Week 9 Crypto and SSH Part-1

Explain conceptually all the following terms, and how/why they are needed for SSH and TLS/SSL

- **Symmetric Encryption**
    - Symmetric encryption is a type of encryption where only one key is used to both encrypt and decrypt data. The devices that communicates via symmetric encryption has to exchange the key, so that it can be used in the process of decrypting the data.

- **Asymmetric Encryption**
    - Asymmetric encryption, is a when the keys are created in paris, one for encryption and only the other key of the pair can decrypt the data. The keys are usually interchangeable. Even though it is common to be able to swap the keys functionality with eachother, this is not necessary.

- **Hashing**
    - Hashing is a the process of converting the input of a fixed length of text.
    - An hashing function can only function one way, so you cannot use the hashing function to retrieve your original input.
    - When hashing is done, there is a danger that two keys will generate the same hash value.

Explain what it takes to safely log in to an SSH server, without having to provide a password

- At first, there are a pair of SSH keys that gets generated, one public and one private key. The public key is used to store on, for example, a droplet server. The private key is stored with the client. Only clients with the private key that fits the pair can then connect to the server
- In the process of the connection between the client and the server, the server authenticates itself by giving its public key to the client, to confirm where it has or hasnt the correct private key to make a pair.

Explain the term SSH-tunnel, and provide a practical example for its use

- The tunnel is used to send data through a safe and encrypted connection, or tunnel. As an example, you could use SSH to transfer files in a safe way, using for example the FTP protocol. So even if the protocol itself isnt encrypted, it is used inside of an encrypted tunnel.

Explain conceptually the purpose of Symmetrical Encryption, Asymmetrical Encryption and hashing for an SSH-connection

- Symmetric
    - Bruges til selve forbindelsen til at kryptere dataen mellem server og klient.
- Asymmetric
    - Bruges ved udvekslingen af keys når man skal oprette den krypterede forbindelse.
- Hashing

    - Hashing is used to check the integrity of the data, and to make sure that the received data is intact and uncompromised.

Explain the steps you have to go through to set up a server with MySQL, as secure as possible →

- How can we limit the client IP's that can connect
    - We can limit the ips by a firewall on a server'
- If set up to allow only localhost and a firewall that deny 3306, can we still connect "safely" from a remote server
    - Yes, through an ssh tunnel
- how to set up an SSL connection that anyone can use.
    - `bind-address i /etc/mysql/my.cnf to 0.0.0.0`
    - More info here: https://docs.google.com/document/d/1L3DTzTv3yR9yM3h843e1LxAmQnHX0p7-A58OJLBBgsA/edit#
      Under "Connecting directly to MySQL with Mandatory SSL"