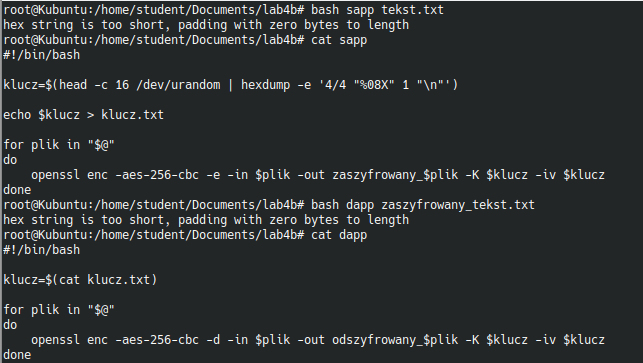
Sprawozdanie

LABORATORIUM 4. KRYPTOGRAFIA SYMETRYCZNA, TRYBY PRACY ALGORYTMÓW KRYPTOGRAFICZNYCH.

# Zadanie 4.6

## D.4.3

### Skrypt szyfrujący



#!/bin/bash

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

echo $klucz > klucz.txt

for plik in "$@"

do

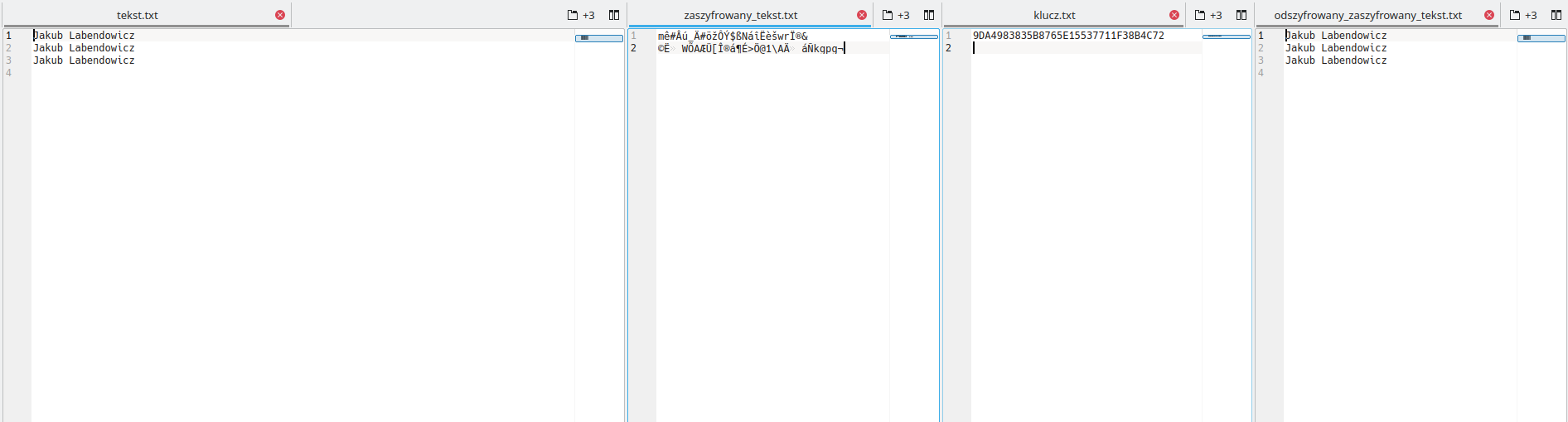
openssl enc -aes-256-cbc -e -in $plik -out zaszyfrowany\_$plik -K $klucz -iv $klucz

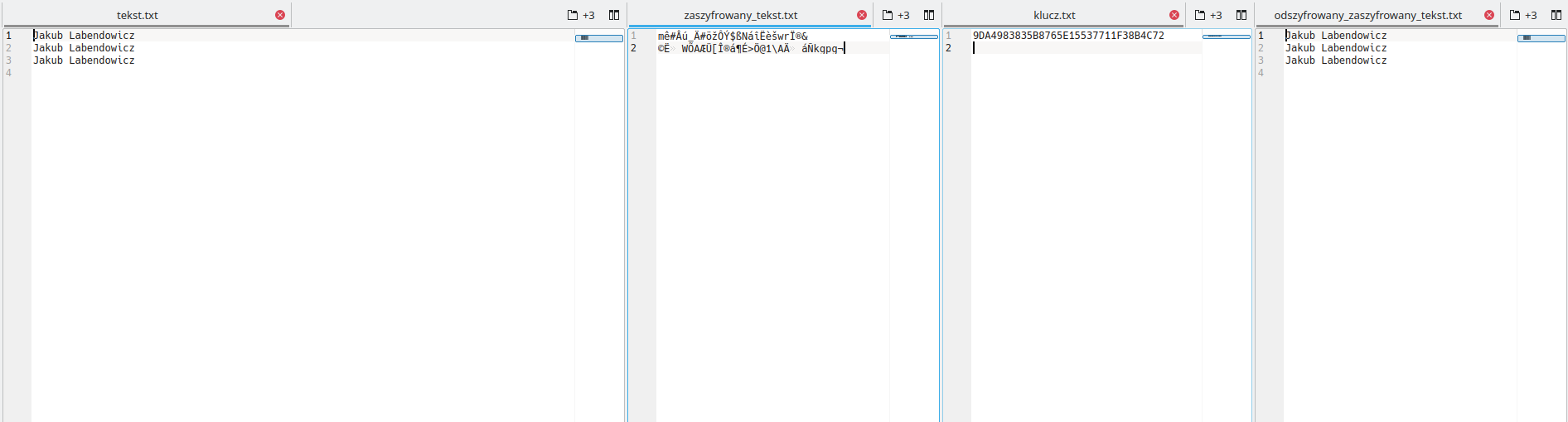
done

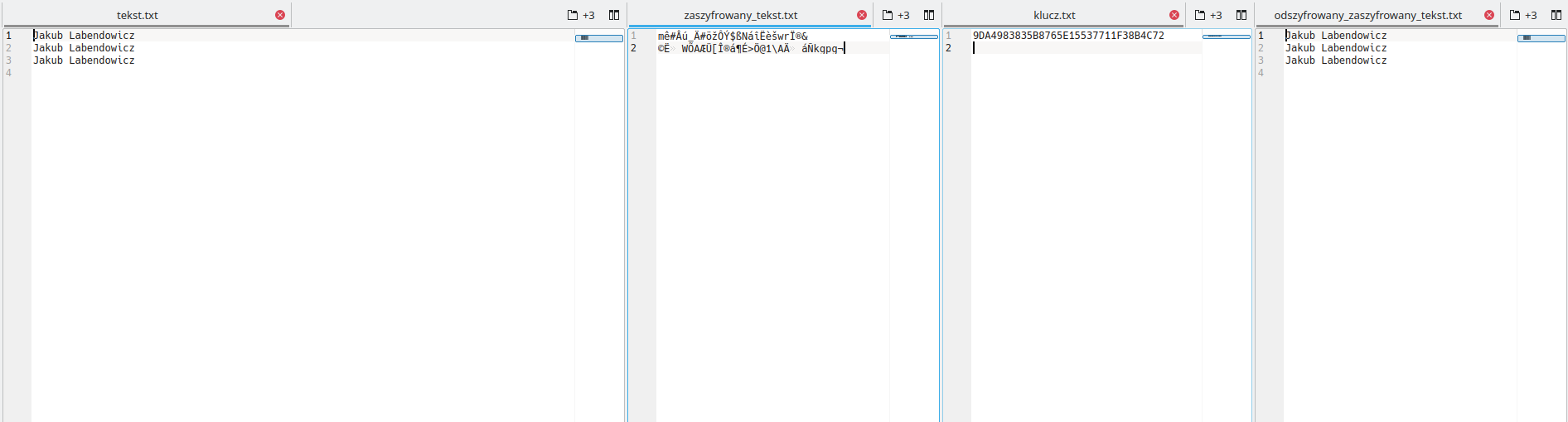
Użycie: bash sapp [plik]

Skrypt jest napisany w bash’u.

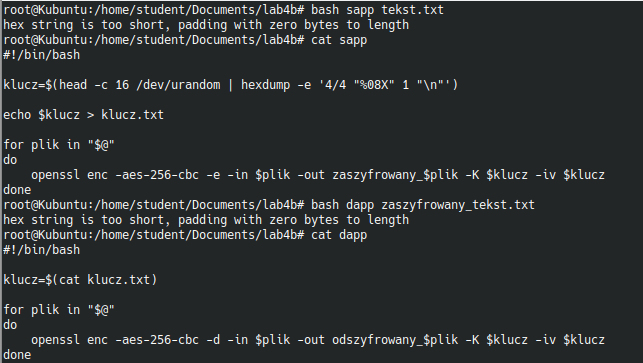
Skrypt zapisuje do zmiennej „klucz” 16 bajtowy klucz kryptograficzny na podstawie pobranych danych pseudolosowych z urządzenia /dev/random, następnie klucz zapisywany jest do pliku. Dla każdego podanego jako argument pliku następuje szyfrowanie szyfrem aes-256-cbc na podstawie klucza.







### Skrypt deszyfrujący



#!/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.

