IN3210/4210 2020 – Exercise 3

1) Compute the digest of some file using sha1sum and sha256sum respectively. Make a small modification to the input file (e.g., changing one bit or one character). Compute the updated digests. What do you observe and why? What is the problem with ensuring the integrity of a file just with a hash value?
2) Generate a 2048-bit RSA keypair using *openssl*. Also extract the public key in a separate file. You may refer to the Key Generation section in https://www.feistyduck.com/library/openssl-cookbook/online/ch-openssl.html for information on how to do this, or refer to the man pages (e.g. https://www.openssl.org/docs/man1.0.2/man1/openssl.html).
3) Use the *openssl dgst* command to sign some file using the private key from above and your choice of sha hash algorithm (see man dgst). Then use *openssl dgst* to verify the signature. Afterwards, modify the signed file slightly before trying to verify the signature again.

The exercise is not to be submitted.