

Міністерство освіти, науки, молоді та спорту України

Національний технічний університет України

«Київський політехнічний інститут»

Фізико-технічний інститут

**АСИМЕТРИЧНІ КРИПТОСИСТЕМИ**

**ТА ПРОТОКОЛИ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1**

**Побудова тестів для перевірки якості випадкових та псевдовипадкових послідовностей**

**Виконали:**

Студенти групи ФІ-73

Морозюк Анастасія,

Гетьман Дмитро

**Перевірив:**

Деркач О. Г.

Київ 2020

**1. 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.

**2. Постановка задачі**

1) Написати програми, які реалізують генератори псевдовипадкових бітів, наведені у розділі 2.3 теоретичних відомостей, а саме:

1) вбудований генератор вашої мови програмування;

2) генератор LehmerLow;

3) генератор LehmerHigh;

4) генератор L20;

5) генератор L89;

6) генератор Джиффі (Geffe);

7) генератор «Бібліотекар»;

8) генератор Вольфрама;

9) генератор Блюма-Мікалі BM;

10) генератор BM\_bytes (байтова модифікація генератору Блюма-Мікалі);

11) генератор BBS;

12) генератор BBS\_bytes (байтова модифікація генератору BBS).

2) Розробити програми для реалізації трьох тестів перевірки якості двійкових послідовностей: про рівноімовірність розподілу, про незалежність і про однорідність. Програми повинні враховувати можливості введення випробовуваної послідовності різної довжини із зазначених датчиків, а також із зовні заданого файлу, можливості задавати різні значення рівня значимості α = 0.01; 0.05; 0.1.

3) Провести обробку трьома побудованими тестами прикладів послідовностей, згенерованих зазначеними датчиками, для значень α = 0.01; 0.05; 0.1.

В даній роботі кожна згенерована послідовність містить 218 байт ( або 2 097 152 біта).

**3. Хід роботи**

**Опис труднощів:**

В ході виконання роботи в нас виникли труднощі з генераторами LehmerHigh та Librarian. Проблема в генераторі LehmerHigh полягала в тому, що він не проходив тест на рівноймовірність, це було пов’язано з особливістю роботи вбудованого методу ToByteArray(), який переводить велике число в масив байтів. Даний метод пряцює таким чином, що він не включає старший байт в масив, якщо він дорівнює нулю, таким чином в генерованій послідовності ніколи не зустрічались нулі. Ми вирішили цю проблему шляхом додавання перевірки довжини отриманого масиву, і якщо вона менше 4(більше 4 вийти не може, оскільки кожний xi  береться за модулем числа довжиною 4 байти), то ми додавали 0 в нашу послідовність. Проблема в генераторі Librarian полягала в тому, що він не проходив тест на однорідність. Ми вирішили цю проблему шляхом додаваня функції фільтрації тексту, яка залишає лише літери, усі в нижньому регістрі.

**Отримані результати:**

**Generator: | Test: | Alpha: | X^2 : | X^2\_alpha : | Result**:

--------------------------------------------------------------------------------------------------

Inbuild | Equiprobability | 0,01 | 236,634765625 | 307,5284 | True

--------------------------------------------------------------------------------------------------

Inbuild | Independence | 0,01 | 64929,157596069126| 65863,8124 | True

--------------------------------------------------------------------------------------------------

Inbuild | Uniformity | 0,01 | 3555,335996047599| 3766,54355914 | True

--------------------------------------------------------------------------------------------------

Inbuild | Equiprobability | 0,05 | 236,634765625 | 292,1493 | True

--------------------------------------------------------------------------------------------------

Inbuild | Independence | 0,05 | 64929,157596069126| 65618,2272 | True

--------------------------------------------------------------------------------------------------

Inbuild | Uniformity | 0,05 | 3555,335996047599 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

Inbuild | Equiprobability | 0,1 | 236,634765625 | 283,9516 | True

--------------------------------------------------------------------------------------------------

Inbuild | Independence | 0,1 | 64929,157596069126| 65487,3205 | True

--------------------------------------------------------------------------------------------------

Inbuild | Uniformity | 0,1 | 3555,335996047599 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

LehmerLow | Equiprobability | 0,01 | 0 | 307,5284 | True

--------------------------------------------------------------------------------------------------

LehmerLow | Independence | 0,01 | 16646144 | 65863,8124 | False

--------------------------------------------------------------------------------------------------

LehmerLow | Uniformity | 0,01 | 10,96888747334515| 3766,54355914 | True

--------------------------------------------------------------------------------------------------

LehmerLow | Equiprobability | 0,05 | 0 | 292,1493 | True

--------------------------------------------------------------------------------------------------

LehmerLow | Independence | 0,05 | 16646144 | 65618,2272 | False

--------------------------------------------------------------------------------------------------

LehmerLow | Uniformity | 0,05 | 10,96888747334515 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

LehmerLow | Equiprobability | 0,1 | 0 | 283,9516 | True

--------------------------------------------------------------------------------------------------

LehmerLow | Independence | 0,1 | 16646144 | 65487,3205 | False

--------------------------------------------------------------------------------------------------

LehmerLow | Uniformity | 0,1 | 10,96888747334515 | 3678,32710353| True

--------------------------------------------------------------------------------------------------

LehmerHigh | Equiprobability | 0,01 | 40,88671875 | 307,5284 | True

--------------------------------------------------------------------------------------------------

LehmerHigh | Independence | 0,01 | 66846,891090238 | 65863,8124 | False

--------------------------------------------------------------------------------------------------

LehmerHigh | Uniformity | 0,01 | 3359,1101186441033 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

LehmerHigh | Equiprobability | 0,05 | 40,88671875 | 292,1493 | True

--------------------------------------------------------------------------------------------------

LehmerHigh | Independence | 0,05 | 66846,891090238 | 65618,2272 | False

--------------------------------------------------------------------------------------------------

LehmerHigh | Uniformity | 0,05 | 3359,1101186441033 | 3709,00006655| True

--------------------------------------------------------------------------------------------------

LehmerHigh | Equiprobability | 0,1 | 40,88671875 | 283,9516 | True

--------------------------------------------------------------------------------------------------

LehmerHigh | Independence | 0,1 | 66846,891090238 | 65487,3205 | False

--------------------------------------------------------------------------------------------------

LehmerHigh | Uniformity | 0,1 | 3359,1101186441033 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

L\_20 | Equiprobability | 0,01 | 206,55078125 | 307,5284 | True

--------------------------------------------------------------------------------------------------

L\_20 | Independence | 0,01 | 56640,630130157195 | 65863,8124 | True

--------------------------------------------------------------------------------------------------

L\_20 | Uniformity | 0,01 | 3669,578752857684 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

L\_20 | Equiprobability | 0,05 | 206,55078125 | 292,1493 | True

--------------------------------------------------------------------------------------------------

L\_20 | Independence | 0,05 | 56640,630130157195 | 65618,2272 | True

--------------------------------------------------------------------------------------------------

L\_20 | Uniformity | 0,05 | 3669,578752857684 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

L\_20 | Equiprobability | 0,1 | 206,55078125 | 283,9516 | True

--------------------------------------------------------------------------------------------------

L\_20 | Independence | 0,1 | 56640,630130157195 | 65487,3205 | True

--------------------------------------------------------------------------------------------------

L\_20 | Uniformity | 0,1 | 3669,578752857684 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

L\_89 | Equiprobability | 0,01 | 213,02734375 | 307,5284 | True

--------------------------------------------------------------------------------------------------

L\_89 | Independence | 0,01 | 65161,39269975573 | 65863,8124 | True

--------------------------------------------------------------------------------------------------

L\_89 | Uniformity | 0,01 | 3655,9317391289064 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

L\_89 | Equiprobability | 0,05 | 213,02734375 | 292,1493 | True

--------------------------------------------------------------------------------------------------

L\_89 | Independence | 0,05 | 65161,39269975573 | 65618,2272 | True

--------------------------------------------------------------------------------------------------

L\_89 | Uniformity | 0,05 | 3655,9317391289064 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

L\_89 | Equiprobability | 0,1 | 213,02734375 | 283,9516 | True

--------------------------------------------------------------------------------------------------

L\_89 | Independence | 0,1 | 65161,39269975573 | 65487,3205 | True

--------------------------------------------------------------------------------------------------

L\_89 | Uniformity | 0,1 | 3655,9317391289064 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

Geffe | Equiprobability | 0,01 | 221,953125 | 307,5284 | True

--------------------------------------------------------------------------------------------------

Geffe | Independence | 0,01 | 69006,24718157997 | 65863,8124 | False

--------------------------------------------------------------------------------------------------

Geffe | Uniformity | 0,01 | 3441,5113954703843 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

Geffe | Equiprobability | 0,05 | 221,953125 | 292,1493 | True

--------------------------------------------------------------------------------------------------

Geffe | Independence | 0,05 | 69006,24718157997 | 65618,2272 | False

--------------------------------------------------------------------------------------------------

Geffe | Uniformity | 0,05 | 3441,5113954703843 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

Geffe | Equiprobability | 0,1 | 221,953125 | 283,9516 | True

--------------------------------------------------------------------------------------------------

Geffe | Independence | 0,1 | 69006,24718157997 | 65487,3205 | False

--------------------------------------------------------------------------------------------------

Geffe | Uniformity | 0,1 | 3441,5113954703843 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

Wolfram | Equiprobability | 0,01 | 2641,19921875 | 307,5284 | False

--------------------------------------------------------------------------------------------------

Wolfram | Independence | 0,01 | 309726,52484034526 | 65863,8124 | False

--------------------------------------------------------------------------------------------------

Wolfram | Uniformity | 0,01 | 3441,5113954703843 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

Wolfram | Equiprobability | 0,05 | 2641,19921875 | 292,1493 | False

--------------------------------------------------------------------------------------------------

Wolfram | Independence | 0,05 | 309726,52484034526 | 65618,2272 | False

--------------------------------------------------------------------------------------------------

Wolfram | Uniformity | 0,05 | 3441,5113954703843 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

Wolfram | Equiprobability | 0,1 | 2641,19921875 | 283,9516 | False

--------------------------------------------------------------------------------------------------

Wolfram | Independence | 0,1 | 309726,52484034526 | 65487,3205 | False

--------------------------------------------------------------------------------------------------

Wolfram | Uniformity | 0,1 | 3441,5113954703843 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

Librarian | Equiprobability | 0,01 | 4361062,705078125 | 307,5284 | False

--------------------------------------------------------------------------------------------------

Librarian | Independence | 0,01 | 178282,83471801842 | 65863,8124 | False

--------------------------------------------------------------------------------------------------

Librarian | Uniformity | 0,01 | 2893,140910202084 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

Librarian | Equiprobability | 0,05 | 4361062,705078125 | 292,1493 | False

--------------------------------------------------------------------------------------------------

Librarian | Independence | 0,05 | 178282,83471801842 | 65618,2272 | False

--------------------------------------------------------------------------------------------------

Librarian | Uniformity | 0,05 | 2893,140910202084 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

Librarian | Equiprobability | 0,1 | 4361062,705078125 | 283,9516 | False

--------------------------------------------------------------------------------------------------

Librarian | Independence | 0,1 | 178282,83471801842 | 65487,3205 | False

--------------------------------------------------------------------------------------------------

Librarian | Uniformity | 0,1 | 2893,140910202084 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Equiprobability | 0,01 | 244,45703125 | 307,5284 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Independence | 0,01 | 65357,60229037813 | 65863,8124 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Uniformity | 0,01 | 3529,996509895643 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Equiprobability | 0,05 | 244,45703125 | 292,1493 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Independence | 0,05 | 65357,60229037813 | 65618,2272 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Uniformity | 0,05 | 3529,996509895643 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Equiprobability | 0,1 | 244,45703125 | 283,9516 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Independence | 0,1 | 65357,60229037813 | 65487,3205 | True

--------------------------------------------------------------------------------------------------

BBS bytes | Uniformity | 0,1 | 3529,996509895643 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

BBS bits | Equiprobability | 0,01 | 243,611328125 | 307,5284 | True

--------------------------------------------------------------------------------------------------

BBS bits | Independence | 0,01 | 65214,07364769254 | 65863,8124 | True

--------------------------------------------------------------------------------------------------

BBS bits | Uniformity | 0,01 | 3514,4134941818256 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

BBS bits | Equiprobability | 0,05 | 243,611328125 | 292,1493 | True

--------------------------------------------------------------------------------------------------

BBS bits | Independence | 0,05 | 65214,07364769254 | 65618,2272 | True

--------------------------------------------------------------------------------------------------

BBS bits | Uniformity | 0,05 | 3514,4134941818256 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

BBS bits | Equiprobability | 0,1 | 243,611328125 | 283,9516 | True

--------------------------------------------------------------------------------------------------

BBS bits | Independence | 0,1 | 65214,07364769254 | 65487,3205 | True

--------------------------------------------------------------------------------------------------

BBS bits | Uniformity | 0,1 | 3514,4134941818256 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

BM bytes | Equiprobability | 0,01 | 258,609375 | 307,5284 | True

--------------------------------------------------------------------------------------------------

BM bytes | Independence | 0,01 | 65127,336748204165 | 65863,8124 | True

--------------------------------------------------------------------------------------------------

BM bytes | Uniformity | 0,01 | 3574,731309272961 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

BM bytes | Equiprobability | 0,05 | 258,609375 | 292,1493 | True

--------------------------------------------------------------------------------------------------

BM bytes | Independence | 0,05 | 65127,336748204165 | 65618,2272 | True

--------------------------------------------------------------------------------------------------

BM bytes | Uniformity | 0,05 | 3574,731309272961 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

BM bytes | Equiprobability | 0,1 | 258,609375 | 283,9516 | True

--------------------------------------------------------------------------------------------------

BM bytes | Independence | 0,1 | 65127,336748204165 | 65487,3205 | True

--------------------------------------------------------------------------------------------------

BM bytes | Uniformity | 0,1 | 3574,731309272961 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

BM bits | Equiprobability | 0,01 | 263,005859375 | 307,5284 | True

--------------------------------------------------------------------------------------------------

BM bits | Independence | 0,01 | 64936,23687588176 | 65863,8124 | True

--------------------------------------------------------------------------------------------------

BM bits | Uniformity | 0,01 | 3580,7266557587677 | 3766,54355914 | True

--------------------------------------------------------------------------------------------------

BM bits | Equiprobability | 0,05 | 263,005859375 | 292,1493 | True

--------------------------------------------------------------------------------------------------

BM bits | Independence | 0,05 | 64936,23687588176 | 65618,2272 | True

--------------------------------------------------------------------------------------------------

BM bits | Uniformity | 0,05 | 3580,7266557587677 | 3709,00006655 | True

--------------------------------------------------------------------------------------------------

BM bits | Equiprobability | 0,1 | 263,005859375 | 283,9516 | True

--------------------------------------------------------------------------------------------------

BM bits | Independence | 0,1 | 64936,23687588176 | 65487,3205 | True

--------------------------------------------------------------------------------------------------

BM bits | Uniformity | 0,1 | 3580,7266557587677 | 3678,32710353 | True

--------------------------------------------------------------------------------------------------

**Порівняння генераторів:**

На основі отриманих результатів, можна побачити, що найгіршим генераторами виявились Librarian та Wolfram, оскільки Librarian проходить лише тест на рівноімовірність, а Wolfram поводить себе досить непередбачувано, хоча в даному випадку показав гарні результати. Найкращими генераторами виявились BM, BBS, L89, L20 та вбудованний генератори, тому вони можуть використовуватись в криптографічних цілях.

**Висновок:**

В ході роботи ми навчилися методам побудови тестів для перевірки статистичних властивостей бінарних випадкових і псевдовипадкових послідовностей, а саме *критерій перевірки рівноімовірності знаків, критерій перевірки незалежності знаків* та *критерій перевірки однорідності двійкової послідовності.* Кожен з тестів проводився на послідовностях, згенерованих 12 різними генераторами, з 3 рівнями значимості.