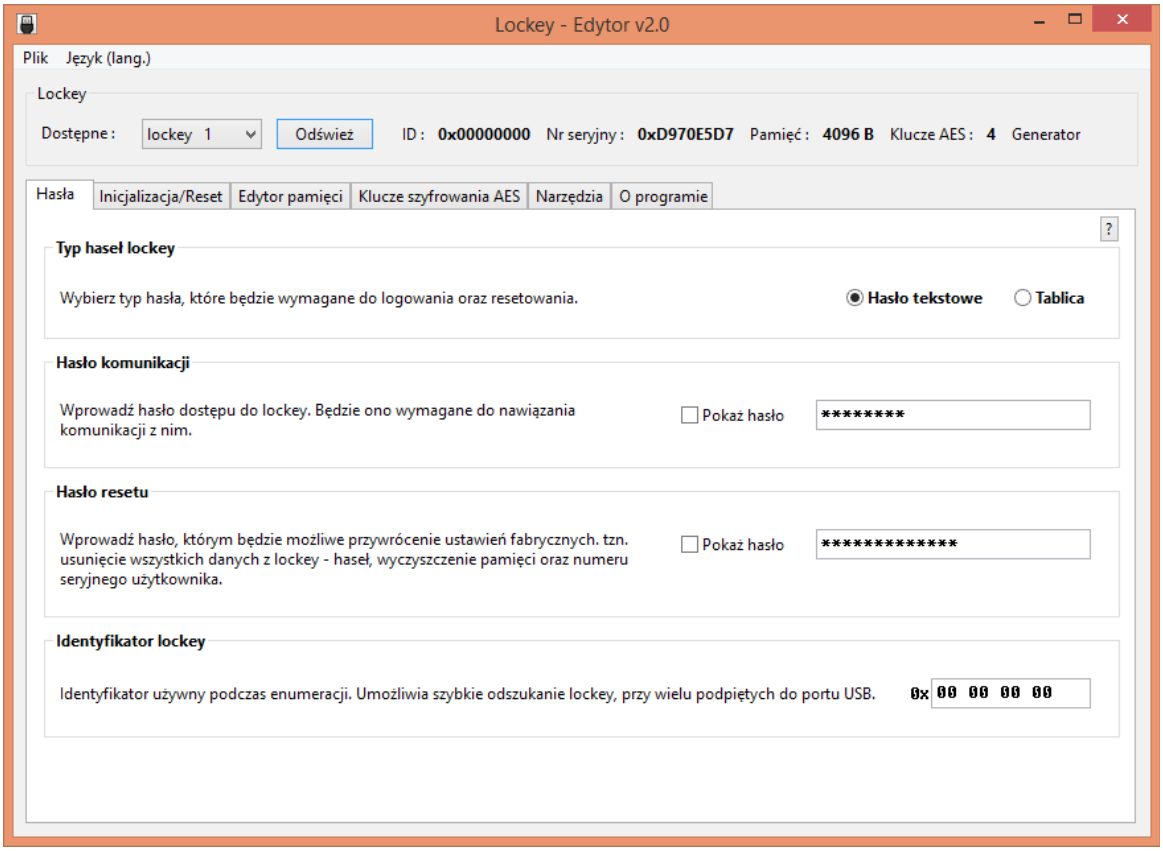
Sprzętowe zabezpieczenie oprogramowania

edytor

Data dokumentu 3.07.2020

Spis treści

O edytorze



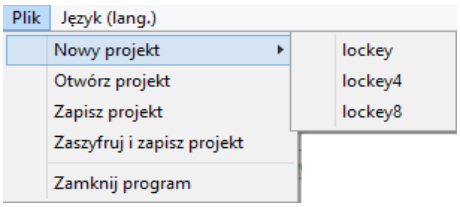
Edytor przeznaczony jest do ułatwienia konfiguracji **lockey.** Przy jego pomocy możliwe jest przeprowadzenie czynności :

- inicjalizacja nowych **lockey-ów**
- przywrócenie ustawień fabrycznych dla **lockey-ów** zainicjalizowanych wcześniej
- odczyt i zapis pamięci
- zapis kluczy szyfrowania AES
- test i sprawdzenie wyniku sprzętowego szyfrowania wybranym kluczem AES
- sprzętowe generowanie bloków liczb pseudolosowych
- zapis i odczyt czasu zegara RTC (opcja dostępna w lockey i2c)

Edytor umożliwia stworzenie i zapisanie do pliku projektu haseł użytych podczas inicjalizacji oraz pozostałych danych, takich jak obraz pamięci czy klucze szyfrowania AES.
Umożliwia seryjne przygotowanie wielu **lockey-ów,** które mają być wykorzystywane do zabezpieczania aplikacji.

Menu programu

Menu zostało podzielone na części:



Opcje odczytu i zapisu pliku projektu.

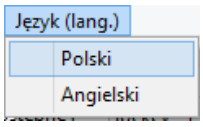
Nowy projekt Tworzy nowy projekt dla wybranego typu **lockey-a**.

Otwórz projekt Otwiera istniejący plik projektu.

Jeżeli projekt jest chroniony hasłem, program poprosi o jego wprowadzenie.

Zapisz projekt Zapisuje do pliku projektu edytowane dane takie jak hasła inicjalizacji/resetu, obraz pamięci, klucze szyfrowania AES.

Zaszyfruj i zapisz projekt Opcja analogiczna do ***Zapisz projekt*** jednak przed zapisem wymaga wprowadzenia hasła. Używana jest do zaszyfrowania pliku projektu, aby nie został otwarty przez osoby do tego nieupoważnione.



Wybór języka.

Praca z programem

Po uruchomieniu programu z głównego menu **Plik** należy wybrać :

- **Nowy projekt** – aby utworzyć nowy projekt dla wybranego typu **lockey-a**

  lub

- **Otwórz projekt** – aby odczytać utworzony wcześniej plik projektu

Po dokonaniu wyboru zostaną wyświetlone zakładki programu segregujące tematycznie dostępne opcje i ustawienia.

Lista dostępnych kluczy lockey

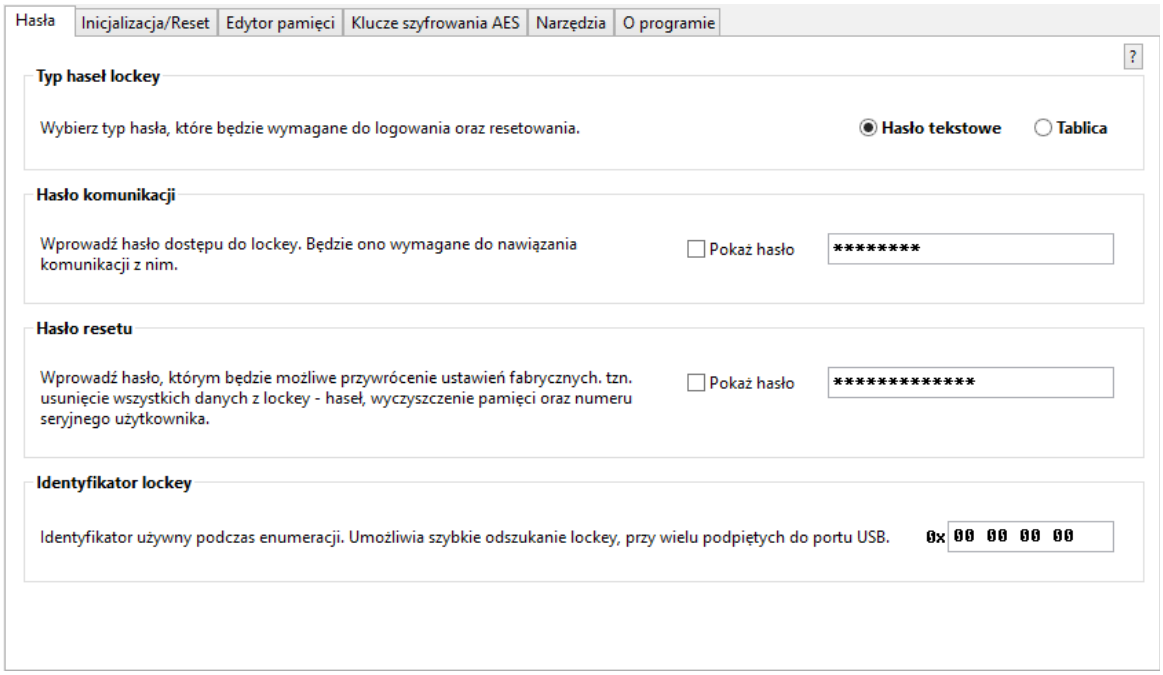
Lista **lockey-ów**, podpiętych do portów komputera jest dostępna w części okna **Lockey** :

Wyboru **lockey-a,** z którym edytor ma w danej chwili współpracować dokonuje się poprzez otwarcie rozwijanej listy **Dostępne** i wybranie jednej z pozycji.

W przypadku jeżeli lista jest pusta, należy sprawdzić czy do komputera został podłączony **lockey** i nacisnąć przycisk **Odśwież**.

Po wybraniu pozycji zostaje automatycznie wyświetlony numer identyfikacji oraz seryjny produktu, rozmiar pamięci, liczba dostępnych kluczy szyfrowania oraz informacja o tym czy **lockey** posiada generator liczb pseudolosowych lub RTC.

Zakładka – Hasła



Lockey zakupiony u producenta, przed pierwszym użyciem wymaga wstępnej inicjalizacji tzn. ustalenia haseł komunikacji, resetu oraz opcjonalnie nadania numeru identyfikacji.
W tej zakładce należy wybrać typ haseł oraz wypełnić wymagane pola.

UWAGA

lockey *dla którego po dokonaniu inicjalizacji nie są znane hasła komunikacji(logowania) i resetu staje się* ***bezużyteczny****.*

Nigdy nie należy doprowadzić do takiej sytuacji dlatego BARDZO WAŻNE ! :

Po utworzeniu nowego projektu i wprowadzeniu haseł lub ich modyfikacji, zalecany jest ich bezzwłoczny zapis do pliku projektu ***Plik/Zapisz projekt****.*

Typy haseł lockey

Metoda **Login** (*patrz opis w dokumentacji programisty i API - „lockeyapi_pl.pdf”*), zestawiając komunikację z **lockey-em** korzysta z hasła komunikacji. Hasło to może być metodzie przekazywane w jednej z postaci :

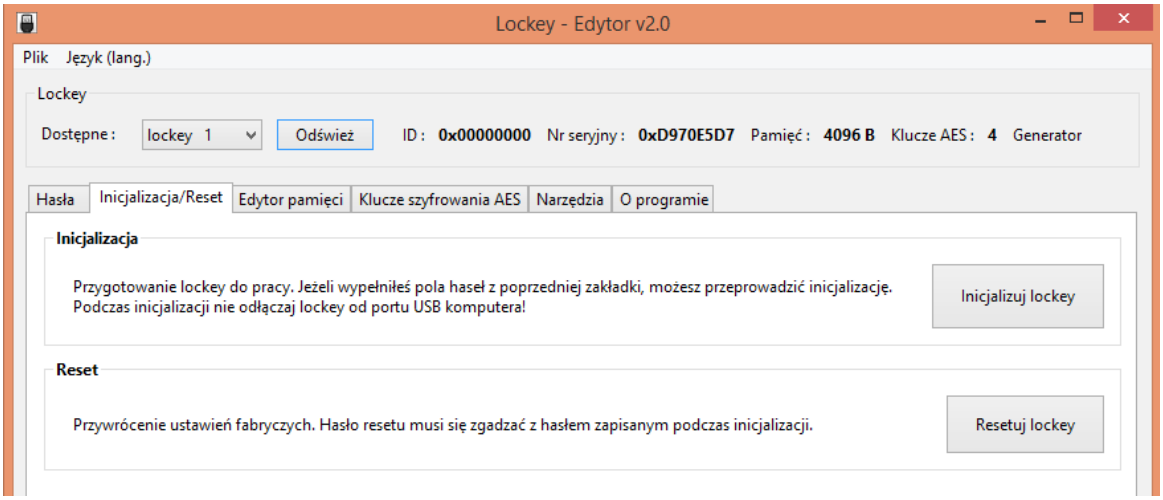
- tekstu
  lub
- tablicy 32 bajtowej

Analogiczna sytuacja odnosi się w stosunku do metody **Reset**.
Na etapie tworzenia nowego projektu, należy zdecydować jakiego typu hasła będą używane z kodu zabezpieczanego programu do nawiązywania komunikacji z **lockey-em**.

Identyfikator lockey

Jeżeli podczas enumeracji (*patrz opis **ClockeyEnum** w dokumentacji programisty i API - „lockeyapi_pl.pdf”*), mają być brane pod uwagę tylko klucze z konkretnym identyfikatorem, w tym miejscu należy go wprowadzić.

Inicjalizacja/Reset



Opis przycisków :

Inicjalizuj lockey

Zapisuje w **lockey-u** ustawione na poprzedniej zakładce :

- hasło (klucz) wymagane do komunikacji
- hasło (klucz) przywracające ustawienia fabryczne
- opcjonalnie – identyfikator dla **lockey-a.** Jeżeli nie został wprowadzony będzie nim wartość 0.

Uwaga!

Inicjalizację można przeprowadzić tylko w dwóch przypadkach :

- na niezainicjalizowanym **lockey-u**, czyli w takim stanie, w jakim znajduje się po dostarczeniu od producenta
- jeśli dokonano przywrócenia ustawień fabrycznych poprzez **Reset**.

Resetuj lockey

Przywraca ustawienia fabryczne, usuwając z **lockey-a** :

- hasła komunikacji i resetu
- dane z pamięci
- klucze szyfrowania
- identyfikator

Wymaga podania prawidłowego hasła resetu z którym była przeprowadzona wcześniejsza inicjalizacja **lockey-a**.

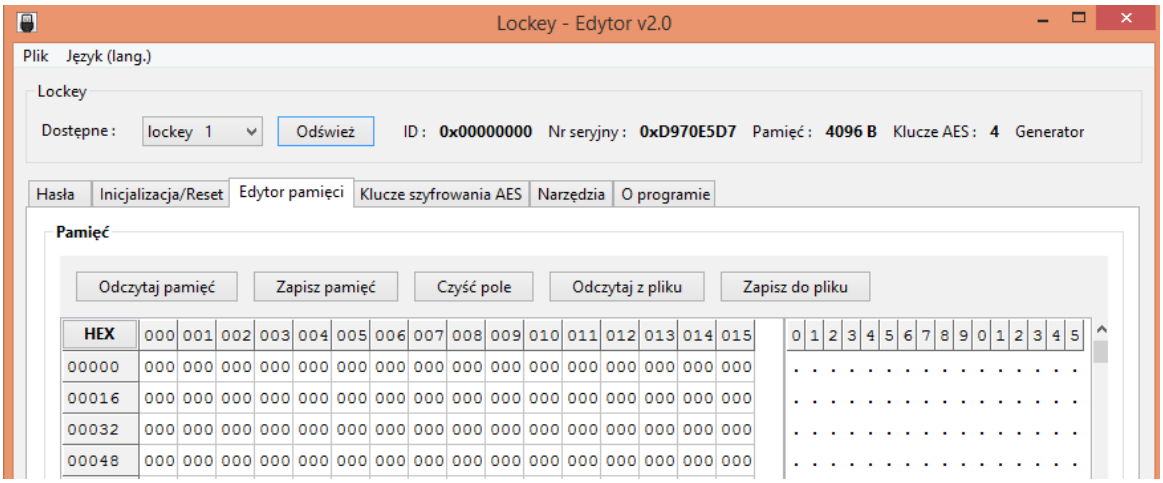
UWAGA

*Pamiętaj, nieznajomość haseł po inicjalizacji **lockey** jest równoznaczna z :*

- *całkowitym brakiem dostępu do **lockey-a***
- *brakiem możliwości przywrócenia ustawień fabrycznych **lockey-a***

*Ze względu na długość tablic haseł i siłę użytego w **lockey** algorytmu AES, nie bierze się pod uwagę sytuacji złamania haseł znanymi metodami w rozsądnym czasie.*

Edytor pamięci



Zakładka z opcjami przeznaczonymi do edycji, odczytu i zapisu komórek pamięci **lockey-a**.

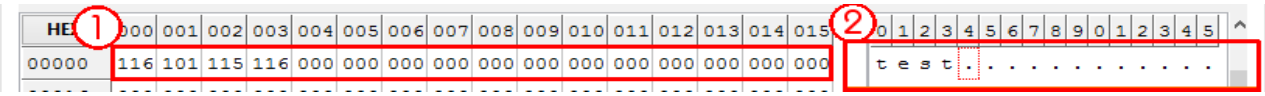
Jako jednostkę pojedynczej komórki pamięci **lockey-a** przyjęto bajt. Każdy bajt pamięci posiada swój adres. W celu ułatwienia adresowania pamięci w edytorze, podzielono ją na bloki po 16 bajtów.

Opis ustawień i przycisków :

Odczytaj pamięć	Odczytuje pamięć z klucza **lockey,** wybranego na rozwijanej liście **Dostępne.**
Zapisz pamięć	Zapisuje całą edytowaną pamięć do **lockey,** wybranego na rozwijanej liście **Dostępne.**
Czyść pole	Zeruje wartości komórek pamięci w całym polu edycyjnym.
Odczytaj z pliku	Odczytuje wskazany plik a jego wartości binarne wstawia do pola edycyjnego. Jeżeli plik ma rozmiar większy niż pole edycyjne, zostanie odczytana z niego maksymalna ilość danych możliwa do wyświetlenia w polu.
Zapisz do pliku	Zapisuje do wybranego pliku obraz edytowanej pamięci.
HEX/DEC	Przełącza system wyświetlania liczb w polu edycyjnym - szesnastkowy/dziesiętny

Edycja pamięci

Każdą komórkę można modyfikować wpisując pod adres wybraną wartość liczbową (1) lub wpisując znak lub tekst w polu (2) :



Po zakończeniu edycji obrazu pamięci możliwe jest jego zapisanie do **lockey-a** (przycisk **Zapisz pamięć**).

UWAGA

*Zapisu można dokonać tylko na zainicjalizowanym **lockey-u**.*

Przykład wykorzystania pamięci

Pamięć **lockey-a** można wykorzystać w zabezpieczanej aplikacji odczytując jej fragmenty i analizując dane. Na ich podstawie możliwe jest tworzenie dowolnych mechanizmów ograniczonych tylko wyobraźnią programisty, np. licencjonowania:

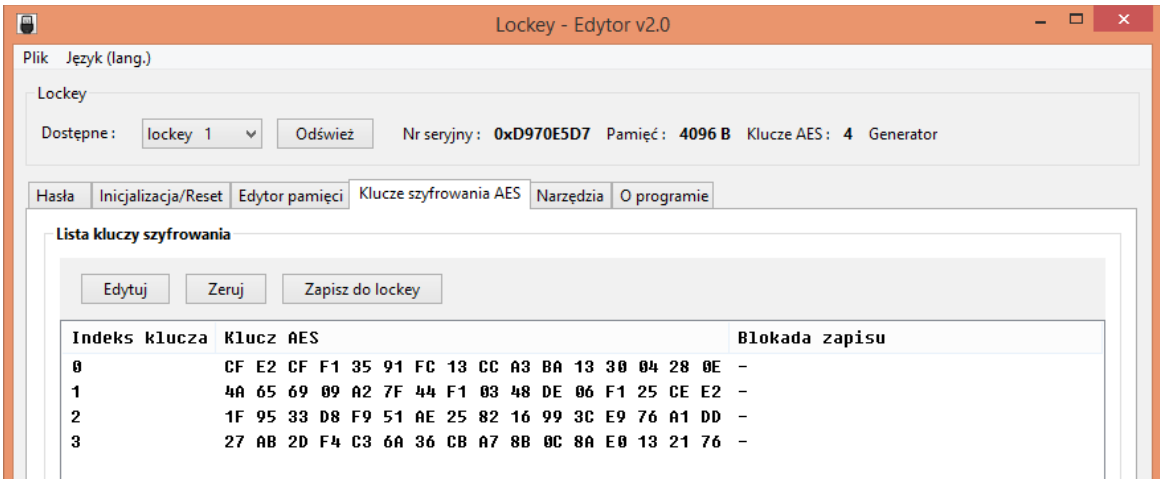
- na liczbę uruchomień aplikacji
- określony w minutach czas działania aplikacji
- tworzenie zezwoleń dla np. drukowania z aplikacji, zapisu plików projektu, dostępu do innych zasobów

Wcześniej jednak należy przemyśleć jakie informacje powinny znaleźć się w jej wnętrzu i w jakich jej obszarach.

Do odczytu pamięci z poziomu kodu zabezpieczanego programu należy użyć metody **ReadByte** lub **ReadMemo**. (*patrz opis **ReadByte/ReadMemo** w dokumentacji programisty i API - „lockeyapi_pl.pdf”*)

Klucze szyfrowania AES

Rozdział dotyczy kluczy **lockey4/lockey8/lockeyi2c** w których zostało zaimplementowane sprzętowe szyfrowanie.



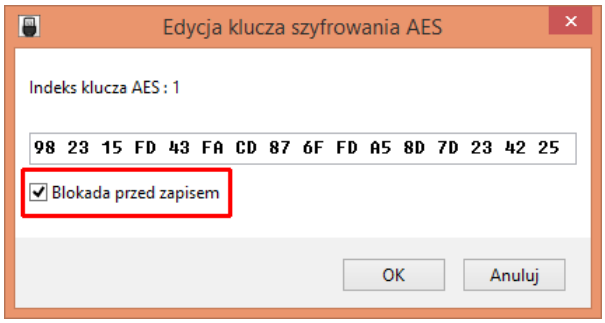
Zakładka przeznaczona do utworzenia i zapisania w **lockey-u,** kluczy szyfrowania AES.
Ze względów bezpieczeństwa, **lockey** nie posiada mechanizmu odczytu przechowywanych kluczy szyfrowania. Przy ich użyciu możliwe są jedynie operacje szyfrowania/deszyfrowania danych wewnątrz **lockey-a**.

Opis przycisków :

Edytuj	Otwiera okno z możliwością edycji klucza szyfrowania wybranego na liście kluczy.
	UWAGA *Nie edytuje klucza bezpośrednio w **lockey-u**, tylko w obrębie listy.*
Zeruj	Zeruje wybrany na liście klucz szyfrowania.
	UWAGA *Nie zeruje klucza bezpośrednio w **lockey-u**, tylko w obrębie listy.*
Zapisz do lockey	Zapisuje do **lockey** klucze szyfrowania utworzone na liście.

Edycja kluczy szyfrowania

Należy zaznaczyć na liście klucz szyfrowania o wybranym indeksie i nacisnąć przycisk **Edytuj**.
Jeżeli podczas edycji klucza szyfrowania, zostanie zaznaczona opcja **Blokada przed zapisem**, to po dokonaniu zapisu do **lockey-a**, nie będzie możliwości zmiany klucza szyfrowania o indeksie z ustawioną blokadą.



UWAGA

Blokada przed zapisem klucza może zostać zdjęta w **lockey-u** *tylko poprzez przywrócenie ustawień fabrycznych czyli procedurę resetu.*

Zapis kluczy szyfrowania

Po naciśnięciu przycisku **Zapisz do lockey**, klucze zostaną zapisane zgodnie z indeksem widocznym na liście.
Jeżeli do **lockey-a,** były już zapisywane klucze szyfrowania z ustawioną ochroną przed zapisem nie będzie możliwości ich nadpisania.

Przykład wykorzystania kluczy szyfrowania

Użycie kluczy szyfrowania z poziomu zabezpieczanego kodu programu polega na skorzystaniu z metod **Encrypt** lub **Decrypt**, którym należy przekazać tylko indeks klucza i blok danych do zaszyfrowania lub odszyfrowania (*patrz opis* ***Encrypt/Decrypt*** *w dokumentacji programisty i API - „lockeyapi.pdf”*).

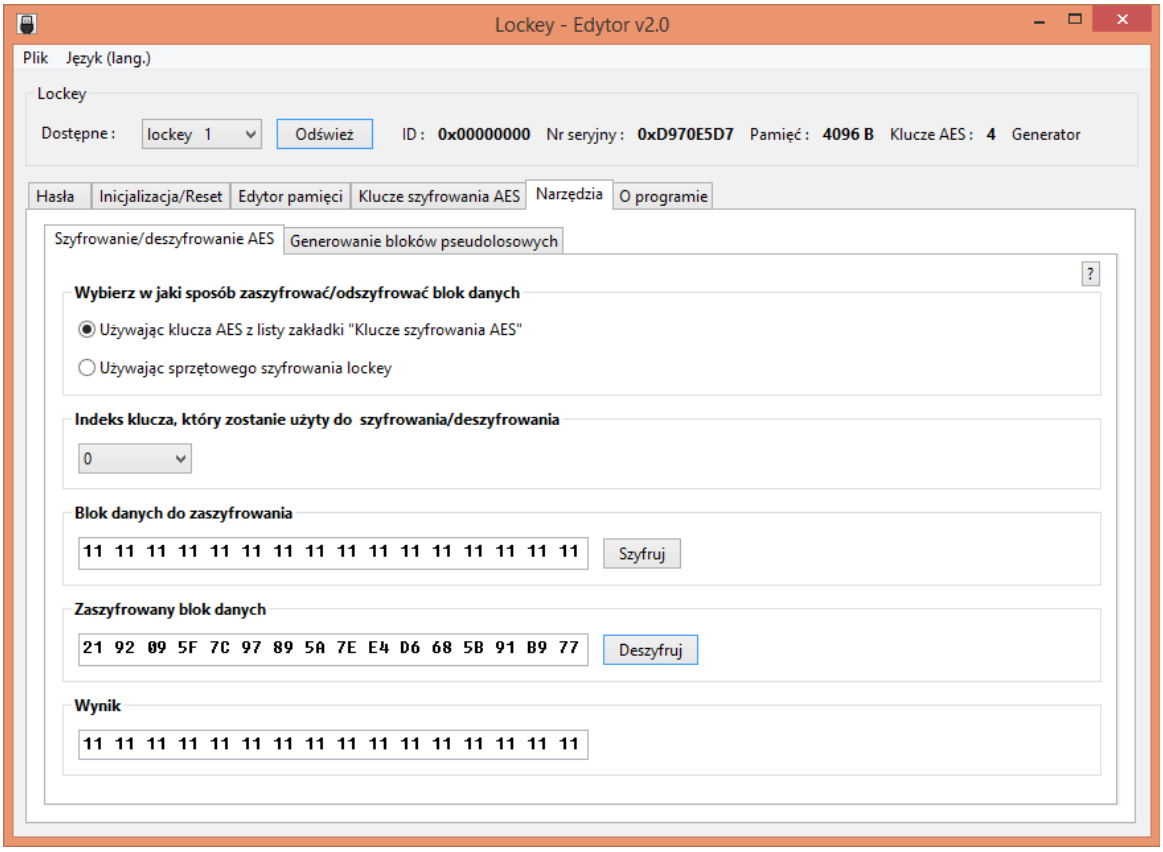
Szyfrowanie można wykorzystać np. do :

- zabezpieczania plików aplikacji, projektów, tekstów, grafik itp.
- ochrony danych wysyłanych przez sieć
- generowania podpisów elektronicznych dla danych lub dokumentów

Narzędzia

Zakładka zawiera pomocnicze narzędzia przeznaczone do wykorzystania podczas procesu zabezpieczania oprogramowania.

Szyfrowania/Deszyfrowanie AES



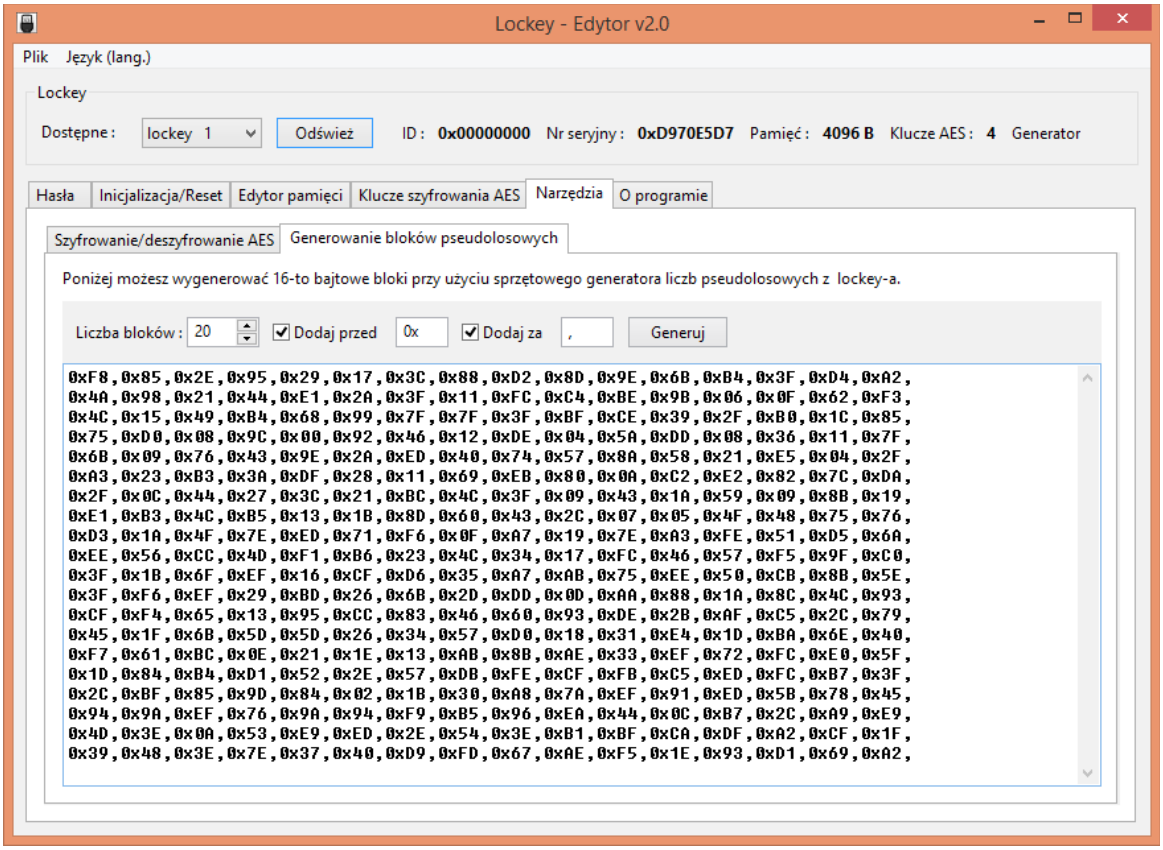
Zestaw narzędzi umożliwiający zaszyfrowanie lub odszyfrowanie pojedynczego bloku danych algorytmem szyfrowania AES.

Szyfrowania można dokonać używając klucza szyfrowania z listy (w zakładce **Klucze szyfrowania AES**) lub używając do tego celu sprzętowego szyfrowania zaimplementowanego w **lockey-u**.

Przykładowe wykorzystanie :

- ochrona wrażliwych fragmentów tablic lub dowolnych danych w kodzie zabezpieczanego programu
- test poprawności wyników algorytmu AES

Generowanie bloków pseudolosowych



Przy użyciu **lockey-a** możliwe jest wygenerowanie bloków pseudolosowych.
Bloki mogą posłużyć np. do tworzenia tablic w których możliwe będzie ukrycie wrażliwych informacji, generowania silnych haseł itp.
Generator można również użyć np. jako źródło liczb pseudolosowych do wygenerowania kluczy szyfrowania AES.

Inicjalizacja i reset lockey-a dla przykładów demonstracyjnych

Do nauki API klucza oraz użycia przykładów demonstracyjnych, **zalecamy przeprowadzić inicjalizację w oparciu o ogólnie znane hasła zapisane w projekcie demonstracyjnym.**
W każdym momencie będzie istniała możliwość przywrócenia ustawień fabrycznych dla klucza **lockey** i ponowna inicjalizacja z dowolnymi, tajnymi hasłami.

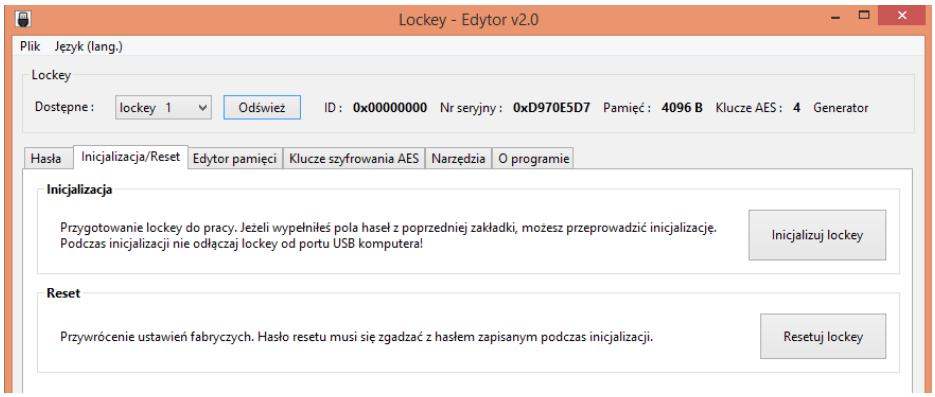
W tym celu należy wykonać kroki :

1) Podłączyć tylko jeden, nie zainicjalizowany **lockey** do komputera.

2) Uruchomić edytor **lockeyedit.**

3) W menu edytora wybrać **Plik/Otwórz projekt** i wczytać dołączony projekt demonstracyjny **demo.lkp/demo_lockey4.lkp/ demo_lockey8.lkp/demo_lockeyi2c.lkp** (w zależności od posiadanego typu klucza).
Na rozwijanej liście w części okna **Lockey/Dostępne** pojawi się **lockey**, który został podłączony do komputera.

4) Kliknąć na zakładkę **Inicjalizacja/Reset**



5) Nacisnąć przycisk **Inicjalizuj lockey** i poczekać na zakończenie inicjalizacji.

Procedurę przywrócenia ustawień fabrycznych na zainicjalizowanym kluczu **lockey** należy przeprowadzić analogicznie z tą różnicą, że finalnie należy nacisnąć przycisk **Resetuj lockey**.

UWAGA

*Pamiętaj, nieznajomość haseł po inicjalizacji klucza **lockey** jest równoznaczna z :*

- *<u>całkowitym brakiem dostępu do klucza **lockey**</u>*
- *brakiem możliwości przywrócenia ustawień fabrycznych klucza **lockey***

Ze względu na długość tablic haseł i siłę użytego algorytmu AES, nie przyjmuje się sytuacji złamania haseł znanymi metodami w rozsądnym czasie (przy założeniu, że podczas inicjalizacji lockey-a zostały użyte, mocne hasła w postaci tablic wypełnionych wartościami losowymi).

*Podczas inicjalizacji/resetu nie wolno odłączać klucza **lockey** od komputera!*

Domyślne hasła inicjalizacji dla projektów demonstracyjnych :

Hasło komunikacji (logowania) : lalamido
Hasło resetu : lalamidoreset

Notatki

Notatki

www: lockey.pl

e-mail: biuro@lockey.pl