[Hands-on Exercises](https://sofia.instructure.com/courses/4984/assignments/syllabus" \l "id14)

**# install openssl on MacOS**

* sudo port install openssl
* openssl dgst -md5 -r # for md5
* openssl dgst -sha1 -r # for sha1
* openssl dgst -sha256 -r # for sha256

**# play with hash fuctions:**

* # hex digit: 0123456789abcdef
* # one nibble = 4 bits = one hex character = half byte

>>> $ md5 tmp

>>> md5: tmp: Is a directory

>>>

>>> $ md5 i

>>> md5: i: No such file or directory

>>>

>>> $ md5 j

>>> MD5 (j) = 9190e032fe2adee69d67316eda9014d5

>>>

>>> $ md5 20180106\_computer.pdf

>>> MD5 (20180106\_computer.pdf) = 29da59b016356edb77c1557ddf38c574

>>>

>>> openssl dgst -sha256 20180106\_computer.pdf #64\*4=256

>>> SHA256(20180106\_computer.pdf)= 2e9561cc02af8863dd578cfccf9551225f19ce327d74a2971e4f997b919c1004

[Homework #1](https://sofia.instructure.com/courses/4984/assignments/syllabus#id15)

* hash fundamentals
  + What is hash?

**Ans: Hashing means map a string of arbitrary size to a string of fixed size.**

* + What are md5 and SHA-2 hash?

**Ans: They are both widely used hash function. MD5 produces a 128-bit hash value. SHA stands for Secure Hashing Algorithm and SHA-2 is a set of hash functions.**

* + How md5 and SHA-2 works?

**Ans: Each algorithm can be described in two stages: preprocessing and hash computation. Preprocessing involves padding a message, parsing the padded message into m-bit blocks, and setting initialization values to be used in the hash computation. The hash computation generates a message schedule from the padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest.**

* + Play with md5 and SHA-2 hash, each with 5 of your files
* play with git on the backgrounds
  + create a project structure and control it in git
  + mkdir blockchaain && cd blockchaain
  + mkdir howework1
  + mkdir howework2
  + mkdir howework3
  + mkdir project
  + # create a README file in each folder
  + # write your experience/notes in the README
  + git init
  + git add .
  + git commit -a -m "Sofia Blockchain Technology"
  + # play with git with push/pull throughout the course
* Read "A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto"
* Start to install Hyperledger Fabric
* Start to think what is the best for your final project:
  + What bitcoin is?
  + What blockchain is?
  + What blockchain does?
  + Why blockchain becomes so hot?
  + How blockchain is being used?