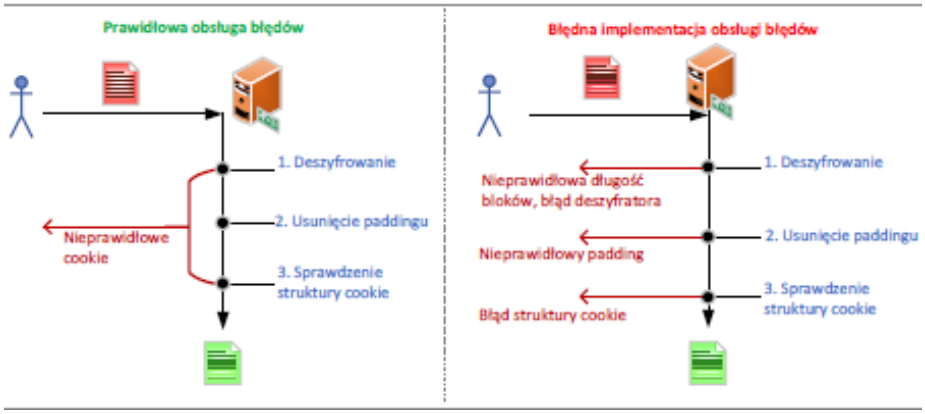
Laboratorium 2
Demonstracja ataku AES-CBC Padding Oracle

23 października 2021

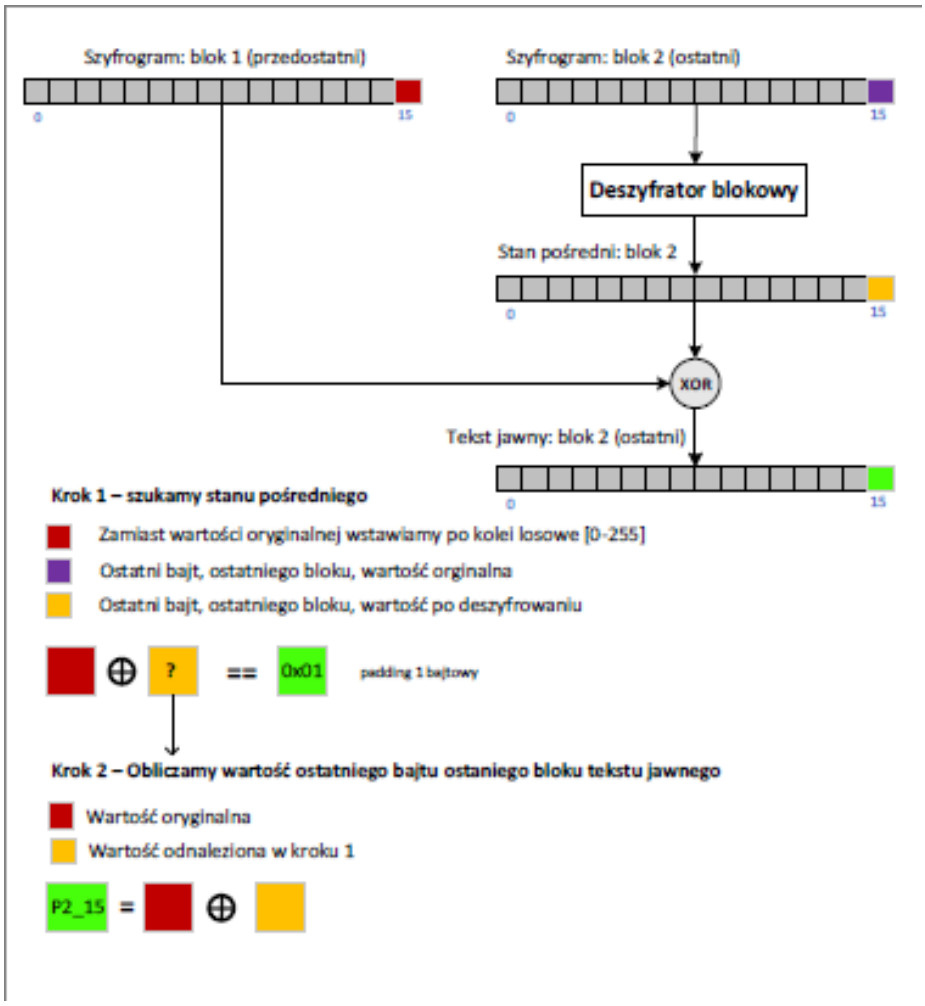
1 Opis problemu

Celem laboratorium jest napisanie programu demonstrującego działanie ataku na algorytm AES działający w trybie CBC. Atak ten umożliwia odczytanie wszystkich boków oprócz ostatniego. Atak ten jest możliwy, gdy dostępna jest wyrocznia, np. serwer zwracający informacje czy podany szyfrogram ma prawidłowy padding (np. według standardu 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 (1).



Rysunek 1: Deszyfrowanie plików cookie

W ataku w pierwszej kolejności staramy się odczytać ostatni bajt z ostatniego bloku. Schemat postępowania przedstawiono na Rysunku 2.



Rysunek 2: Wytłumaczenie przebiegu ataku na przykładzie ostatniego bajta ostatniego bloku

2 Materiały do zajęć

- Artykuł przedstawiający atak - Link 1
- Opis z wikipedii - Link 2
- Opis ataku krok po kroku - Link 3

W czasie programowania problemu polecam bazować szczególnie na 3 odnośniku. Natomiast w trakcie implementacji, w przypadku języka Python, pole-

cam wykorzystać bibliotekę Crypto, która zawiera gotowe rozwiązania do algorytmu AES oraz do obliczania paddingu.

3 Zadania

Do zaimplementowania jest skrypt bazujący na schemacie działania przedstawionym w materiałach z punktu 2.

- Program ma działać w konsoli w trybie tekstowym
- Należy pobierać od użytkownika ciąg tekstowy, a następnie go zaszyfrować
- Program nma wyświetlać ciąg bazowy i szyfrogram
- Następnie należy przeprowadzić atak i wyświetlić odczytane boki (przykładowy zrzut ekranu znajduje się na Rysunku 4)
- Program implementujemy w języku Python
- Termin wykonania zadania: do następnych zajęć laboratoryjnych

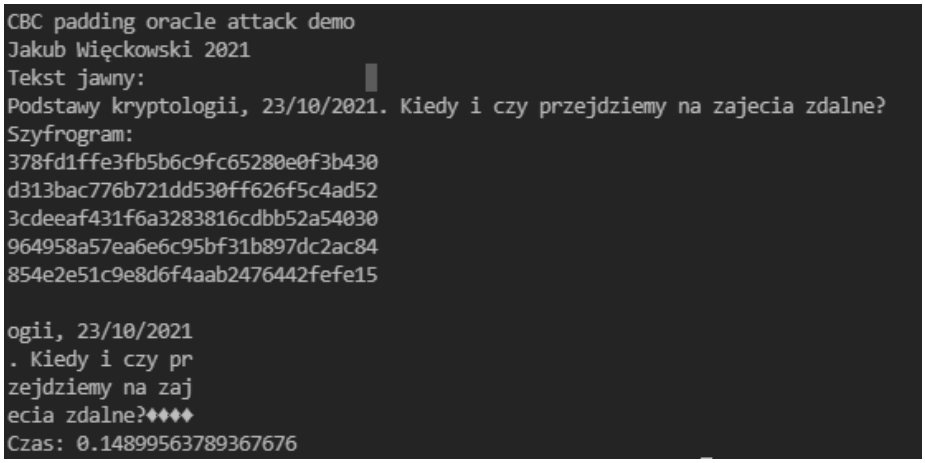
Zadanie 1 (2pkt + 2 pkt przy oddaniu działajacej funkcji na zajęciach) – należy odczytać ostatni bajt ostatniego bloku

Zadanie 2 (1pkt + 2 pkt przy oddaniu działajacej funkcji na zajęciach) – należy odczytać ostatni blok

Zadanie 3 (2pkt) – należy odczytać cały tekst jawny bez pierwszego bloku. Oczekiwany efekt działania pokazuje zrzut ekranu na Rysunku 3

Zadanie 4 (1pkt) – odpowiedzieć na poniższe pytania:

- Jaki jest czas wykonania ataku dla szyfrogramu składającego się z 5 bloków? Test należy wykonać 3-krotnie i podać uśrednione wyniki.
- Kiedy możliwy jest odczyt również pierwszego bloku?
- Jaki błąd przy implementacji należy popełnić, aby atak był możliwy?
- Czy atak działa tylko dla algorytmu AES? Jeśli tak to dlaczego, jeśli nie to podać inny algorytm, dla którego atak zadziała.
- Ile razy maksymalnie należy odpytać wyrocznię w celu odczytania jednego bloku?
- Czy w przypadku zastosowania innych schematów padding'u atak będzie działał?



Rysunek 3: Przykładowy wynik działającego programu.