POLITECHNIKA CZĘSTOCHOWSKA
WYDZIAŁ INŻYNIERII MECHANICZNEJ I INFORMATYKI
INSTYTUT INTELIGENTNYCH SYTSEMÓW INFORMATYCZNYCH

Bezpieczeństwo komunikacji elektronicznej

Laboratorium 1

Kryptografia XOR

Paweł Kalwik

1. Cel zadania

Celem zadania jest przeprowadzenie odszyfrowania czterech plików za pomocą programu KryptoXOR, który wykorzystuje algorytm XOR do szyfrowania.

XOR, alternatywa wykluczająca lub binarne sumowanie modulo 2. Szyfr XOR jest szyfrem symetrycznym, oznacza to, że tak samo się go szyfruje i odszyfrowuje. Operacja ta jest częścią składową wielu rozbudowanych algorytmów kryptograficznych jak np. DES (ang. Data Encryption Standard). Operacja ta sama w sobie stanowi również prosty algorytm szyfrowania, który nie zapewnia jednak większego bezpieczeństwa. Jednak przy spełnieniu kilku bardzo ważnych warunków może stanowić, mimo swej prostoty, algorytm niemożliwy do złamania. Algorytm ten jest nie do złamania w przypadku kiedy hasło jest takiej samej długości co tekst jawny.

2. Odszyfrowanie plików

Przy pomocy programuKryptoXOR możemy zarówno szyfrować pliki jak i je odszyfrować wykorzystując do tego celu dwie wersje algorytmu. Do realizacji zadania wybrano wersję B algorytmu oraz podjęto próbę odszyfrowania czterech plików. Poniżej zaprezentowano odszyfrowane pliki.

Plik 1 – klucz „kluczyk”:

Rysunek 1 - okno z odszyfrowanym pierwszym tekstem

Plik 2 – klucz „telefon”:

Rysunek 2 - okno z odszyfrowanym drugim tekstem

Plik 3 – klucz „adapter”:

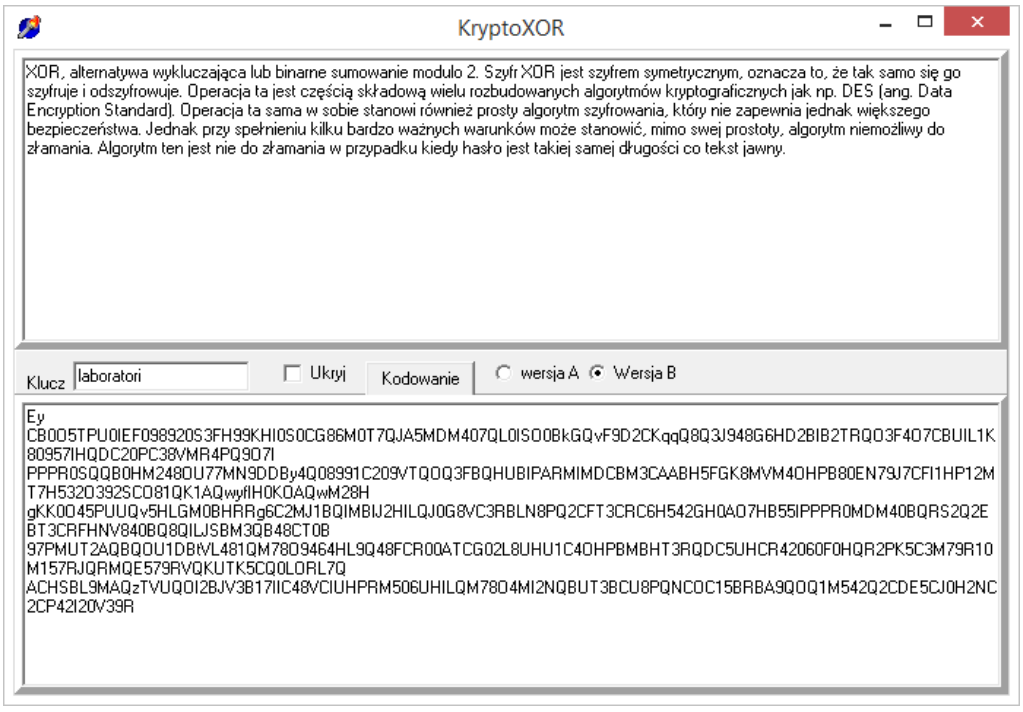
Rysunek 3 - okno z odszyfrowanym trzecim tekstem

Plik 4 – klucz „monitor”:

Rysunek 4 - okno z odszyfrowanym czwartym tekstem

3. Dodatkowy plik – test szyfrowania

Dla urozmaicenia zadania wybrano jeden dodatkowy tekst i zaszyfrowano go kluczem „laboratori”. A następnie dano innym osobom w celu odszyfrowania. Zrzut ekranu z procesu szyfrowania przedstawiono poniżej.



Rysunek 5 - okno z własnym zaszyfrowanym tekstem

4. Wnioski

Przy pomocy programu KryptoXOR możemy zarówno szyfrować pliki jak i je odszyfrować. W niektórych przypadkach można się wspomagać znakami spacji lub znakami zapytania co zdecydowania ułatwia rozkodowywania. Po pewnym czasie można zauważyć pewne schematy kodowania poszczególnych liter co również nie pozostaje bez echa. W aktualnej wersji aplikacji można było wykorzystać jedynie klucz o 10 znakach. Po pewnym czasie dało się zaobserwować, że jeśli tekst jawny i hasło są takie same to w wyniku dostajemy same zera.