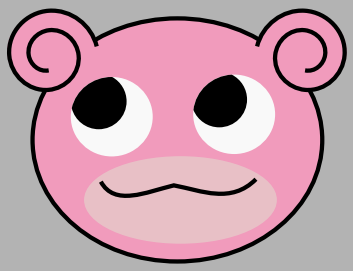
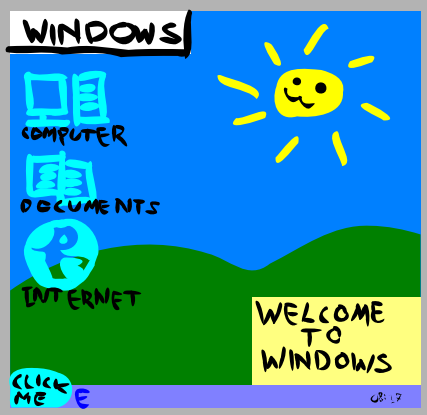
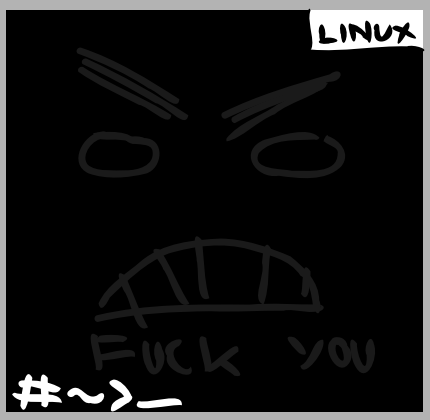
Как работать с GPG

Шаг первый:
Установи Tails
на флешку







Шаг второй:
Открывай терминал
и создай свой ключ в GPG

```
# gpg --gen-key
```

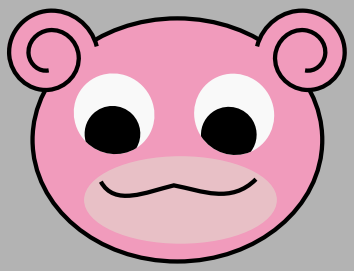
Вводи любое имя и почту
Как пароль советую шесть+ слов
«Diceware passphrase»

Подожди и проверь ключ:

```
# gpg --list-secret-keys
```

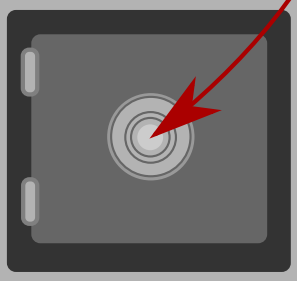
Как работать с GPG

Шаг третий: Опубликовать открытый ключ



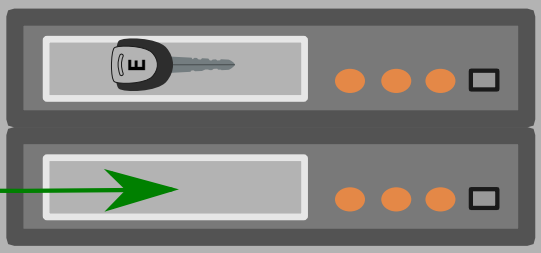
D-ключ для чтения шифра

Защищено паролем



E-ключ для шифрования

pgp.mit.edu



Сначала узнай ID ключа:

```
# gpg --list-secret-keys
-------------------------
sec    rsa/2048/????????
```

Отправь ключ на сервер:
(пиши команду в одну строку)

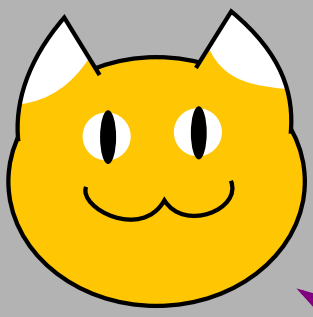
```
# gpg --keyserver pgp.mit.edu
      --send-keys ????????
```

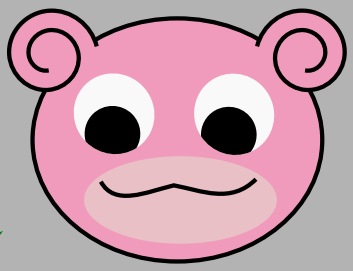
Теперь проверь результат:

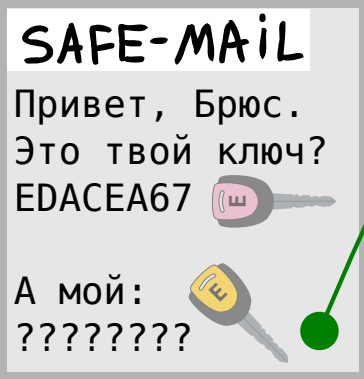
```
# gpg --keyserver pgp.mit.edu
      --search-keys ????????
```

Как работать с GPG

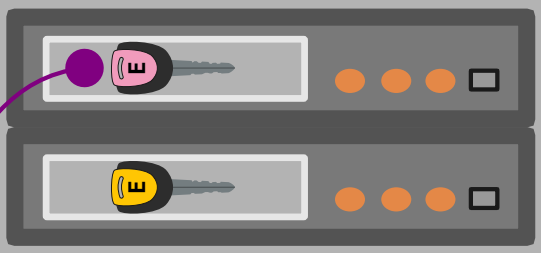
Шаг четвёртый: получить ключ собеседника







pgp.mit.edu



Запроси ключ с сервера:
(пиши команду в одну строку)

```
# gpg --keyserver pgp.mit.edu
      --recv-keys EDACEA67
```

Или загрузи ключ с диска:
(например «Tails signing key»)

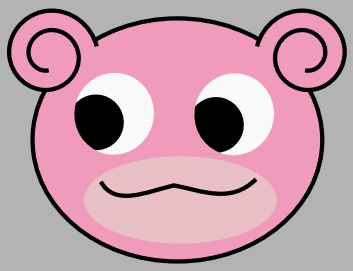
```
# gpg --import ~/tails-signing.key
```

Не забудь проверить ключи:

```
# gpg --list-public-keys
```

Как работать с GPG

Шаг пятый: Зашифровать



SAFE-MAiL

message.txt

```
Здравствуй,
друг мой.
У меня тут
секретное
сообщение…
```

message.txt.asc

```
-----BEGIN PGP MESSAGE-----
hQIMA0Ix/nnXtjDfAQ//UI/qqnJ
aBa6PSZEubCgxEfGcIvNtWM
wHtADOCjmETV5J5f6F/VBJ/gs
Cu44MvIvk5/sSKUnIQfEyG3Ke
-----END PGP MESSAGE-----
```

/tmp/msg-decrypt

```
Здравствуй,
друг мой.
У меня тут
секретное
сообщение…
```

Шифрование, это несложно:

```
# gpg -e -a -r EDACEA67 ~/message.txt
```

-e — зашифровать
-a — в текстовую форму
-r — указать ID получателя
~/ — каталог пользователя

answer.txt

```
Привет,
Лисичка.
Подпиши
сообщение
пожалуйста.
```

Шаг шестой: Расшифровать

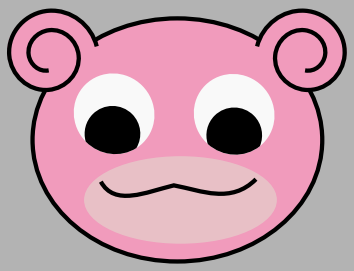
answer.asc

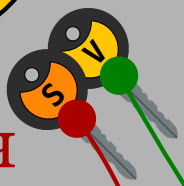
```
-----BEGIN PGP MESSAGE-----
hQEMA+kPha8bFQ4CAQf+M
ypYoTVlRGJ4Mk8wUKwnhaH
Uemj9hIIHSxDS0Z4BpY6Aqd
3BUnGfPVxKCdB/13vrXgzeI3
-----END PGP MESSAGE-----
```

```
# gpg -d ~/answer.asc > ~/answer.txt
```

Как работать с GPG

Шаг седьмой: подписать сообщение

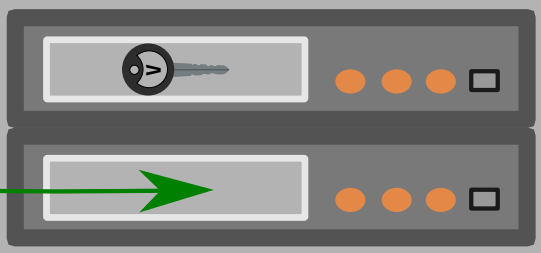




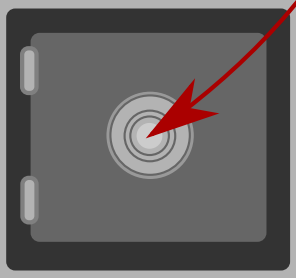
S-ключ для подписи

V-ключ для проверки подписи

pgp.mit.edu



Защищено паролем



Личный ключ для подписи

Публичный ключ для проверки

Теперь подпиши и зашифруй:

```
# gpg -sea -r EDACEA67 ~/message.txt
```

-sea — подпись, шифр, текст

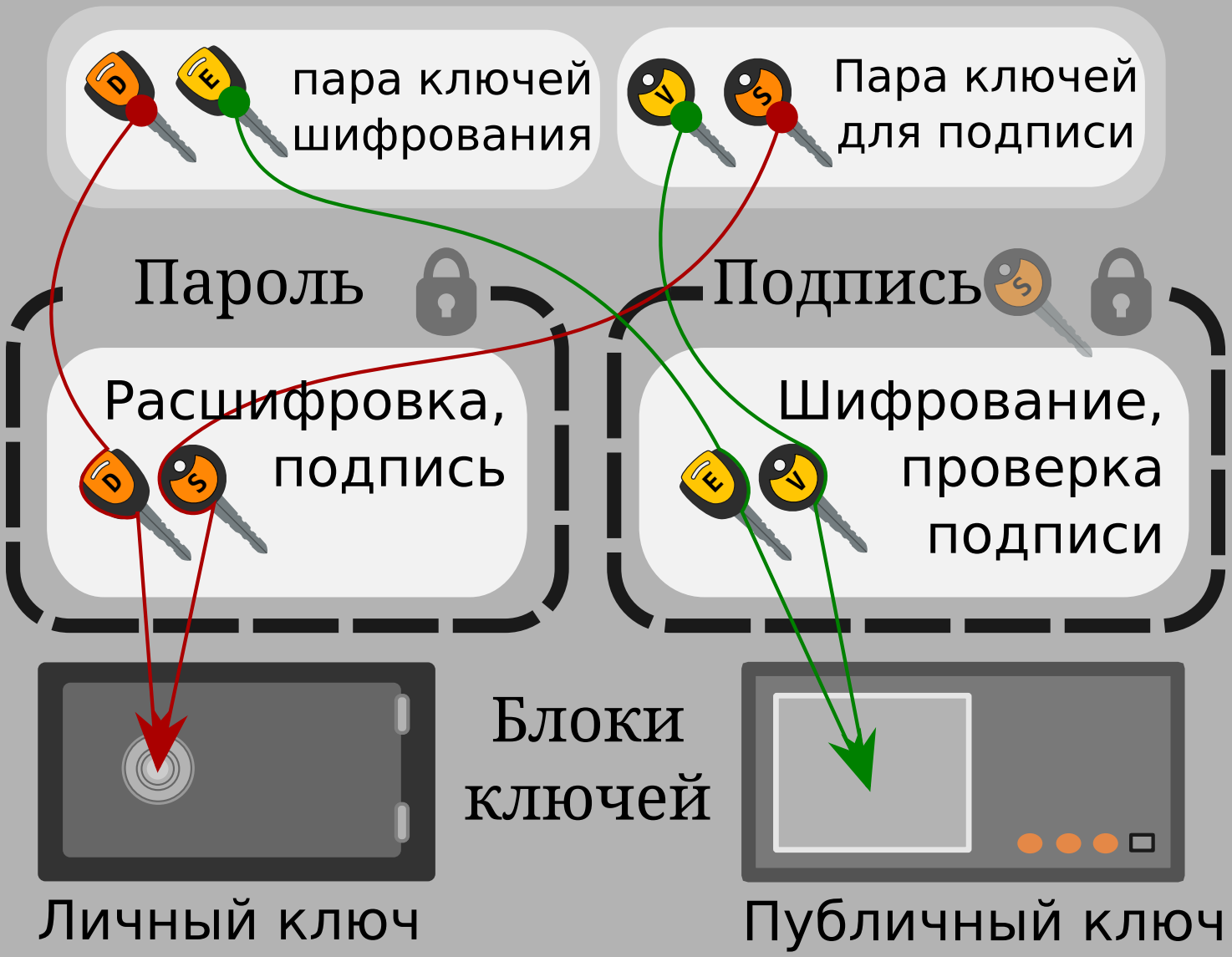
Чтобы проверить подпись:
(для примера образ диска Tails)

```
# gpg --verify ./tails.iso.sig
               ./tails.iso
```

Как работать с GPG

Немного теории: ключевые пары и блоки

```
# gpg --gen-key
```



Появились вопросы?

```
# man gpg
```

```
/
```

— кнопка поиска

Что ж, это всё.