НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

**АCИМЕТРИЧНА КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1 Побудова тестів для перевірки якості випадкових та**

**псевдовипадкових послідовностей**

Виконав:

студент групи ФІ-33

Богуцький Олександр

Прийняв:

Яковлев С. В.

Київ

2016

**Мета роботи**

Вивчення критеріїв згоди і набуття навичок у побудові та застосуванні тестів для перевірки статистичних властивостей бінарних випадкових і псевдовипадкових послідовностей, ознайомлення з поняттям М-послідовності.

Труднощів при виконанні лабораторного практикуму не виникло.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Назва генератора | Тест 1  Критерій перевірки рівноімовірності знаків | | | | Тест 2  Критерій перевірки незалежності знаків | | | | Тест 3  Критерій перевірки однорідності двійкової послідовності (r = 30) | | | |
| χ²(α = 0.01) = 307.5363 | χ²(α = 0.05) = 292.146 | | χ²(α = 0.1) = 283.9415 | χ²(α = 0.01) = 65863.94 | χ²(α = 0.05) = 65618.17 | | χ²(α = 0.1) = 65487.16 | χ²(α = 0.01) = 7677.91682 | χ²(α = 0.05) = 7595.03751 | | χ²(α = 0.1) = 7550.85484 |
| Значення | | Результат | | Значення | | Результат | | Значення | | Результат | |
| 1 | Вбудований генератор | 280.694 | | +++ | | 64873.424 | | +++ | | 7659.823 | | +-- | |
| 2.1 | LehmerLowGenerator | 0.1059 | | +++ | | 6.35E7 | | --- | | 93.671 | | +++ | |
| 2.2 | LehmerHighGenerator | 89.796 | | +++ | | 66003.615 | | --- | | 7274.186 | | +++ | |
| 3 | L20Generator | 219.188 | | +++ | | 61168.185 | | +++ | | 7378.855 | | +++ | |
| 4 | L89Generator | 278.121 | | +++ | | 64915.375 | | +++ | | 6963.685 | | +++ | |
| 5 | GeffeGenerator | 217.832 | | +++ | | 73190.940 | | --- | | 7081.863 | | +++ | |
| 6 | WolframGenerator | 264.084 | | +++ | | 64981.388 | | +++ | | 7376.690 | | +++ | |
| 7 | LibraryGenerator | 1997782.819 | | --- | | 277847.502 | | --- | | 4830.337 | | +++ | |
| 8 | BMGenerator | 252.300 | | +++ | | 64576.546 | | +++ | | 7305.477 | | +++ | |
| 8.2 | BMBytesGenerator | 253.6811 | | +++ | | 65419.567 | | +++ | | 7322.081 | | +++ | |
| 9 | BBSGenerator | 254.766 | | +++ | | 65138.415 | | +++ | | 7380.498 | | +++ | |
| 9.2 | BBSGeneratorByBytes | 243.100 | | +++ | | 64677.944 | | +++ | | 7012.653 | | +++ | |