Leszifr3

(JPW 2018)

Użycie

(WINDOWS)

Leszifr3 pozwala na zaszyfrowanie pliku do archiwizacji, deszyfrowanie pliku,

oraz odczyt załączonych meta danych (dodatkowy opis pliku).

Dodatkowy opis pliku jest również zaszyfrowany.

Leszifr3 domyślnie używa kodowania utf-8 dla polskich znaków diakrytycznych.   
 W przypadku WINDOWS następuje automatyczne rekodowanie z utf-8 na   
 cp1250.

----------------------------------------------------------------------------

**Użycie z poziomu wiersza poleceń**

----------------------------------------------------------------------------

Szyfrowanie:

**leszifr3 [-c] [nazwa pliku do szyfrowania] [hasło]**

(wszystkie argumenty są wymagane)

**leszifr3 [-cg] [nazwa pliku do szyfrowania] [hasło]**

(jak wyżej oraz włącza windows progress bar)

Plik zaszyfrowany będzie miał ta sama nazwę z sufiksem ".archi"

np.: pic.jpeg po zaszyfrowaniu będzie miał nazwę: pic.jpeg.archi

Plik pic.jpeg nie zostanie usunięty po zaszyfrowaniu.

Uwaga! Nazwa pliku szyfrowanego będzie miała zastąpione   
 polskie znaki diakrytyczne ich odpowiednikami w ASCII oraz  
 zostaną zastąpione podkreślnikiem "\_" wszystkie inne znaki  
 poza "-" (minus) oraz "." (kropka). Na przykład nazwa pliku   
 szyfrowanego:

"moje zdjęcie z wakacji [2016].jpg"

dla pliku po szyfrowaniu będzie następująca:   
 "moje\_zdjecie\_z\_wakacji \_\_2016\_.jpg.archi"

Pierwotna nazwa pliku po rozszyfrowaniu zostanie przywrócona.

Oryginalny plik, który będzie szyfrowany leszifr3 nie będzie skasowany.

---------------------------------------------------------------------------

**Odszyfrowanie całego pliku**

**leszifr3 [-d] [nazwa pliku zaszyfrowanego] [hasło]**

(wszystkie argumenty są wymagane)

**leszifr3 [-dg] [nazwa pliku zaszyfrowanego] [hasło]**

(jak wyżej oraz włącza windows progress bar)

Jeśli istnieje w katalogu juz istnieje plik np. pic.jpeg to podczas

odszyfrowania pliku pic.jpeg.archi plik pic.jpeg zostanie nadpisany

lub jeśli był błąd to zostanie skasowany.

Uwaga! Zostanie przywrócona pierwotna nazwa pliku przed  
 szyfrowaniem.   
 Zaszyfrowany plik nie będzie skasowany po odszyfrowaniu.

---------------------------------------------------------------------------

**Odczyt meta danych (dołączonych do pliku szyfrowanego przez użytkownika)**

**leszifr3 [-m] [nazwa pliku zaszyfrowanego] [hasło]**

(wszystkie argumenty są wymagane)

W przypadku braku opisu (nie był dodany przez użytkownika),

pojawi sie informacja: "no added file description"

Uwaga! Plik dodawany jako wbudowana metryczka (abstrakt) nie  
 może przekroczyć 3000 bajtów. Polskie znaki diakrytyczne w szyfrowanej  
 wbudowanej metryczce są kodowane domyślnie w utf-8.   
 Leszifr3 automatycznie będzie je rekodować do typowo używanego   
 w Windows cp1250. Odczytując zawartość metryczki np. w Linux  
 nie trzeba rekodować z cp1250 do utf-8.

----------------------------------------------------------------------------

**Odczyt wersji leszifr**

**leszifr3 [-v]**

----------------------------------------------------------------------------

**Odczyt wersji generatora PRANDOM**

**leszifr3 [-vg]**

----------------------------------------------------------------------------

**Help**

**leszifr [-h]**

(argument może być dowolny rożny od: [-m],[-d],[-c],[-v],[-vg])

-----------------------------------------------------------------------------

**Dodawanie meta danych - metryczka pliku (dodatkowy opis tekstowy)**

-----------------------------------------------------------------------------

W dowolnym, ulubionym edytorze tekstowym należy przygotować opis,

którego długość nie powinna przekroczyć 3000 bajtów ponieważ leszifr3

automatycznie obetnie dłuższe opisy do 3000 bajtów. Długość podawana   
 jest w bajtach ze względu na kodowanie utf-8 polskich znaków diakrytycznych.  
 W przeciwieństwie do typowego w Windows jednobajtowego kodowania cp1250,

kodowanie polskich znaków diakrytycznych w utf-8 jest dwubajtowe.

Plik metryczki jest plikiem tekstowym i jeśli format będzie złożony np. docx  
 tekst może nie być zrozumiały po wyświetleniu. Dlatego nie należy   
 używać w metryczce innych formatów tekstowych niż prosty format ".txt".

Plik należy zachować pod nazwa pliku wyjściowego z rozszerzeniem ".met"

i zapisać w katalogu gdzie znajduje sie plik do szyfrowania. Leszifr3 rozpozna  
 i skojarzy nazwę z rozszerzeniem ".met" i dołączy jego zawartość do   
 do pliku zaszyfrowanego. Metryczka tekstowa również jest zaszyfrowana   
 i nie może być odczytana w żadnym standardowym edytorze poza leszifr3.

Np.: opis pliku: pic.jpeg musi być zapisany pod nazwa: pic.jpeg.met

Metryczka (plik tekstowy) nie będzie usunięty po dodaniu do pliku

szyfrowanego.

Nie jest dodawana żadna automatyczna informacja do metryczki.

----------------------------------------------------------------------------

----------------------------------------------------------------------------

**Błędy zawarte w pliku szyfrowanym**

----------------------------------------------------------------------------

W trakcie szyfrowania w pliku szyfrowanym są umieszczone informacje

haszowania kontrolującego szyfrowane bloki danych. Po rozszyfrowaniu bloki

danych ponownie są poddawane haszowaniu i sprawdzana jest zgodność z haszami

bloków przed szyfrowaniem. Występujące niezgodności sa zapisywane do pliku

o tej samej nazwie co plik po rozszyfrowaniu z rozszerzeniem ".err".

Plik jest plikiem tekstowym i zawiera numery błędnych bloków danych.

----------------------------------------------------------------------------

----------------------------------------------------------------------------

**Bledy w działaniu aplikacji leszifr3**

----------------------------------------------------------------------------

Jeśli wystąpi błąd, to zostanie on zgłoszony przez leszifr3.

----------------------------------------------------------------------------