказывать минимальное влияние на рабочий процесс пользователя.



ДОСТУПНОСТЬ.

☞ Инструмент должен предъявлять разумные требования, иначе его никто не будет использовать.

- Необходима интеграция с существующим рабочим окружением пользователя, а не наоборот.



Fig. 3.



Fig. 4.



Fig. 5.



Fig. 6.

ENGINEER'S HAMMERS.

ЭФФЕКТИВНОСТЬ.

☞ Инструмент должен обеспечивать характеристики, которые были "по гарантии".

- Сообщество должно иметь возможность провести независимый аудит инструмента.
- Следовательно, исходный код инструмента, документация и описание протоколов должны быть доступны сообществу (желательно, под свободной лицензией.)

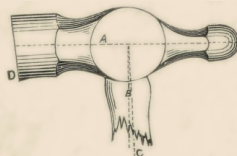


FIG. 84. —HANDLE AT RIGHT ANGLE TO PLANE OF LENGTH OF HAMMER HEAD.

НАДЁЖНОСТЬ.

☞ Если “что-то пошло не так”, то инструмент должен сделать всё возможное, чтобы уменьшить урон.

“[...] a general principle of robustness: be conservative in what you do, be liberal in what you accept from others.”
– Jon Postel

(Общий принцип надёжности Джона Постела: будьте консервативны в том, что делаете, и либеральны в том, что получаете от других.)



ДОСТУПНЫЕ ИНСТРУМЕНТЫ.

- GNU Privacy Guard (GnuPG)
- Off-The-Record Messaging (OTR)

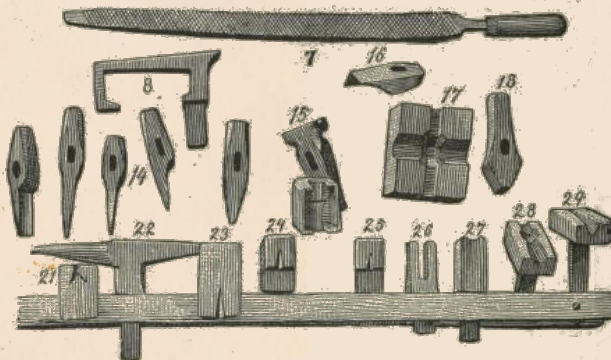


FIG. 156.

GNU PRIVACY GUARD.

☞ GNU Privacy Guard (GnuPG) – свободная программа шифрования информации и создания электронных цифровых подписей (ЭЦП).

- GnuPG относительно удобен в использовании, есть дружественные графические интерфейсы.
- Программа доступна на большинстве платформ и интегрируется с рабочим окружением пользователя.

Задачи, решаемые с помощью GnuPG:

- Электронная подпись данных
- Шифрование данных

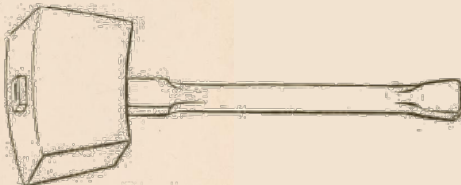


Fig. 12. Carpenter's Wooden Mallet.

УСТАНОВКА GnuPG.

На большинстве дистрибутивов GNU/Linux GnuPG можно поставить из репозитория. Пример для Ubuntu GNU/Linux:

```
$ sudo apt-get install gnupg gnupg-agent
```

На Microsoft Windows можно воспользоваться **Gpg4win** (gpg4win.org).

☞ Руководство от Electronic Frontier Foundation:

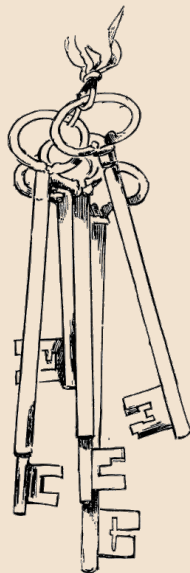
- ssd.eff.org/ru

☞ “Самозащита электронной почты” от Free Software Foundation:

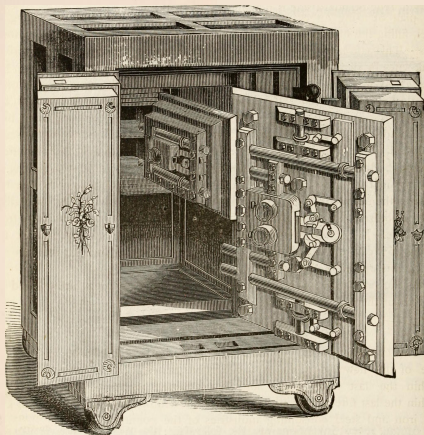
- emailselfdefense.fsf.org/ru/

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ – 1.

☞ Криптография с открытым ключом (или *асимметричная криптография*) – система шифрования и/или электронной подписи, при которой используется пара открытый ключ-закрытый ключ, и открытый ключ передаётся по незащищённому каналу.



КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ – 2.



СОЗДАНИЕ ПАРЫ КЛЮЧЕЙ – 1.

Пара “закрытый ключ – публичный ключ” может быть создана следующей командой:

```
$ gpg --gen-key
```

При создании ключа необходимо:

① Выбрать тип ключа:


Please select what kind of key you want:

(1) RSA and RSA (default)

(2) DSA and Elgamal

(3) DSA (sign only)

(4) RSA (sign only)

Your selection? 1 

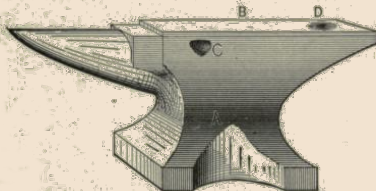



FIG. 56.—DEVICE FOR FACILITATING THE FORGING OF CLIPS FOR FIFTH WHEELS.

СОЗДАНИЕ ПАРЫ КЛЮЧЕЙ – 2.

2. Выбрать длину ключа:

RSA keys may be between 1024 and 4096 bits long.

What keysize do you want? (2048) 2048 

Requested keysize is 2048 bits

3. Выбрать “срок годности” ключа:

Please specify how long the key should be valid.


0 = key does not expire

<n> = key expires in n days


<n>w = key expires in n weeks

<n>m = key expires in n months

<n>y = key expires in n years

Key is valid for? (0) 1y 

Key does not expire at all

Is this correct? (y/N) y 

СОЗДАНИЕ ПАРЫ КЛЮЧЕЙ – 3.

- ④ Указать реальное имя владельца ключа:

Real name: Vasiliy I. Pupkin 🖱️

- ⑤ Указать адрес электронной почты владельца:

Email address: vip@example.ru 🖱️

- ⑥ (Опционально) указать комментарий к ключу.

- ⑦ Проверить указанную информацию и подтвердить её:

You selected this USER-ID:

"Vasiliy I. Pupkin <vip@example.ru>"

Change (N)ame, (C)omment, (E)mail

or (O)kay/(Q)uit? 0 🖱️

- ⑧ Задать пароль для доступа к закрытому ключу.

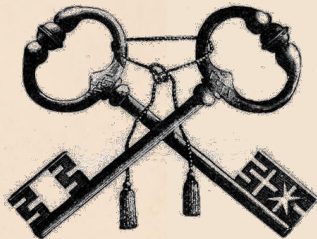
- ⑨ “Пошуметь” для генерации достаточного количества энтропии.

СОЗДАНИЕ ПАРЫ КЛЮЧЕЙ – 4.

Результат:

```
$ gpg --list-secret-keys  
/home/vip/.gnupg/secring.gpg
```

```
-----  
sec    2048R/F4A78166 2016-08-29  
uid                               Vasiliy I. Pupkin <vip@example.ru>  
ssb    2048R/BAED1502 2016-08-29
```



СЕРТИФИКАТ ОТЗЫВА КЛЮЧА.

☞ Сертификат отзыва ключа (англ. *revocation certificate*) – Сертификат, который, будучи опубликованным, говорит о том, что связанный с ним ключ более не должен использоваться.

- Сертификат должен храниться в безопасном месте (например, в сейфе.)
- Сертификат должен быть создан сразу после генерации приватного ключа.

Случаи, при которых необходимо отзывать ключ:


- Забыт (утерян) пароль к ключу.
- Ключ был скомпрометирован.
- Ключ более не действителен.
- ...

ГЕНЕРАЦИЯ СЕРТИФИКАТА ОТЗЫВА КЛЮЧА.

```
$ gpg --output revoke.asc --gen-revoke F4A78166
```

```
sec 2048R/F4A78166 2016-08-29
```

```
Vasiliy I. Pupkin <vip@example.ru>
```

Create a revocation certificate for this key? (y/N) y 

Please select the reason for the revocation:

0 = No reason specified


1 = Key has been compromised

2 = Key is superseded

3 = Key is no longer used


Q = Cancel

(Probably you want to select 1 here)

Your decision? 1 



ОТЗЫВ КЛЮЧА.

 Вы не должны выполнять отзыв ключа без причины!

- Импортировать сертификат:

```
$ gpg --import revoke.asc
gpg: key F4A78166: "Vasiliy I. Pupkin <vip@example.ru>"
    revocation certificate imported
gpg: Total number processed: 1
gpg:    new key revocations: 1
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:    3  signed:    0
    trust: 0-, 0q, 0n, 0m, 0f, 3u
```

- Загрузить обновлённый ключ на сервер:

```
$ gpg --keyserver gpg.mit.edu --send-keys F4A78166
```



ЭЛЕКТРОННАЯ ПОДПИСЬ.

Электронная подпись обеспечивает следующие свойства:

- **Целостность** – гарантия отсутствия искажений данных с момента формирования подписи.
- **Авторство** – принадлежность подписи владельцу ключа.
- **Неотказуемость** – фиксирование невозможности отказа от авторства

Примеры практического применения электронных подписей:

- Подпись важных писем и документов.
- Подпись релизов пакетов в DVCS Git.
- Подпись дистрибутивов программ.
- ...

ЭЛЕКТРОННАЯ ПОДПИСЬ ФАЙЛОВ.

Подписать файл можно следующим образом:

```
$ touch important-file.txt
```

```
$ gpg --detach-sign important-file.txt
```

Электронная подпись будет сохранена файле
important-file.txt.sig:

```
$ ls important-file*
```

```
important-file.txt important-file.txt.sig
```

Проверка подписи:

```
$ gpg --verify important-file.txt.sig
```



ШИФРОВАНИЕ.

- ❶ **Ассимметричное** шифрование документа для доктора Ватсона с помощью его открытого ключа:

```
$ gpg --output doc.gpg --encrypt --recipient \  
    dr.watson@example.ru doc
```

Расшифровка ранее зашифрованного документа с помощью приватного ключа доктора Ватсона:

```
$ gpg --output doc --decrypt doc.gpg
```

- ❷ Или можно использовать **симметричное** шифрование:

```
$ gpg --output doc.gpg --symmetric doc
```



Недостатки GNUPG – 1.



НЕДОСТАТКИ GNUPG – 2.



НЕДОСТАТКИ GnuPG – 3.

- ❶ Используются долгоживущие закрытые ключи для шифрования.
- ❷ Благодаря цифровым подписям можно с уверенностью сказать, кто автор сообщения, и доказать авторство третьим лицам.
- ❸ Относительно сложен в использовании.

👉 GnuPG не обладает свойствами, необходимыми для обеспечения приватного разговора через IM-протокол.

OFF-THE-RECORD MESSAGING.

☞ Цель Off-the-Record Messaging (OTR) – обеспечить для IM свойства, присущие обычным беседам.

Возможности:

- Шифрование
- Аутентификация
- Отрицаемая аутентификация (англ. *deniable authentication*) не позволяет доказать аутентичность собеседника третьим лицам.
- Совершенная прямая секретность (англ. *perfect forward secrecy*) – компроментация долговременных ключей не приводит к компроментации сессионных ключей.

Недостатки:

- Хорошо работает только с протоколами общения в реальном времени.

IM-КЛИЕНТЫ, ПОДДЕРЖИВАЮЩИЕ OTR.

Из коробки:

- Adium
- BitlBee
- ChatSecure
- IM+
- Jitsi
- LeechCraft
- MCabber
- Psi+
- Xabber

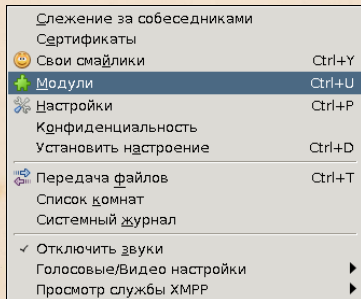
С использованием плагина:

- Pidgin (Gaim) – Через плагин `pidgin-otr`
- Kopete
- Miranda IM
- irssi
- Gajim
- Tkabber
- Vacuum-IM

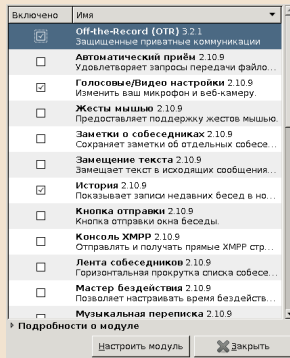
УСТАНОВКА И НАСТРОЙКА PIDGIN-OTR – 1.

```
$ sudo apt-get install pidgin-otr
```

Из меню “Средства” открываем список модулей и включаем OTR:



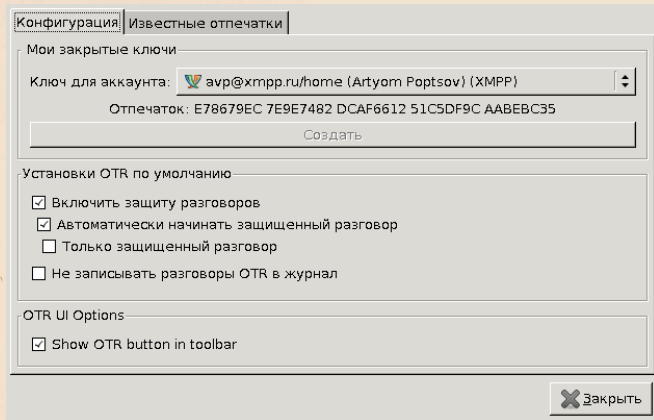
Открытие списка модулей



Включение модуля

УСТАНОВКА И НАСТРОЙКА PIDGIN-OTR – 2.

- Необходимо сгенерировать ключ (нажать на кнопку “Создать”)



The screenshot shows the 'Configuration' tab of the Pidgin OTR settings window. It is divided into three sections: 'My private keys', 'OTR default settings', and 'OTR UI Options'. In the 'My private keys' section, the 'Key for account' field is populated with 'avp@xmpp.ru/home {Artyom Poptsov} {XMPP}', and the 'Fingerprint' field shows 'E78679EC 7E9E7482 DCAF6612 51C5DF9C AABEBC35'. A 'Create' button is located below these fields. The 'OTR default settings' section contains four checkboxes: 'Enable conversation protection' (checked), 'Automatically start protected conversation' (checked), 'Only protected conversation' (unchecked), and 'Do not record OTR conversations in the log' (unchecked). The 'OTR UI Options' section has one checked checkbox: 'Show OTR button in toolbar'. A 'Close' button is in the bottom right corner.

Конфигурация | Известные отпечатки

Мои закрытые ключи

Ключ для аккаунта: avp@xmpp.ru/home {Artyom Poptsov} {XMPP}

Отпечаток: E78679EC 7E9E7482 DCAF6612 51C5DF9C AABEBC35

Создать

Установки OTR по умолчанию

- ☒ Включить защиту разговоров
- ☒ Автоматически начинать защищенный разговор
- ☐ Только защищенный разговор
- ☐ Не записывать разговоры OTR в журнал

OTR UI Options

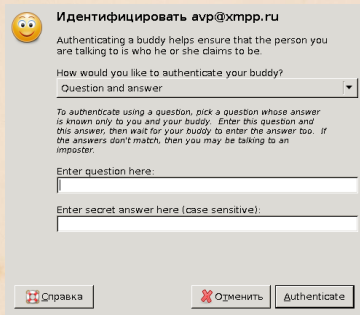
- ☒ Show OTR button in toolbar


Закрыть

Генерация закрытого ключа

УСТАНОВКА И НАСТРОЙКА PIDGIN-OTR – 3.

Далее следует аутентифицировать собеседника при первом разговоре:



 Идентифицировать avp@xmpp.ru




Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?
Question and answer ▼

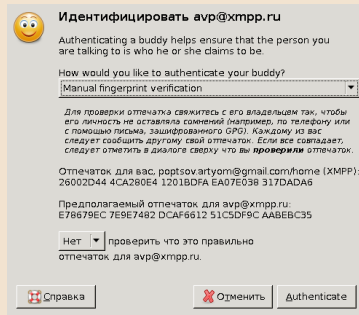
To authenticate using a question, pick a question whose answer is known only to you and your buddy. Enter this question and this answer, then wait for your buddy to enter the answer too. If the answers don't match, then you may be talking to an imposter.


Enter question here:
|

Enter secret answer here (case sensitive):
|

 Справка  Отменить  Authenticate

Аутентификация с помощью
вопроса



 Идентифицировать avp@xmpp.ru

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.




How would you like to authenticate your buddy?
Manual fingerprint verification ▼

*Для проверки отпечатка свяжитесь с его владельцем так, чтобы его личность не оставяля сомнений (например, по телефону или с помощью письма, зашифрованного GPG). Каждому из вас следует сообщить другому свой отпечаток. Если все совпадает, следует отметить в диалоге сверху что вы **проверили** отпечаток.*

Отпечаток для вас, poptsov.artiom@gmail.com/home (XMPP):
26002D44 4CA280E4 1201BDFA EA07E038 317DADA6

Предполагаемый отпечаток для avp@xmpp.ru:
E78679EC 7E9E7482 DCAF6612 51C5DF9C AABEBC35

проверить что это правильно
отпечаток для avp@xmpp.ru.

 Справка  Отменить  Authenticate

Аутентификация по отпечатку
ключа

СПАСИБО ЗА ВНИМАНИЕ!

Контакты:

- Web-сайт: poptsov-artyom.narod.ru
- Эл. почта: poptsov.artyom@gmail.com
- Отпечаток ключа GnuPG: D0C2 EAC1 3310 822D 98DE
B57C E9C5 A2D9 0898 A02F

Презентация и её “исходники” под лицензией Creative Commons: github.com/artyom-poptsov/talks/tree/master/defcon-nn/

Вопросы?

Лицензия.

Copyright ©2017 Artyom V. Poptsov
<poptsov.artiom@gmail.com>

Права на копирование других изображений, использованных в данной работе, принадлежат их владельцам.

Данная работа распространяется на условиях лицензии Creative Commons Attribution-ShareAlike 4.0 International:
<https://creativecommons.org/licenses/by-sa/4.0/>

ИСПОЛЬЗОВАННЫЕ МАТЕРИАЛЫ.

Использованные источники:

- Ian Goldberg, "OTR messaging" (CC-BY-NC-ND 3.0) –
<https://archive.org/details/IanGoldberg-OtrMessaging>
- Nikita Borisov, Ian Goldberg, Eric Brewer (2004-10-28).
"Off-the-Record Communication, or, Why Not To Use PGP":
<https://otr.cypherpunks.ca/otr-wpes.pdf>
- Ian Goldberg, "Off-the-Record Messaging: Useful Security and
Privacy for IM":
<https://www.youtube.com/watch?v=uI1x-z5oafc>

Основа для дизайна:

- Richardson, Milton Thomas (ed.), "Practical blacksmithing",
volume 1 (PD) – <https://archive.org/details/practicalblacksm01richuoft>
- Richardson, Milton Thomas (ed.), "Practical blacksmithing",
volume 2 (PD) –
<https://archive.org/details/practicalblacksm00rich>