Ćwiczenia laboratoryjne z przedmiotu Kryptografia i Bezpieczeństwo Danych

Temat: Wprowadzenie do narzędzia CrypTool 2

Autor: Sławomir Samolej

Wprowadzenie

1. Jednym z ważnych z punktu widzenia dydaktyki i analizy systemów szyfrowania, darmowym narzędziem jest CrypTool 2. Umożliwia ono graficzne projektowanie algorytmów, systemów oraz protokołów kryptograficznych. Przebieg działania danego algorytmu/systemy/protokołu jest na bieżąco wizualizowany, co stanowi dodatkowy atut narzędzia.
2. Narzędzie, dzięki przygotowanemu zestawowi wzorców, pozwala na analizę gotowych konstrukcji kryptograficznych oraz na przeprowadzenie na nich ataków.

Uwagi:

W przebiegi ćwiczenia założono, że zostało już pobrane ze strony [1] i zainstalowane narzędzie Cryptool 2.

Przebieg ćwiczenia

1. Proszę prześledzić wprowadzenie prowadzącego do posługiwania się narzędziem CrypTool 2.
2. Proszę zapoznać się z wprowadzeniem zamieszczonym w pozycji [2] literatury.
3. Proszę zapoznać się z wprowadzeniem zamieszczonym w pozycji [3] literatury.
4. Proszę skonstruować prosty demonstrator szyfrowania z zastosowaniem szyfru Cezara.
5. Proszę skonstruować prosty demonstrator działania szyfrowania AES.
6. Proszę przeanalizować przykład ataku na padding w szyfrowaniu AES CBC.

Literatura

[1] (Strona narzędzia CrypTool) https://www.cryptool.org

[2] (Materiał wprowadzający do pracy z CrypTool 2 (1)) https://www.youtube.com/watch?v=5DJH2bd8yo8

[3] (Materiał wprowadzający do pracy z CrypTool 2 (2)) https://www.youtube.com/watch?v=dELT2-Vgsr8&t=633s