POLITECHNIKA CZĘSTOCHOWSKA
WYDZIAŁ INŻYNIERII MECHANICZNEJ I INFORMATYKI

Sprawozdanie
Szyfrowanie danych XOR

Piotr Zyszczak

Nr albumu: 113066

Kierunek: Informatyka

Studia: stacjonarne

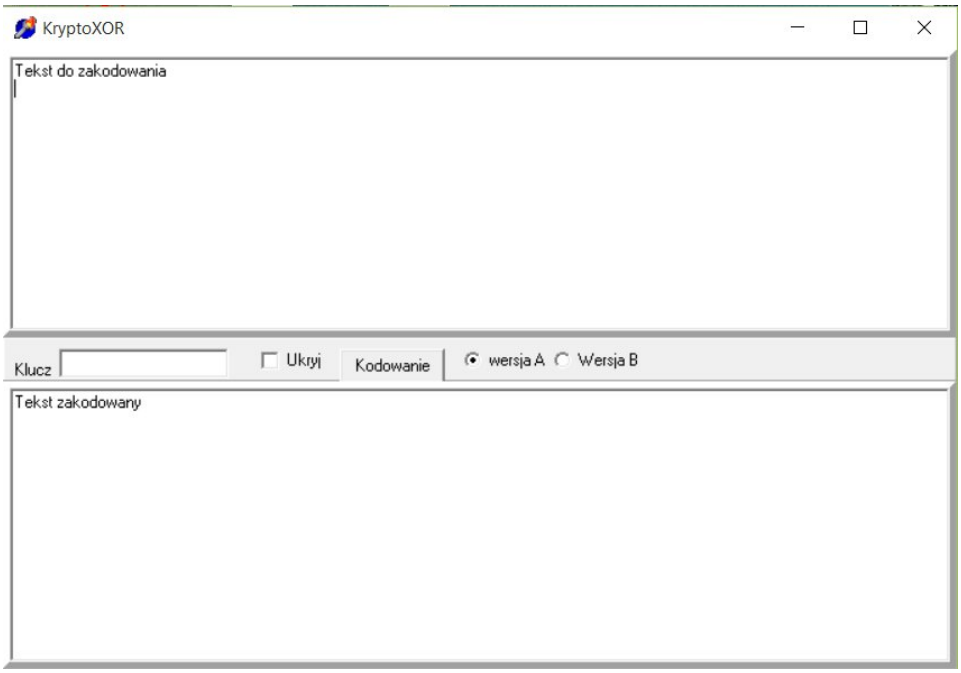
Poziom studiów: II

Częstochowa, 2015

Spis treści

1. Cel i zakres zajęć

Celem zajęć było zapoznanie się z szyfrowaniem XOR i demonstracje szyfrowania tą metodą przy użyciu programu "KryptoXOR".



Rysunek 1.1: Interfejs programu.

2. Wstęp teoretyczny

Szyfr XOR to odmiana szyfru Vigenère'a. Różni się tym, że zamiast manipulować na literach i znakach, zmienia bity i bajty wiadomości przechowywanej w pamięci.

Zamiast dodawać do siebie dwie litery, jak w oryginalnej wersji, w szyfrze XOR algorytm sumuje kolejne bajty tekstu jawnego i klucza o dowolnej długości za pomocą działania XOR. Po wykorzystaniu ostatniego bajtu, przechodzi się z powrotem do pierwszego (jak w klasycznej wersji).

W celu odszyfrowania postępowanie jest takie samo, czyli dodaje się bajty klucza do bajtów szyfrogramu za pomocą operacji XOR.

Szyfrowanie i deszyfrowanie można w przedstawić za pomocą następujących wzorów: M XOR K = C, C XOR K = M

3. Przebieg

Na laboratorium mieliśmy kodować i rozkodowywać przykładowe teksty przy wykorzystaniu wspomnianego wcześniej programu. Procedura kodowania wygląda następująco.

Rysunek 3.1: Kodowanie tekstu.

Z kolei rozkodowanie wykonuje się odwrotnie. Trzeba tylko wyliczyć lub wpaść na klucz kodujący. Litery klucza których nie znamy można zastąpić znakami zapytania.

Rysunek 3.2: Rozszyfrowanie tekstu.

4. Wnioski

Szyfrowanie metodą XOR nie jest zbyt bezpieczne przy krótkich hasłach ponieważ dla komputera znalezienie szyfru jest kwestją czasu. Za to jeśli klucz jest przynajmniej tak długi jak tekst i jednorazowy powinno stanowić dużo większe wyzwanie. Jednak powstają przy okazji inne problemy związane z zarządzaniem dożą ilością kluczy i ryzykiem z tym związanym.