

Laboratorium nr 2

Demonstracja ataku AES-CBC Padding Oracle

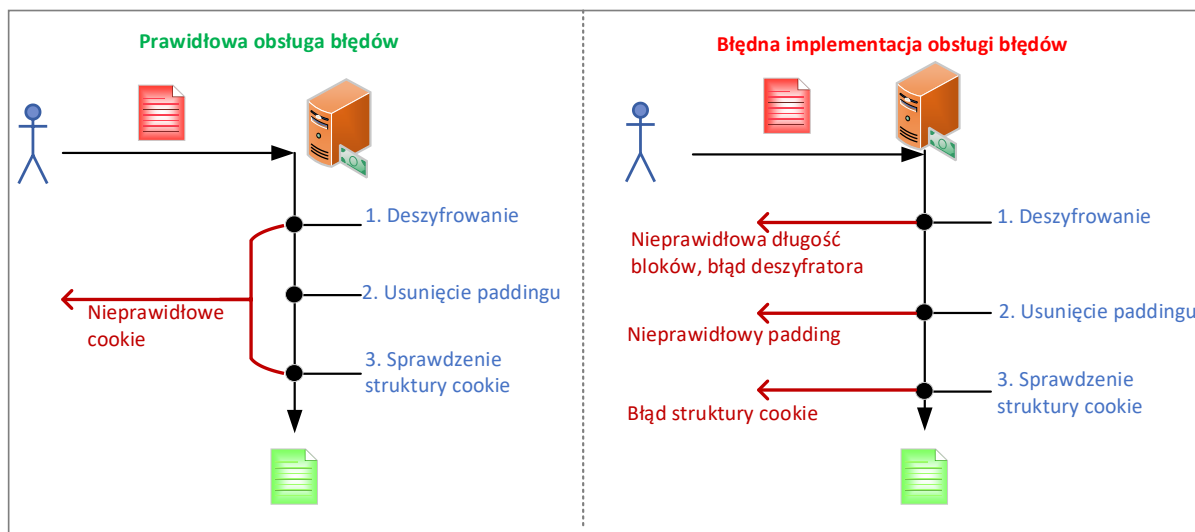
Termin wykonania: **do lab 4**Liczba punktów: **4 + 1**

PRK: T-L-1

1. Opis laboratorium

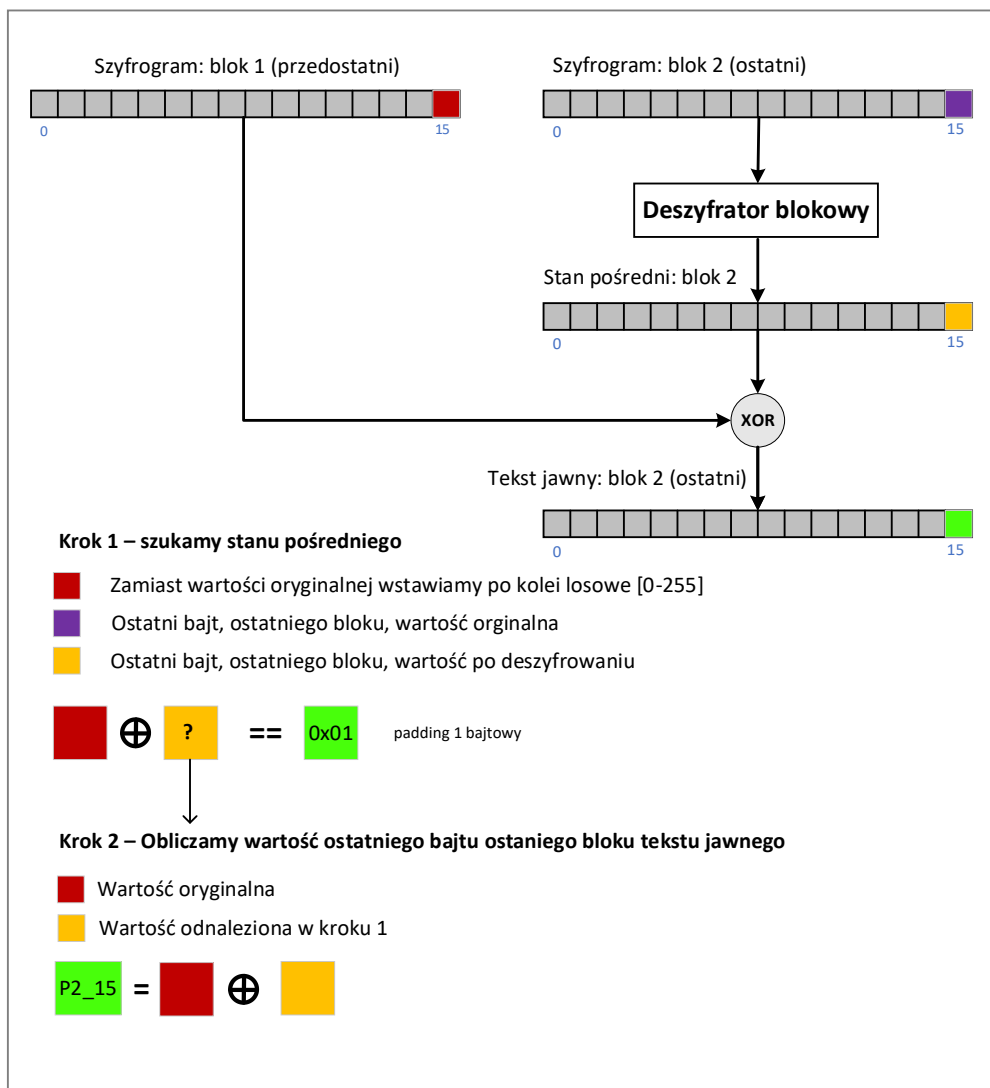
Celem laboratorium jest napisanie programu demonstrującego działanie ataku na algorytm AES działający w trybie CBC, który umożliwia odczytanie wszystkich boków oprócz pierwszego. Atak ten jest możliwy, gdy dostępna jest wyrocznia, np. serwer zwracający informacje czy podany szyfrogram ma prawidłowy *padding* (np. wg PKCS7). Atakujący nie poznaje zawartości klucza, a pomimo to jest w stanie odczytać wiadomość bez ostatniego bloku.

Atak jest możliwy, kiedy błędnie wykonana jest implementacja obsługi błędów serwera przetwarzającego zaszyfrowane pliki cookie, co przedstawiono na rysunku poniżej.



RYS. 1 – DESZYFROWANIE PLIKÓW COOKIE

W ataku w pierwszej kolejności staramy się odczytać ostatni bajt z ostatniego bloku. Schemat postępowania przedstawiono na rysunku 2 na następnej stronie. Natomiast rysunek 3 pokazuje jak wygląda wyjątek zwracany w przypadku nieprawidłowego padding w C#.



RYS. 2 – KONCEPCJA ATAKU NA PRZYKŁADZIE OSTATNIEGO BAJTA OSTATNIEGO BLOKU

```

176 public int DecryptOracle(byte[] ciphertext)
177 {
178     int result = 0;
179     try
180     {
181         var plaintext = dec.TransformFinalBlock(ciphertext, 0, ciphertext.Length);
182     }
183     catch (Exception ex)
184     {
185         if (ex.Message == "Padding is invalid and cannot be removed.")
186         {
187             // ...
188         }
189         else
190         {
191             // ...
192         }
193     }
194     return result;
195 }

```

Exception: ("Padding is invalid and cannot be removed.")

Properties:

- Data: {System.Collections.ListDictionaryInternal}
- HResult: -2146233087
- HelpLink: null
- IPForWatsonBuckets: 0x00007ff9a77a555f
- InnerException: null
- IsTransient: false
- Message: "Padding is invalid and cannot be removed."
- RemoteStackTrace: null
- Source: "System.Security.Cryptography.Algorithms"

RYS. 3 – OBSŁUGA BŁĘDU W C# - WYJĄTEK NIEPRAWIDŁOWEGO PADDINGU

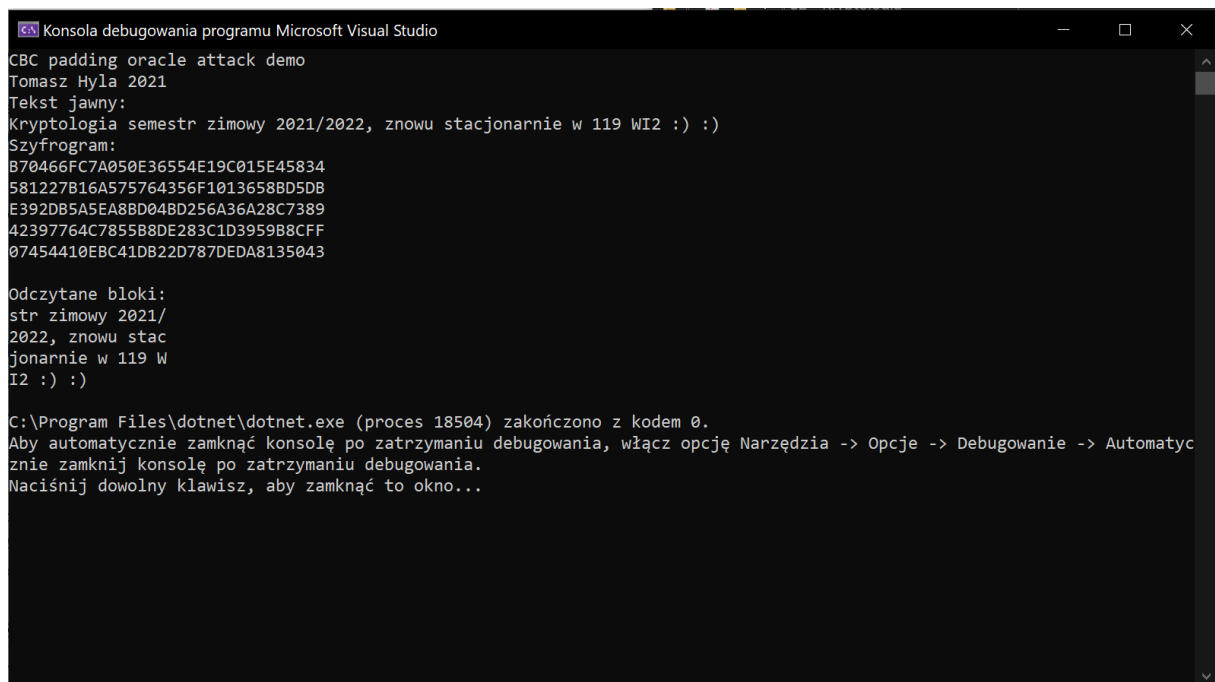
2. Materiały

- Oryginalny artykuł przedstawiający atak:
<https://www.iacr.org/cryptodb/archive/2002/EUROCRYPT/2850/2850.pdf>
- Artykuł ze strony sekurak.pl:
<https://sekurak.pl/czym-jest-padding-oracle-atak-i-ochrona/>
- Wikipedia:
https://en.wikipedia.org/wiki/Padding_oracle_attack
- Inny opis krok po kroku:
<https://robertheaton.com/2013/07/29/padding-oracle-attack/>
- Film instruktażowy na YT:
<https://www.youtube.com/watch?v=05SeQxErXA4>

3. Zadania do wykonania

Napisz program demonstrujący działanie ataku na podstawie materiałów z pkt. 2:

- a) program ma działać w konsoli w trybie tekstowym, pobierać od użytkownika ciąg tekstowy, szyfrować ten ciąg, wyświetlać ciąg i szyfrogram, następnie przeprowadzić atak i wyświetlić odczytane boki (przykładowy zrzut ekranu znajduje się na Rys. 4);
 - b) wyrocznie (ang. *oracle*) należy zaimplementować jako funkcję w celu uproszczenia programu;
 - c) język programowania jest dowolny.
1. **Zadanie 1** (1 pkt + 1 pkt do lab2) – należy odczytać ostatni bajt ostatniego bloku.
 2. **Zadanie 2** (1 pkt) – należy odczytać ostatni blok.
 3. **Zadanie 3** (1 pkt) – należy odczytać cały tekst jawny bez pierwszego bloku. Oczekiwany efekt działania pokazuje zrzut ekranu na rysunku 4 na następnej stronie.
 4. **Zadanie 4** (1 pkt) – odpowiedz na poniższe pytania
 - a) Jaki jest czas wykonania ataku dla szyfrogramu składającego się z 5 bloków? Podaj również dane techniczne komputera, na którym przeprowadzono test. Test wykonaj 3-krotnie i podaj uśrednione wyniki.
 - b) Kiedy możliwy jest odczyt również pierwszego bloku?
 - c) Jaki błąd przy implementacji należy popełnić, aby atak był możliwy?
 - d) W jakich środowiskach zaimplementowano ten atak? (wymień przynajmniej 3)
 - e) Czy atak działa tylko dla algorytmu AES? Odpowiedź uzasadnij.
 - f) Ile razy maksymalnie należy odpytać wyrocznie w celu odczytania jednego bloku?
 - g) Czy w przypadku zastosowania innych schematów padding'u atak będzie działał? Odpowiedź uzasadnij.



```
Konsola debugowania programu Microsoft Visual Studio
CBC padding oracle attack demo
Tomasz Hyla 2021
Tekst jawny:
Kryptologia semestr zimowy 2021/2022, znowu stacjonarnie w 119 WI2 :) :)
Szyfrogram:
B70466FC7A050E36554E19C015E45834
581227B16A575764356F1013658BD5DB
E392DB5A5EA8BD04BD256A36A28C7389
42397764C7855B8DE283C1D3959B8CFF
07454410EBC41DB22D787DEDA8135043

Odczytane bloki:
str zimowy 2021/
2022, znowu stac
jonarnie w 119 W
I2 :) :)

C:\Program Files\dotnet\dotnet.exe (proces 18504) zakończono z kodem 0.
Aby automatycznie zamknąć konsolę po zatrzymaniu debugowania, włącz opcję Narzędzia -> Opcje -> Debugowanie -> Automatycznie zamknij konsolę po zatrzymaniu debugowania.
Naciśnij dowolny klawisz, aby zamknąć to okno...
```

RYS. 4 – ZRZUT EKRANU Z PRZYKŁADOWEGO PROGRAMU