

Znajdują się tutaj dwa programy. Jeden (first) służy do stworzenia skrótu z hasła. Tak otrzymany skrót wykorzystujemy do złamania metodą słownikową, stosując drugi program (second).

Prezentacja:

W pierwszej kolejności wybieramy z pliku 'xyz.txt' hasło, jakie nas interesuje, na którym chcemy sprawdzić, czy program je 'złamie' lub obliczyć czasy ile wątków poradzi sobie w jakim czasie.

Po nazwie uruchamianego programu wpisujemy 'hasło' i domieszkę (salt). Domieszka musi być 5MfvmFOaDU, inaczej w drugim programie będzie trzeba ją zmienić, gdyż jest statyczna.

```
aaa@aaa-VirtualBox: ~/Pulpit/So2 moje programy z zajec/8-9
aaa@aaa-VirtualBox:~/Pulpit/So2 moje programy z zajec/8-9$ ./first 'Agnieszka1953' 5MfvmFOaDU
$6$5MfvmFOaDU$Wzlw1ABzHs3ofhdk.LvYh35pj0Kq/ueaaLq80AaX73zLNQWr22efkg2YxJFzzxKq/G7r4.F.p3In/tctk
UF01
aaa@aaa-VirtualBox:~/Pulpit/So2 moje programy z zajec/8-9$
```

Otrzymany hash jest nam potrzebny w drugim programie. Kopiujemy całość i wklejamy w program second.

```
aaa@aaa-VirtualBox: ~/Pulpit/So2 moje programy z zajec/8-9
aaa@aaa-VirtualBox:~/Pulpit/So2 moje programy z zajec/8-9$ ./first 'Agnieszka1953' 5MfvmFOaDU
$6$5MfvmFOaDU$Wzlw1ABzHs3ofhdk.LvYh35pj0Kq/ueaaLq80AaX73zLNQWr22efkg2YxJFzzxKq/G7r4.F.p3In/tctk
UF01
aaa@aaa-VirtualBox:~/Pulpit/So2 moje programy z zajec/8-9$

aaa@aaa-VirtualBox:~/Pulpit/So2 moje programy z zajec/8-9$ ./second '$6$5MfvmFOaDU$Wzlw1ABzHs3of
hdk.LvYh35pj0Kq/ueaaLq80AaX73zLNQWr22efkg2YxJFzzxKq/G7r4.F.p3In/tctkUF01' ../xyz.txt 8
```

Oprócz hashu należy jeszcze podać lokalizację słownika haseł oraz liczbę wątków, na których chcemy operować. Podany przykład jest dla 8 wątków wykonywanych równolegle, stąd ich nierówny start.

```
aaa@aaa-VirtualBox: ~/Pulpit/So2 moje programy z zajec/8-9
Proces 0 : utworzony
Proces 1 : utworzony
Proces 2 : utworzony
Proces 4 : utworzony
Proces 3 : utworzony
Proces 6 : utworzony
Proces 7 : utworzony
Proces 5 : utworzony
```

```
aaa@aaa-VirtualBox: ~/Pulpit/So2 moje programy z zajec/8-9
$6$5MfvmFOaDU$Wzlw1ABzHs3ofhdk.LvYh35pj0Kq/ueaalLq80AaX73zlnQWr22efkg2YxJFzzxKq/G7r4.F.p3In/tctkUF01
Rozpoczynam skanowanie...
Postep: 2%
```

Hash, który wyświetla się na początku, posłużył mi tylko do sprawdzenia działania. Widzimy, że poszukiwanie trwa i jest komunikowane poprzez procentowe przeszukiwanie całego pliku. 100% to albo sukces, gdyż w jakimś momencie hasło się znalazło (zostało złamane) lub porażka po przejrzeniu całego słownika.

```
aaa@aaa-VirtualBox: ~/Pulpit/So2 moje programy z zajec/8-9
Skanowanie ukonczone!
Postep: 100%
Poszukiwane haslo to: Agnieszka1953
aaa@aaa-VirtualBox:~/Pulpit/So2 moje programy z zajec/8-9$ ./second '$6$5MfvmFOaDU$Wzlw1ABzHs3ofhdk.LvYh35pj0Kq/ueaalLq80AaX73zlnQWr22efkg2YxJFzzxKq/G7r4.F.p3In/tctkUF01' ../xyz.txt
```

Hasło zostało złamane! W drugiej kolejności sprawdzimy, ile trwa poszukiwanie na ilu wątkach.

```
aaa@aaa-VirtualBox: ~/Pulpit/So2 moje programy z zajec/8-9
Skanowanie ukonczone!
Postep: 100%
Poszukiwane haslo to: Agnieszka1953
aaa@aaa-VirtualBox:~/Pulpit/So2 moje programy z zajec/8-9$ ./second '$6$5MfvmFOaDU$Wzlw1ABzHs3ofhdk.LvYh35pj0Kq/ueaalLq80AaX73zlnQWr22efkg2YxJFzzxKq/G7r4.F.p3In/tctkUF01' ../xyz.txt
Sprawdzanie optymalej liczby watkow
Ilosc watkow: 1
Czasy:
```

Tak prezentuje się całe zestawienie:

aaa@aaa-VirtualBox: ~/Pulpit/So2 moje programy z zajec/8-9

Sprawdzanie optymalnej liczby watkow

Ilosc watkow: 1

Czasy:

26.669

Calkowity czas trwania: 26.710

Ilosc watkow: 2

Czasy:

16.489

16.521

Calkowity czas trwania: 16.525

Ilosc watkow: 3

Czasy:

10.885

10.937

10.987

Calkowity czas trwania: 10.998

Ilosc watkow: 4

Czasy:

8.681

8.704

8.803

8.862

Calkowity czas trwania: 8.864

Ilosc watkow: 5

Czasy:

8.197

8.297

8.402

8.519

8.843

Calkowity czas trwania: 8.855

Ilosc watkow: 6

Czasy:

8.127

8.279

8.453

8.377

8.409

8.500

Calkowity czas trwania: 8.502

Ilosc watkow: 7

Czasy:

8.123