Bezpieczeństwo komputerowe
Laboratorium, Lista 3

Wojciech Strzelecki

14 listopada 2021

1 Jak na skuteczność programu wpływają długości kryptogramów?

Zróżnicowane długości kryptogramów mogą mieć negatywny wpływ na jakość odszyfrowanych kryptogramów. Najlepsz wynik otrzymamy mając wszystkie kryptogramy o podobnej długości. Wynika to z porównywania wszystkich wszystkich znaków kryptogramu na $i - tej$ pozycji. Świetnie widać to w zadaniu, gdzie początki linijek dla odszyfrowywanych programów tworzą składniowo logiczny teskt, a przy końcówkach dłużych kryptogramów otrzymujemy zlepek kompletnie bezsensownych słów.

2 Jak na skuteczność programu wpływa liczba kryptogramów?

Łatwo możemy to sprawdzić eksperymentalnie, poprzez zmniejszanie listy przechwyconych kryptogramów i sprawdzeniu co zwróci funkcja dekrypcji.

- n = 5: wbwhsc na porgdoakach/ Po‘ska¡wprobadza bedhoynowy/pa.ift.Chrzyst n Cogrzeb
- n = 10: 4owosc na porodowkach/ Polska wprowadza jed‘odniowy pakizt.Chrzest + Pogrzeb
- n = 15: \owosc na porodowkach. Polska wprowadza jednodniowy pakiet Chrzest + Pogrzeb

- n = 20: Nowosc na porodowkach. Polska wprowadza jednodniowy pakiet Chrzest + Pogrzeb

3 Rodzaj szyfru strumieniowego

Szyfry strumieniowe są algorytmami symetrycznymi. Algorytm ten składa się z klucza szyfrującego oraz wykonywania odpowiednio operacji xor. Mój program powinien dać zatem podobne wyniki. To czym różnią się algorytmy strumieniowe to przykładowo długość klucza. W OTP klucz musi być długości co najmniej równej długości wiadomości, a w przypadku Salsa20 klucz ma ustaloną długość (32 bajty).

4 Kodowanie

Kodowanie znaków również może mieć wpływa na wyniki testów. Wynika to z długości zapisu. W kodowaniu $UTF-8$ polskie znaki zapisane są na 2 bajtach, a mój program rozpatruje jedynie chary jedno-bajtowe.