**PSD**

**PSD**(*paranoia satisfaction device*)- устройство, позволяющее безопасно хранить и производить автоматизированный ввод паролей на любой технике, позволяющей подключать устройства ввода через USB порт.

**Устройства, необходимые для использования PSD:**

1) Доверенный PC с которого будут устанавливаться списки паролей

2) Телефон на Android, с которого будет передаваться сигнал на ввод пароля и храниться первые части ключей

3) PSD, на котором хранятся вторые части паролей

4) **Foreign PC** (или что-то, поддерживающее ввод с клавиатуры). На него будет введен пароль

**Данные/ключи, которые должны храниться на устройствах для осуществления работы:**

**1) Доверенный PC:**

* зашифрованный список паролей(любое шифрование подойдет. Оно не влияет на систему)
* USBKey(ключ(32 байт) для заливания данных на PSD с доверенного PC. Ключ нужен т к мы часто коннектим PSD к разным PC, которые теоретически могут попытаться переписать хранимые части паролей с целью распознать части, что прислались с телефона)

**2) Android:**

* BTKey(ключ шифрования BT-канала для AES) - 32 bytes
* HBtKey(ключ для HMAC. Поддерживает целостность) - 32 bytes
* Список из 255 паролей part1(126 байт на каждый пароль + по 2 байта на id)

**3) PSD:**

* BTKey(ключ шифрования BT-канала для AES) - 32 bytes
* HBTKey(ключ для HMAC. Поддерживает целостность) - 32 bytes
* Список из 255 паролей part2(126 байт на каждый пароль + по 2 байта на id)
* USBKey(ключ(32 байт) для заливания данных на PSD с доверенного PC

**4) Foreign PC:**

* none

**Общий принцип работы по действиям:**

1) устанавливаем USB ключ

делается всего один раз за все время пользования PSD

при установке USB ключа, все данные перетираются на PSD

2.1) заливаем список паролей(part2) на PSD, используя авторизацию USBKey

заливаем BTKey(0) и HBTKey(0), сгенерированные на доверенном PC

2.2) заливаем список паролей(part1) на Android

заливаем BTKey(0) и HBTKey(0), сгенерированные на доверенном PC

3) Вставляем PSD в чужой PC  
PSD коннектится к Android через BT  
4) Android посылает шифрованный Package через BT(шифрование Package будет описано ниже)

в package зашифрованы:

* BTKey(1)
* HBTKey(1)
* один пароль из списка(part1)
* ID пароля

5) PSD получает Package и дешифрует его. Записывает новые значения для BTKey и HBTKey

Берет part2 пароля из своего списка, взятого по присланному индексу и XOR-ит part1 ⊕ part2 = resPass

6) resPass вводится на Foreign PC

7) отсылаем нешифрованный пакет об успешности ввода пароля. Текст ошибки, если есть. Или код

**THE PACKAGE:**

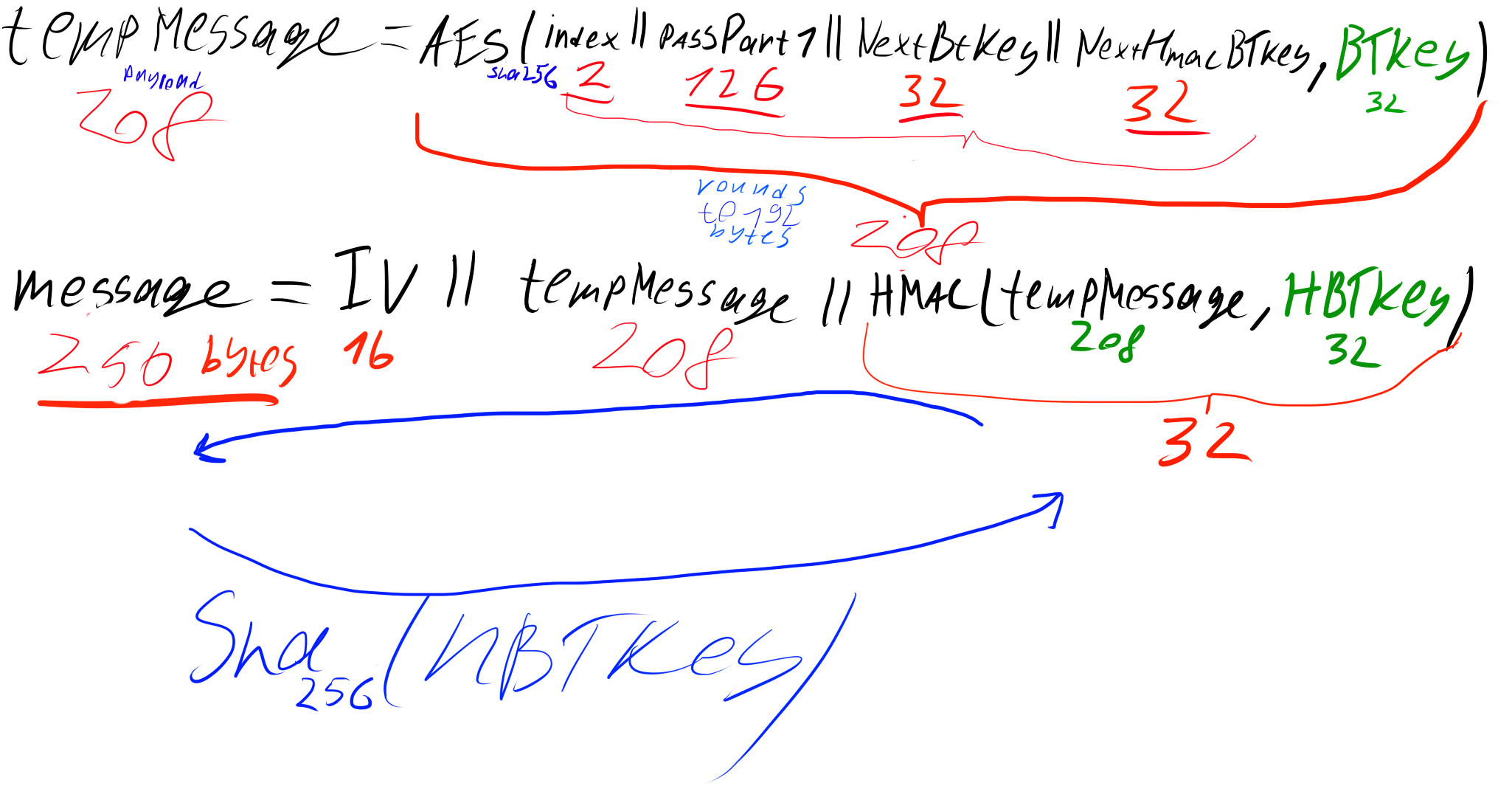
tempMessage = AES(BTKey(0), index + part1Pass + BTKey(1) + HBTKey(1)) //208 bytes

message = IV + tempMessage + HMAC(tempMessage, HBTKey(0)) //256 bytes

в следующем пакете:

HBTKey(0) станет HBTKey(1), а присылать будем HBTKey(2)

BTKey(0) станет BTKey(1), а присылать будем BTKey(2)



**Хранение данных на устройствах**

**Пользователь должен помнить(!!!) свой UserKey**

1) На доверенном PC:

* полные пароли, в формате XML, зашифрованные с AES256 (SHA512(UserKey))

2) На PSD:

* part2 пароли
* следующий HBTKey(ключ для проверки целостности следующего пакета, присланного через BT)
* следующий BTKey(ключ для дешифрования следующего присланного пакета)

3) На телефоне:

* part1 пароли(шифрованные паролем, установленном на телефоне)
* следующий HBTKey(ключ для проверки целостности следующего пакета, отправляемого через BT)
* следующий BTKey(ключ для шифрования следующего отправляемого пакета)
* графический ключ для дешифрования part1 паролей

