Sprawozdanie

LABORATORIUM 4. KRYPTOGRAFIA SYMETRYCZNA, TRYBY PRACY ALGORYTMÓW KRYPTOGRAFICZNYCH.

Zadanie 4.6

D.4.3

Skrypt szyfrujący

```
root@Kubuntu:/home/student/Documents/lab4b# bash sapp tekst.txt
hex string is too short, padding with zero bytes to length
root@Kubuntu:/home/student/Documents/lab4b# cat sapp
#!/bin/bash

klucz=$(head -c 16 /dev/urandom | hexdump -e '4/4 "%08X" 1 "\n"')

echo $klucz > klucz.txt

for plik in "$@"
do
    openssl enc -aes-256-cbc -e -in $plik -out zaszyfrowany_$plik -K $klucz -iv $klucz
done
```

#!/bin/bash

klucz=$(head -c 16 /dev/urandom | hexdump -e '4/4 "%08X" 1 "\n"')

echo $klucz > klucz.txt

for plik in "$@"

do

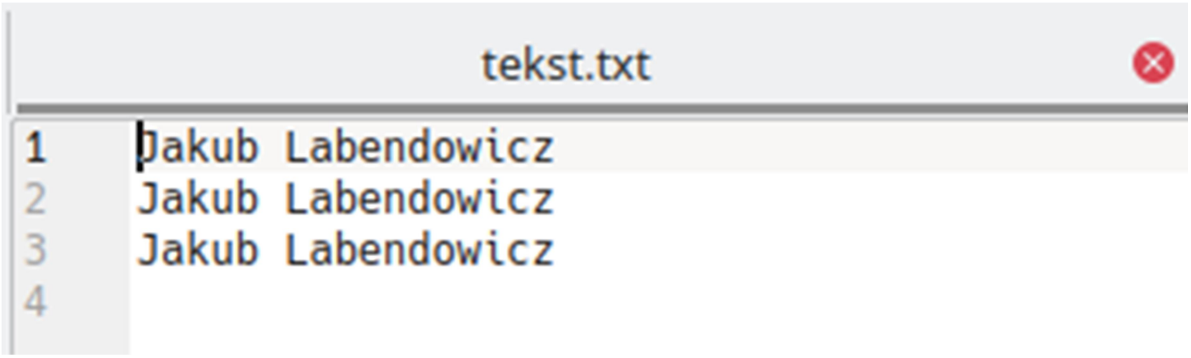
openssl enc -aes-256-cbc -e -in $plik -out zaszyfrowany_$plik -K $klucz -iv $klucz

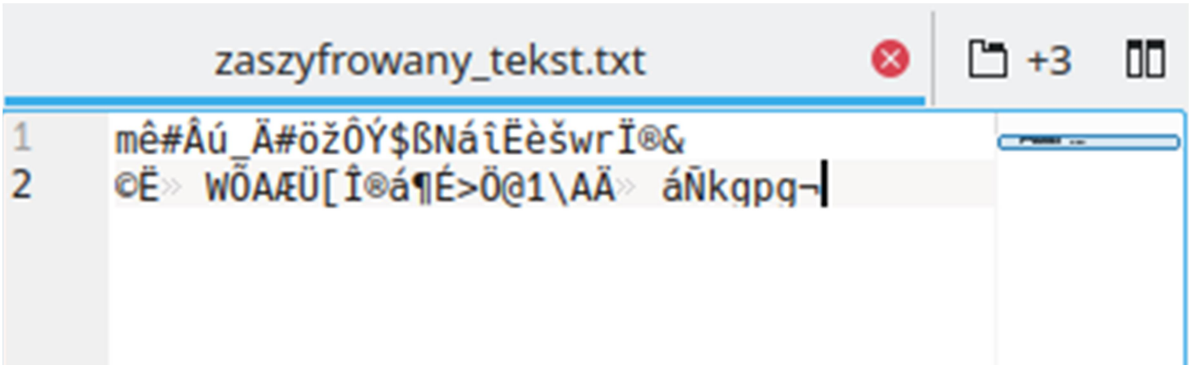
done

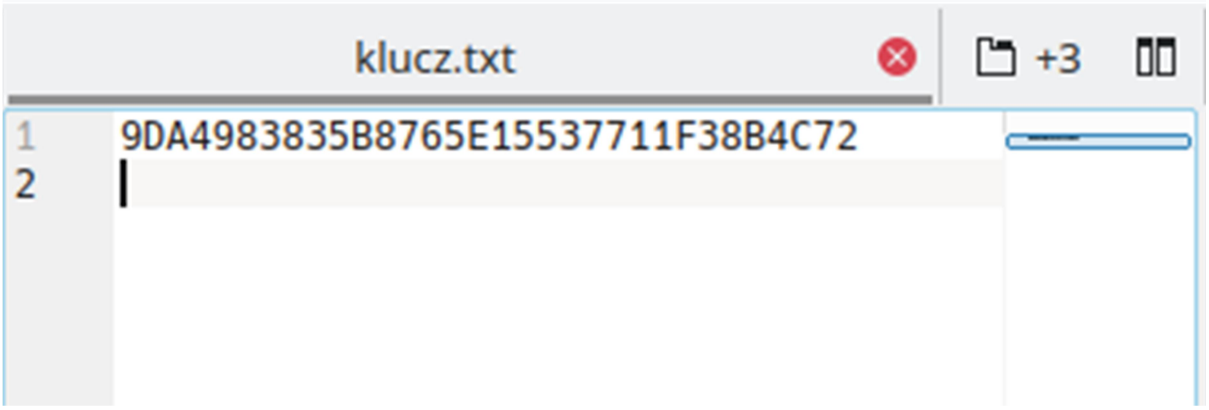
Użycie: bash sapp [plik]

Skrypt jest napisany w bash'u.

Skrypt zapisuje do zmiennej „klucz" 16 bajtowy klucz kryptograficzny na podstawie pobranych danych pseudolosowych z urządzenia /dev/random, następnie klucz zapisywany jest do pliku. Dla każdego podanego jako argument pliku następuje szyfrowanie szyfrem aes-256-cbc na podstawie klucza.


tekst.txt
1 Jakub Labendowicz
2 Jakub Labendowicz
3 Jakub Labendowicz
4


zaszyfrowany_tekst.txt
+3
1 mê#Âú_Ä#öžÔÝ$ßNáîËèšwrÏ®&
2 ©Ë» WÕAÆÜ[Î®á¶É>Ö@1\AÄ» áÑkgpg¬


klucz.txt
+3
1 9DA4983835B8765E15537711F38B4C72
2

Skrypt deszyfrujący

```
root@Kubuntu:/home/student/Documents/lab4b# bash dapp zaszyfrowany_tekst.txt
hex string is too short, padding with zero bytes to length
root@Kubuntu:/home/student/Documents/lab4b# cat dapp
#!/bin/bash

klucz=$(cat klucz.txt)

for plik in "$@"
do
    openssl enc -aes-256-cbc -d -in $plik -out odszyfrowany_$plik -K $klucz -iv $klucz
done
```

#!/bin/bash

klucz=$(cat klucz.txt)

for plik in "$@"

do

openssl enc -aes-256-cbc -d -in $plik -out odszyfrowany_$plik -K $klucz -iv $klucz

done

Użycie: bash dapp [plik]

Skrypt jest napisany w bash'u.

Skrypt zapisuje do zmiennej „klucz" 16 bajtowy klucz kryptograficzny pobrany z pliku „klucz.txt". Dla każdego podanego jako argument pliku następuje odszyfrowywanie szyfrem aes-256-cbc na podstawie klucza.