Podstawy Ochrony Danych – laboratorium AGC

BBS - Implementacja generatora ciągów losowych oraz wybranych testów losowości.

Generator BBS (Blum-Blum-Shub) – to algorytm oparty polegający na obliczaniu reszt kwadratowych modulo n. Pozwala na generowanie kluczy strumieniowych o określonej długości w sposób pseudolosowy. Podstawową trudność użycia algorytmu stanowi wyznaczenie liczby Bluma, czyli liczby N=p*q, przy założeniu, że p i q to odpowiednio duże liczby pierwsze, przystające do 3 modulo 4, od których zależy bezpieczeństwo i jakość generatora.

Algorytm

1. Wyznacz wartość iloczynu N dwóch dużych liczb pierwszych, takich że:

   $p \equiv 3 \ mod \ 4$

   $q \equiv 3 \ mod \ 4$

2. Wybierz w sposób losowy taką liczbę x taką, że x i N są względnie pierwsze.
3. Wyznacz wartość pierwotną generatora:

   $x_0 = x^2 \ mod \ N$

4. Powtarzaj w pętli

   $x_{i+1} = x_i^2 \ mod \ N$

Bit wyjścia stanowi najmłodszy bit (LSB, ang. Least Significant Bit) będący jednocześnie i-tym bitem klucza.

Cel ćwiczenia laboratoryjnego: zapoznanie się z tematyką generatorów ciągów pseudolosowych, analiza własności jakie powinny posiadać takie ciągi, implementacja generatora BBS oraz 4 testów FIPS 140-2 (pojedynczych bitów, długiej serii, serii oraz pokerowego).

Materiały do laboratorium: materiały z wykładu oraz materiały dodatkowe podane przez prowadzącego

Zadanie:

1. Przeanalizuj na podstawie podanej literatury jakie własności powinien posiadać ciąg pseudolosowy.
2. Jak testuje się losowość ciągów?
3. Zaimplementuj generator BBS.
4. Wygeneruj ciąg 20 000 bitów.
5. Zaimplementuj przynajmniej 4 testy FIPS 140-2 i przebadaj wygenerowany wcześniej ciąg.
6. Zinterpretuj otrzymane wyniki.