Bezpieczeństwo komputerowe
Lista 4

Piotr Kasprowicz

November 2018

1 Wprowadzenie

Zadanie polegało złamaniu 20 szyfrogramów o których wiemy, że każdy z nich powstał jako rezultat szyfrowania wiadomości za pomocą szyfru strumieniowego. Każdy z nich został zaszyfrowany przy pomocy tego samego klucza.

2 Rozwiązanie zadania

Rozwiązanie zadania zostało oparte na częstotliwości występowania znaków w języku polskim oraz "ogadywaniu", który ze znaków po XOR daje nam sensowny wynik. Wartość która najlepiej dopasowuje się do danych dodajemy do klucza. Wymaga to jednak, więcej szyfrogramów niż 2. Przy 5 jesteśmy w stanie zobaczyć pierwsze poprawne słowa. A przy 7-8 domyślić się znaczenia zdań. Przy 10 tekst już układa się w logiczny sens, mimo pojedynych pomyłek. Użycie 20 kryptogramów pozwala na praktycznie całkowite zdeszyfrowanie początków wiadomości. Końcówki nie są takie trywialne ze względu na różne długości szyfrogramów i braku wystarczającej ilości próbek,aby znaleźć poprawny klucz dla ostatnich bajtów.

Ostatni zdeszyfrowany kryptogram:
$Szwed, HalejcioiGardiasnagaliOrlenu(DUZOZDJEC)$.