Номер зачетки: 1800189

1. Создайте текстовый файл содержащий вашу фамилию и имя.

```
taiiiga@raw:~$ cat > textfile
Iskander Khisamov
```

2. Вычислите хеш для этого файла алгоритмами MD4, MD5, SHA, SHA512.

```
taiiiga@raw:~$ openssl dgst -md4 textfile
MD4(textfile)= 9c8b9c30b75e80c4cd003ef2114bc562
taiiiga@raw:~$ openssl dgst -md5 textfile
MD5(textfile)= ed0780b5e38fa6ce0e014cd61fe1a744
taiiiga@raw:~$ openssl dgst -sha1 textfile
SHA1(textfile)= ce0fad1462f8c4218d6d6234016f38717eaa531a
taiiiga@raw:~$ openssl dgst -sha512 textfile
SHA512(textfile)= 0b4200f644bcc46de12f62c97186ed6e1ee6ff9c5187636
1fe0b913a01dea205b41a561b0e637508cadda7e8627997ac7986cf3114387403
e7555224d277a373
```

3. Измените содержимое файла, вычислите хеши, сравните с предыдущим хешами.

```
taiiiga@raw:~$ echo "Ravilevich" >> textfile
taiiiga@raw:~$ cat textfile
Iskander Khisamov
Ravilevich
taiiiga@raw:~$ openssl dgst -md4 textfile
MD4(textfile)= 34e153dc7851fd6dc377ba5a0e008f85
taiiiga@raw:~$ openssl dgst -md5 textfile
MD5(textfile)= 9bb372b75ec84ce232e786a127b86923
taiiiga@raw:~$ openssl dgst -sha1 textfile
SHA1(textfile)= 12665926f59704a6355f363981ed9364d267f7f7
taiiiga@raw:~$ openssl dgst -sha512 textfile
SHA512(textfile)= 1b30866e16f1bf0848f17b73b0f22923f1c34458954f221
08cc33392d802f046c7f3bacc8c25c6e8cdbddb476b92af0c3eb89c808f6fd058
c5dbb8c41a0db33a
```

4. Вычислите хеш для большого файла (файл у всех разный) алгоритмами MD4, MD5, SHA, SHA512 засекая время выполнения (команда time).

```
taiiiga@raw:~$ fallocate -l 1G bigfile
taiiiga@raw:~$ time openssl dgst -md4 bigfile
MD4(bigfile)= ca2bc5d1f9b9325b6ea9547104ac26ca

real    0m3,625s
user    0m0,798s
sys     0m2,629s
taiiiga@raw:~$ time openssl dgst -md5 bigfile
MD5(bigfile)= cd573cfaace07e7949bc0c46028904ff

real    0m7,440s
user    0m2,080s
sys     0m4,731s
taiiiga@raw:~$ time openssl dgst -sha1 bigfile
SHA1(bigfile)= 2a492f15396a6768bcbca016993f4b4c8b0b5307

real    0m5,801s
user    0m1,069s
sys     0m4,275s
taiiiga@raw:~$ time openssl dgst -sha512 bigfile
SHA512(bigfile)= c5041ae163cf0f65600acfe7f6a63f212101687d41a57a4e
18ffd2a07a452cd8175b8f5a4868dd2330bfe5ae123f18216bdbc9e0f80d131e6
4b94913a7b40bb5

real    0m7,374s
user    0m4,867s
sys     0m2,056s
```

5. Вычислите имитовставку, используя алгоритм SHA512, для текстового файла с разными ключами, сравните результаты.

```
taiiiga@raw:~$ cat > text.txt
Live Text
^Z
[2]+  Stopped                 cat > text.txt
taiiiga@raw:~$ openssl dgst -sha512 -mac HMAC -macopt key:123456
text.txt
HMAC-SHA512(text.txt)= 7c0c045d4c4f1e7a6b27cfe0c6ec4327a77a620b98
51a883f9ad43020f30fa7594a718e11a6df2b76f28f34a28877547c16cef83296
d79cb9e90a26bb353afac
taiiiga@raw:~$ openssl dgst -sha512 -mac HMAC -macopt key:7890 te
xt.txt
HMAC-SHA512(text.txt)= 08e000dc43201a641d4ca650d5152ae817070f7ec5
dbccdd5766ce0c6a6c1c8ff70eb463daf4a662a355e400541cc0e899bdb69da0d
156dfe24e41585f1ef7a8
```

6. Получите имитовставку для текстового файла с разными ключами, имитовставка длиной 9 байт, в формате base64, используя алгоритм DES-CBC, сравните результаты.

```
taiiiga@raw:~$ openssl rand -base64 9 > key.bin
taiiiga@raw:~$ openssl enc -des-cbc -in textfile -out textfile.b64 -pataiiiga@raw:~$ openssl enc -des-cbc -in textfile -out textfile.b64 -pas
s file:./key.bin -a
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
taiiiga@raw:~$ openssl dgst -sha512 -mac HMAC -macopt key:123456 textfile.b64
HMAC-SHA512(textfile.b64)= 2579a83e3d91928dc3a4a9e10948f8e11e0b5bfd15cd377c0d9c1b371f77b3884d93cdba5a1fae80c859a8df4f3b709a7ac03d8ca6852f6426
8763ec9eae5f01
taiiiga@raw:~$ openssl dgst -sha512 -mac HMAC -macopt key:7890 textfile.b64
HMAC-SHA512(textfile.b64)= a6ee66f23b8468105dcc470309cce777856239db47550290c61ddfede3fe71ad68afad056d8f168717683a729007ea5d65641ee8531a52551e
f4c0b0dd49b59f
```