УДК 004.56.5

О.Г. Собінов[1]
Кіровоградський національний технічний університет

Простий генератор псевдовипадкової послідовності

Вступ. Відомо, що ніяка система захисту інформації не може бути абсолютно надійною. Мова може йти лише про деякий ступінь надійності та ризику, який пов'язаний зі зламом захисту. Не дивлячись на існування великої кількості стандартних, пошук нових методів криптозахисту не полишають як спеціалісти у даній області, так і аматори.

Основна частина. В області математики існує цікавий розділ – математичний більярд. "Теорія більярдів" сьогодні – невід'ємна частина ергодичної теорії та теорії динамічних систем, має важливе застосування у фізиці. Видатний математик Гальперін Г.А. створив спосіб визначення числа π за допомогою біліарда. Як виявилося у "поведінці" куль на біліарді (у кількості зіткнень) сховано число π.

Якщо розглядати не кількість зіткнень кулі з боковими поверхнями, а визначати координати зіткнення окремо по вісях абсцис або ординат, то можна отримати числову послідовність псевдовипадкових чисел, залежних від π.

Алгоритм простого генератора, побудованого на засадах математичного біліарду наступний:

1. вибирається довільне прямокутне поле *a*b*, де a та *b* взаємно прості (відносно великі числа);

2. вибирається кут нахилу *p/n* (дискретне зміщення по вісі абсцис та ординат), де *p* та *n* – взаємно прості;

3. вибирається координати запуску кулі x та y (цілочисельні) – в межах прийнятого прямокутного поля *a*b*;

4. при досягненні кулею границь поля(бортів) визначаються координати зіткнення, які і будуть псевдовипадковими числами для створення секретної послідовності.

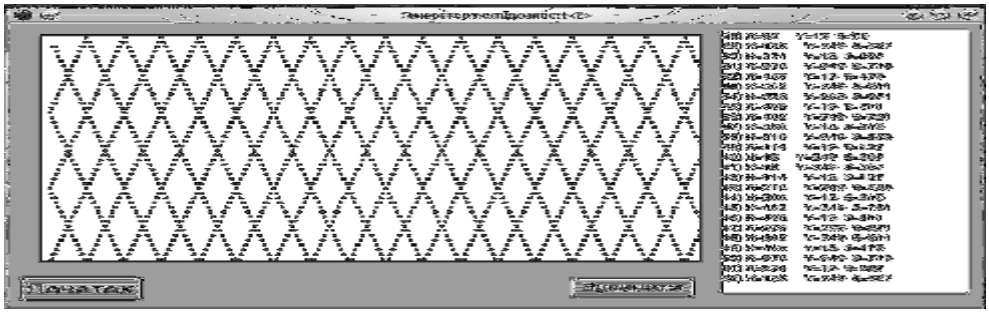

Рисунок 1 – Зовнішній вигляд вікна програми, яка генерує секретну послідовність з графічною інтерпретацією зіткнень кулі з "бортами"

Висновки. Теорія математичного біліарду і, зокрема, його приховані можливості щодо обчислення числа π можуть дати цікаві алгоритми створення ключів для криптографічного захисту інформації.

[1] викладач кафедри програмного забезпечення