2.1 Generating Message Digest and MAC

Email used: marsamu@kth.se

Question 1:
The output length varies for each hash function with MD5 consisting of 128-bits, SHA1 160-bits, SHA256 256-bits. MD5 is faster than both SHA1 and SHA256, as it is less complex and generates a smaller number.

Question 2:

- MD5 = b506fd2764abbef73fba3f5fe4276ef1
- SHA1 = db12e2f776d774c18b333fa8a90d025911089304
- SHA256 = 1d972b709006c480ecb402a2c532db813fe47280f8b5719aa003028b0b228fb3

2.2 Keyed Hash and HMAC

Question 3:
The security of HMAC depends on the key, which does not have a fixed size. When using HMAC the key is used directly, and when the key is longer than the cryptographic hash functions block size it does compute the key as a function of the hash.

Question 4:

- HMAC-MD5(test.txt)= 7c30a9f906eea922652199ccea2abfc8
- HMAC-SHA1(test.txt)= 62bf3e724fe51a4bc6046e9e83174755e534e804
- HMAC-SHA256(test.txt)= 96f8c8f094a44ba3d54455104032b02df87b30d9d0e787ba9509c18670c4621b

2.3 The Randomness of One-way Hash

Question 5:
Difference between MD5 is 162 bits out of 256, and SHA256 is 348 bits out of 512. Both in decimal and binary the hash looks very different. Hashing with one different bit results in very varying results, because it should not be possible to find patterns.

- MD5 = 9796c700ed053b9897ece3b390c5b554
- MD5**(old)** = b506fd2764abbef73fba3f5fe4276ef1
- SHA256 = ea7af026394f47299e9b10166a370f9b47264ce917cda47fc3810295c7f1d684
- SHA256**(old)** = 1d972b709006c480ecb402a2c532db813fe47280f8b5719aa003028b0b228fb3