zad1

zad 2

Plik do zaszyfrowania

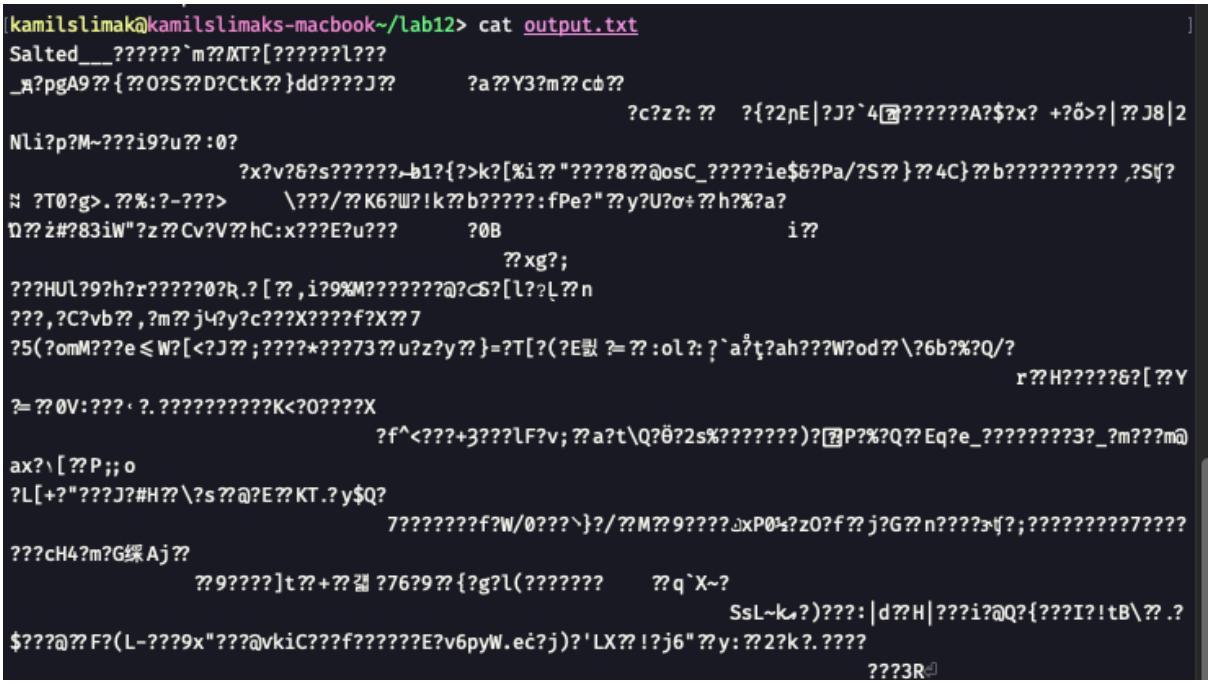
```
kamilslimak@kamilslimaks-macbook~/lab12> cat text.txt
Lorem ipsum dolor sit amet, consectetur adipiscing elit. In cursus mattis orci. Curabitur vel mi ut mag
na lobortis auctor. Maecenas diam libero, aliquet quis enim in, tristique euismod turpis. Praesent laci
nia urna posuere enim luctus mollis. Sed commodo lacinia tellus nec tristique. Praesent ut nulla id tel
lus tincidunt elementum. Nulla convallis faucibus rhoncus. Quisque leo dolor, mollis sit amet tincidunt
 at, aliquam vitae orci. Donec ullamcorper nulla a purus hendrerit accumsan. Proin sollicitudin ferment
um orci a porttitor. Morbi sit amet hendrerit quam.

Nullam at sem pharetra, scelerisque erat nec, commodo urna. Praesent id dolor tincidunt, congue turpis
quis, sagittis nisi. Integer egestas enim at arcu euismod ullamcorper. Curabitur venenatis massa purus,
 ac gravida arcu cursus sed. Vestibulum non elementum dolor, a placerat justo. Aenean tincidunt suscipi
t facilisis. Aenean hendrerit dignissim feugiat. Pellentesque quis erat eros. Vestibulum fermentum tinc
idunt dui quis consequat. Mauris mollis efficitur ipsum quis efficitur. Donec est velit, mattis non max
imus et, suscipit quis purus. Nam aliquet egestas est, id pretium mi pharetra ac.
kamilslimak@kamilslimaks-macbook~/lab12>
```

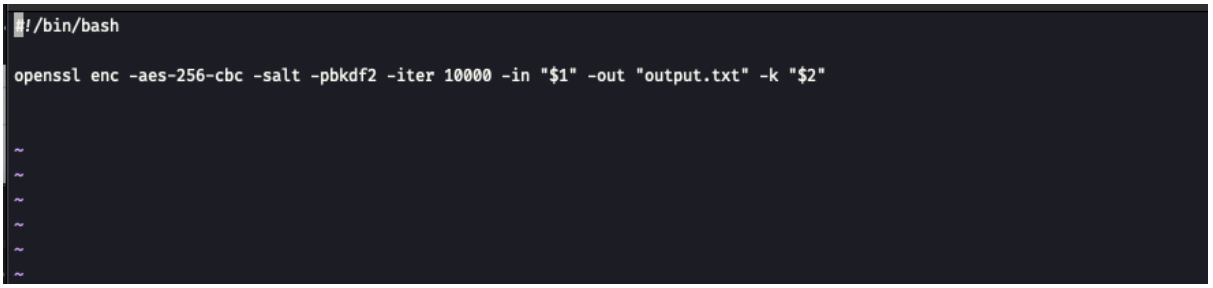
Wykonanie skryptu

```
kamilslimak@kamilslimaks-macbook~/lab12> ./aes.sh text.txt "haslo"
```

Zaszyfrowany plik:

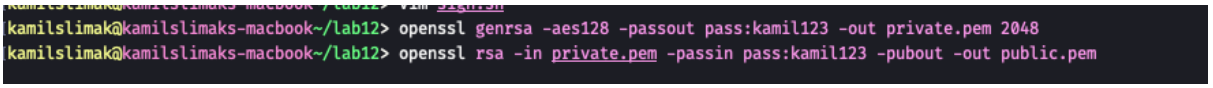


skrypt aes.sh:



zad 3

tworzenie kluczy prywatnego i publicznego



sign.sh:

```
#!/bin/bash


filename=$1
privatekey=$2

if [[ $# -lt 2 ]] ; then
  echo "Usage: sign <file> <private_key>"
  exit 1
fi

openssl dgst -sha256 -sign $privatekey -out /tmp/$filename.sha256 $filename
openssl base64 -in /tmp/$filename.sha256 -out signature.sha256
rm /tmp/$filename.sha256
~
~
~
```

użycie:

```
kamilslimak@kamilslimaks-macbook~/lab12> ./sign.sh example_file.txt private.pem
Enter pass phrase for private.pem:
kamilslimak@kamilslimaks-macbook~/lab12>
```