smerf.net

Ethereum

Ethereum
Blockchain Development
Week 13
Dr Ian Mitchell

1 VM

Following the instructions below:

- Download the Ethereumvirtual machine from: `4125.smerf.net`.
- Decompress the file to a *.vdi file and remember where you saved it.
- Open Oracle Virtual Box v6.1.
- Create a new virtual machine linked to the recently download .vdi file

2 Encryption

1. **Symmetric Keys.** In an essay explain how Symmetric Keys work to encrypt and decrypt a message. Include in your essay the advantages and disadvantages of such a method.

2. **Asymmetric Keys.** In an essay explain how Asymmetric Keys work to encrypt and decrypt a message. Include in your essay the advantages and disadvantages of such a method.

3 Implementation

1. **Sending a message using GPG**

   - Install GPG.
   - Generate a key-pair for user "Ian"
   - Generate a key-pair for user "Mohamed"
   - Create a plain-text message and save in your "week13" folder as "Ian.txt"
   - The objective is to send a message from *local-user* "Mohamed" to the *recipient* "Ian".
   - Encrypt the message using the recipient's public key. Why did you not require a passphrase?
   - Decrypt the message using the recipient's private key. Why do you require a passphrase?

2. **Authentication**

   - Generate a key-pair for user "Trojan".
   - Create a plain-text message and save in your "week13" folder as "trojan.txt".
   - The objective is to send a message to the recipient, "Ian". The problem is to investigate the sender of the message?
   - Encrypt the message using the recipient's public key.
   - Decrypt the message using the recipient's private key.
   - Confirm who sent the message?

3. **Digital Signatures**

   - Create a plain-text message and save in your "week13" folder as "signature.txt".

- The objective is to add a digital signature to the encrypted message so that the recipient can determine the identification of the sender.
- Encrypt the message using local-user "Mohamed" and recipient "Ian" and sign the message with local-user "Mohamed" signature.
- Which user's passphrase do you enter?
- Decrypt the message using the recipient's private key.
- Confirm who sent the message?

4 Building a blockchain

- Open Browser and go to remix
- Download file, `w13ex1.sol`, from 13folder
- Upload: upload this to the remix editor
- Compile the smart contract
- Deploy the smart contract
- Check the `totalSupply`
- Check the balance of the owner
- As the owner transfer 10 IANs to another account
- Check the balances of these accounts

5 Reading

Chapter 1 from [1].

References

[1] X. Wu, Z. Zhihong, and D. Song. *Learn Ethereum.* Packt, 1st edition, 2019.