

Monero Crypto-Lock Basic Demonstration

Prerequisite: You must have a Monero wallet, the monerod daemon running and the monero-wallet-rpc running and available on port 18082.

Two bash script files:

- crypto-lock-sign.sh
- crypto-lock-verify.sh

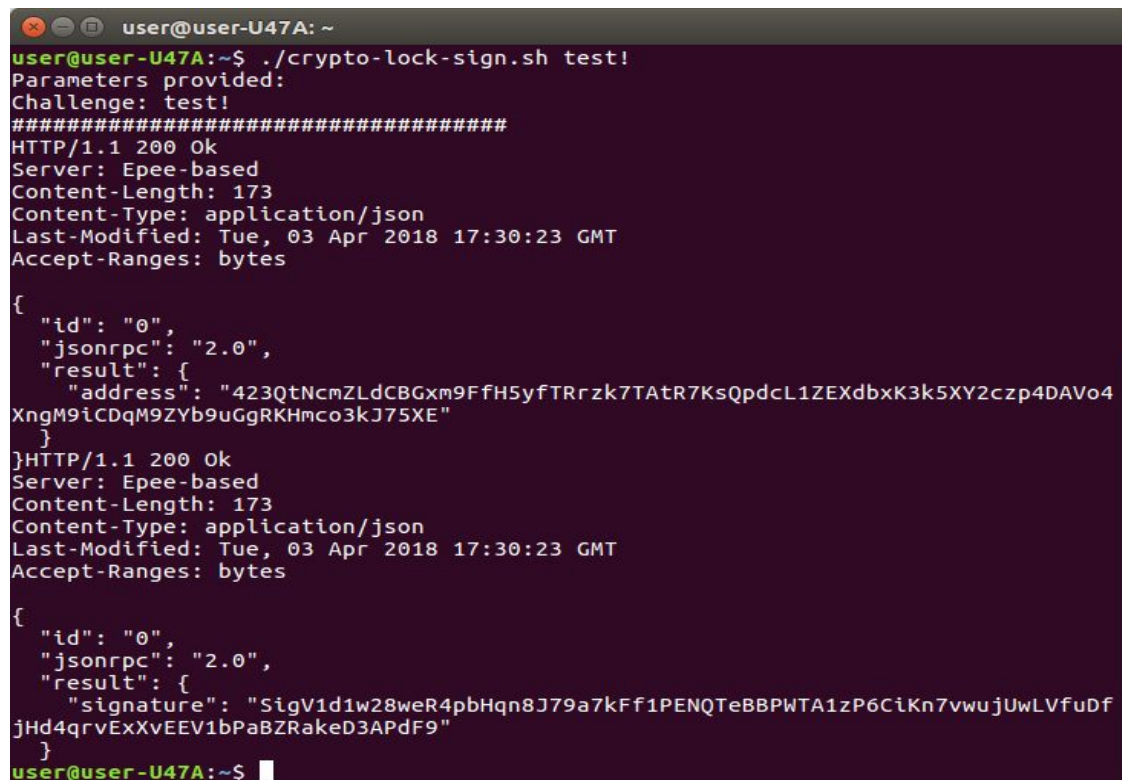
Are provided for this demonstration. These scripts need to be executable by issuing the following commands:

```
chmod +x crypto-lock-sign.sh
chmod +x crypto-lock-verify.sh
```

You can verify that everything is working by running the *crypto-lock-sign.sh* script:

```
./crypto-lock-sign.sh test
```

If successfully executed you should see output similar to that shown below:



```
user@user-U47A: ~
user@user-U47A:~$ ./crypto-lock-sign.sh test!
Parameters provided:
Challenge: test!
#####
HTTP/1.1 200 Ok
Server: Epee-based
Content-Length: 173
Content-Type: application/json
Last-Modified: Tue, 03 Apr 2018 17:30:23 GMT
Accept-Ranges: bytes

{
  "id": "0",
  "jsonrpc": "2.0",
  "result": {
    "address": "423QtNcmZLdCBGxm9FFH5yfTRrzk7TAtR7KsQpdCL1ZEXdbxK3k5XY2czp4DAVo4
XngM9iCDqM9ZYb9uGgRKHmco3kJ75XE"
  }
}HTTP/1.1 200 Ok
Server: Epee-based
Content-Length: 173
Content-Type: application/json
Last-Modified: Tue, 03 Apr 2018 17:30:23 GMT
Accept-Ranges: bytes

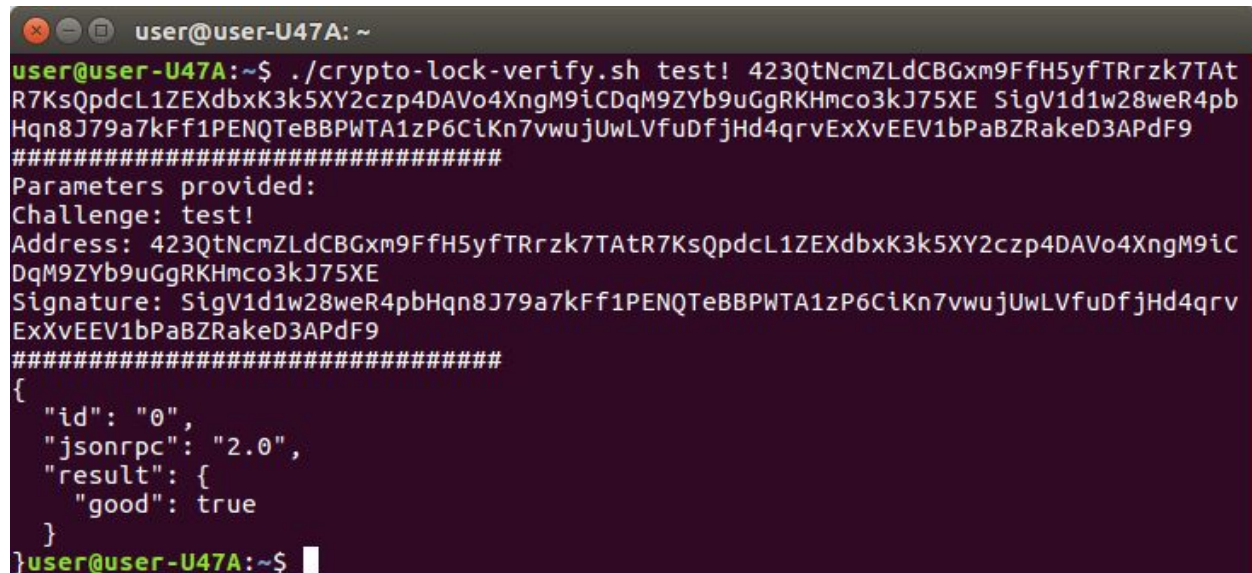
{
  "id": "0",
  "jsonrpc": "2.0",
  "result": {
    "signature": "SigV1d1w28wer4pbHqn8J79a7kFf1PENQTeBBPwTA1zP6CiKn7vwuJUwLVfuDf
jHd4qrVExXvEEV1bPaBZRakeD3APdF9"
  }
}
user@user-U47A:~$
```

Obviously you will have a different wallet address and signature.

Now if you take the output from the above run script and pass the challenge string, address, and signature as input into the *crypto-lock-verify.sh* :

```
./crypto-lock-verify.sh test!  
423QtNcmZLdCBGxm9FfH5yfTRzk7TAtR7KsQpdcL1ZEXdbxK3k5XY2czp4DAVo4XngM9iCDqM9ZYb9uG  
gRKHmco3kJ75XE  
SigV1d1w28weR4pbHqn8J79a7kFf1PENQTeBBPWTA1zP6CiKn7vwujUwLVfuDfjHd4qrvExXvEEV1bPaBZ  
RakeD3APdF9
```

Each input parameter having a space separating it from the next parameter. You should see output similar to:



```
user@user-U47A: ~  
user@user-U47A:~$ ./crypto-lock-verify.sh test! 423QtNcmZLdCBGxm9FfH5yfTRzk7TAt  
R7KsQpdcL1ZEXdbxK3k5XY2czp4DAVo4XngM9iCDqM9ZYb9uGgRKHmco3kJ75XE SigV1d1w28weR4pb  
Hqn8J79a7kFf1PENQTeBBPWTA1zP6CiKn7vwujUwLVfuDfjHd4qrvExXvEEV1bPaBZRakeD3APdF9  
#####  
Parameters provided:  
Challenge: test!  
Address: 423QtNcmZLdCBGxm9FfH5yfTRzk7TAtR7KsQpdcL1ZEXdbxK3k5XY2czp4DAVo4XngM9iC  
DqM9ZYb9uGgRKHmco3kJ75XE  
Signature: SigV1d1w28weR4pbHqn8J79a7kFf1PENQTeBBPWTA1zP6CiKn7vwujUwLVfuDfjHd4qrv  
ExXvEEV1bPaBZRakeD3APdF9  
#####  
{  
  "id": "0",  
  "jsonrpc": "2.0",  
  "result": {  
    "good": true  
  }  
}  
user@user-U47A:~$
```