Week-13 Crypto - 2

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

* Symmetric Encryption
* Asymmetric Encryption
* Hashing and        MAC (Message Authentication Code)
* Digital Signatures
* Certificates
* Certificate Authorities and Certificate Trust Hierarchies
* Cipher Suites
* Diffie–Hellman key exchange

Feel free to introduce some of the terms using a saved Wireshark capture of a TLS-handshake

Explain, and preferably demonstrate,  the consequence of using a self-issued certificate