Kryptografia i kryptoanaliza

Laboratorium 5

Michał Łaskawski

Zadanie 1

Dokonać implementacji kryptosystemu strumieniowego, którego strumień klucza generowany jest przy pomocy `LFSR`. Należy przyjąć, iż:

- Model rejestru zdefiniowany jest następującym wielomianem połączeń: $P(x) = 1 + x + x^3 + x^5 + x^{16} + x^{17}$.
- Sekwencja inicjująca jest następująca: `[0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1]`

Implementowany kryptosystem powinien mieć funkcjonalność szyfrowania fragmentu tekstu odczytanego z pliku tekstowego i zapisu szyfrogramu do nowego pliku.

Zadanie 2

Dokonać ataku na zbudowany w ramach pierwszego zadania kryptosystem. Przyjąć następujące złożenia ataku:

- Znane są tylko: tekst jawny i szyfrogram.
- Celem ataku jest:
  - Odzyskanie klucza.
  - Określenie schematu połączeń rejestru `LFSR`.
  - Zbudowanie własnego kryptosystemu, będącego w stanie odczytać szyfrogramy generowane przez kryptosystem z 1 zadania (kryptosystem nadawcy).

Procedura postępowania:

- Odzyskanie klucza: W tym celu wystarczy wykonać operację: $s_i = x_i \oplus y_i$ dla $i = 1, \ldots, n$ gdzie n jest ilością bitów wiadomości (szyfrogramu).
- Określenie schematu połączeń `LFSR`: Do tego celu należy użyć algorytmu z 3 zadania 4 instrukcji.

Następnie:

- Zbudować kryptosystem w oparciu o zidentyfikowany w ramach przedstawionej procedury rejestr `LFSR`.
- Dokonać implementacji funkcji porównującej odzyskany klucz z kluczem wygenerowanym w ramach nowego kryptosystemu.
  - Uwaga, zgodność kluczy będzie można porównać tylko wtedy gdy, zidentyfikowany (nowy) kryptosystem zostanie zainicjowany taką samą sekwencją inicjującą, jakiej użył nadawca wiadomości. Sekwencja ta będzie znana po wykonaniu procedury odzyskania klucza. Ilość bitów sekwencji inicjującej będzie znana po zidentyfikowaniu schematu połączeń `LFSR`.
- Jeżeli klucze będą się zgadzać, dokonać odszyfrowania szyfrogramu przy pomocy zidentyfikowanego kryptosystemu.

Zadanie 3

Dokonać ataku na zbudowany w ramach pierwszego zadania kryptosystem. Przyjąć następujące złożenia ataku:

- Znane są tylko: szyfrogram i początkowy fragment tekstu jawnego.
- Celem ataku jest:
  - Odzyskanie klucza.
  - Określenie schematu połączeń rejestru `LFSR`.
  - Określenie minimalnej długości (ilości bitów) tekstu jawnego, umożliwiającego odzyskanie kompletnej wiadomości.
  - Określenie zależności pomiędzy złożonością liniową zidentyfikowanego kryptosystemu, maksymalną sekwencją klucza, która generowana jest przez ten kryptosystem a wymaganą minimalną długością znanego tekstu jawnego.