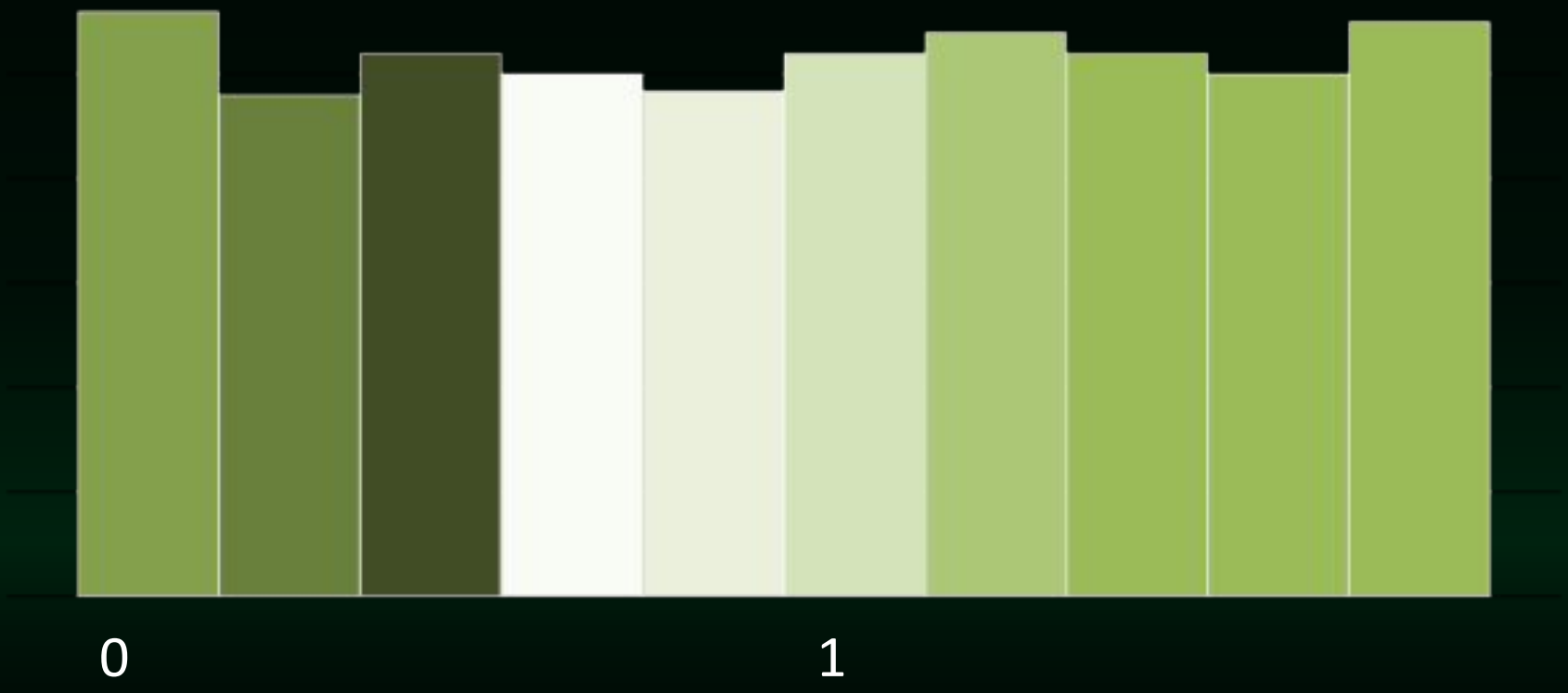
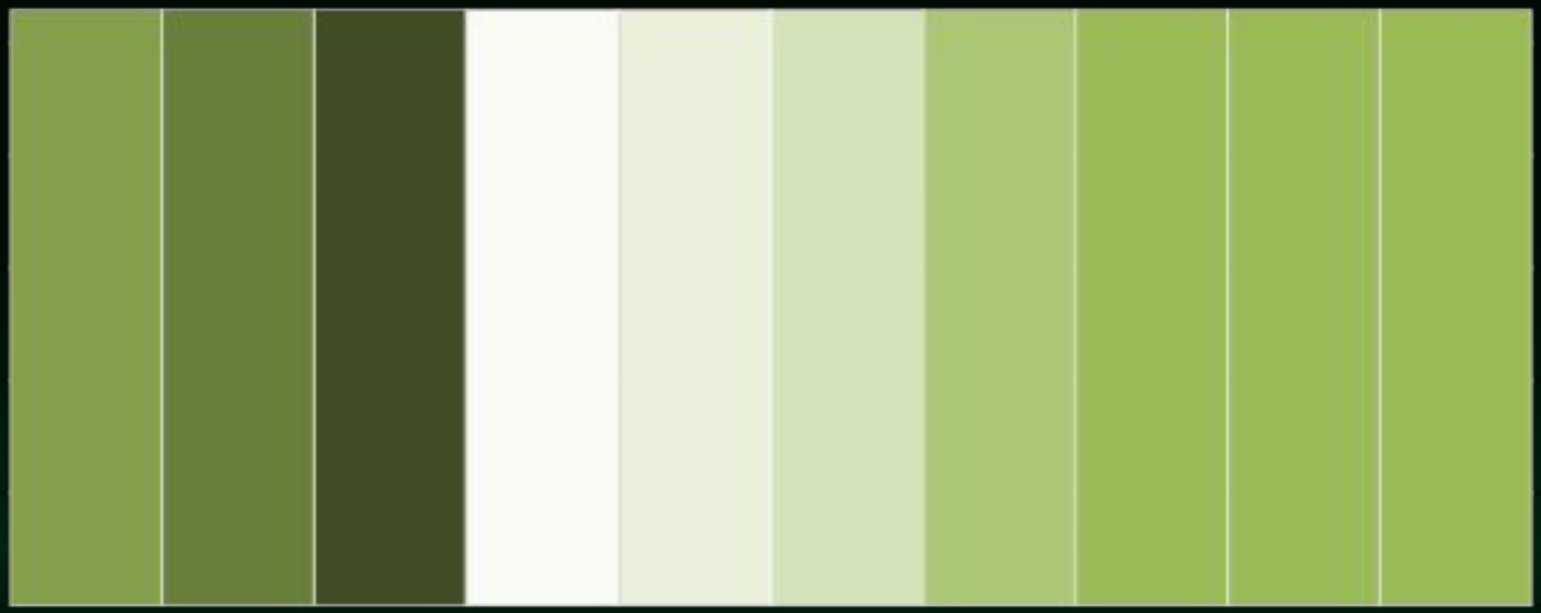
Генерация случайных чисел

Андрей Гейн

Эталон



Эталон



Генераторы

Генераторы

- физические

Генераторы

- физические
- табличные

Генераторы

- физические
- табличные
- алгоритмические

Первые алгоритмы

«Всякий, кто питает слабость к арифметическим методам получения случайных чисел, грешен вне всяких сомнений»

Джон фон Нейман

Первые алгоритмы

- Метод серединных квадратов

Первые алгоритмы

- Метод серединных квадратов

Первые алгоритмы

- Метод серединных квадратов

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений

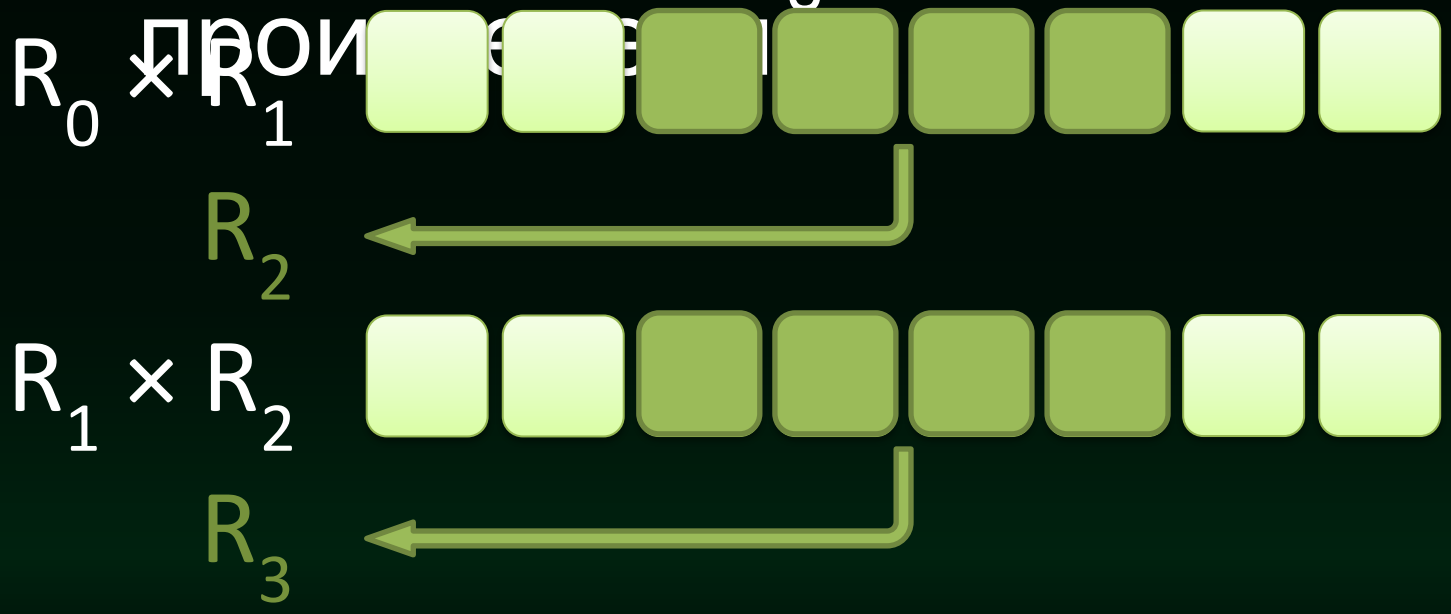
$R_0 \times R_1$ 

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений

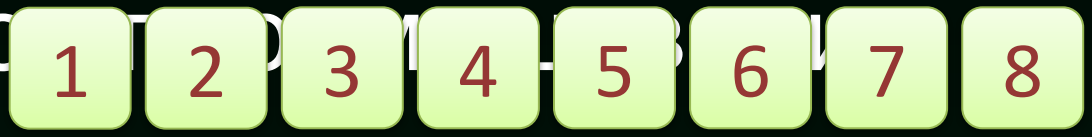


Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Метод перемешивания

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Мето[illegible]

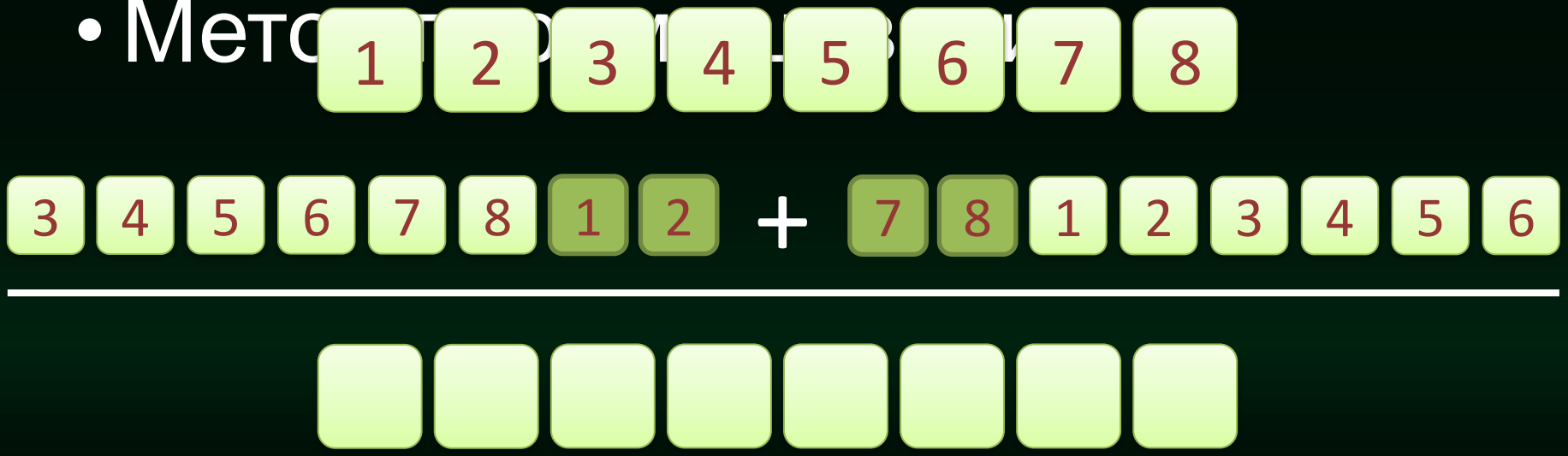


Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Мето[illegible]

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Мето[illegible]



Линейная конгруэнция

Линейная конгруэнция

$$R_{i+1} = (K * R_i + B) \% M$$

Линейная конгруэнция

$$R_{i+1} = (K * R_i + B) \% M$$

- B и M взаимно простые

Линейная конгруэнция

$$R_{i+1} = (K * R_i + B) \% M$$

- B и M – взаимно простые
- K – 1 кратно любому простому делителю M

Линейная конгруэнция

$$R_{i+1} = (K * R_i + B) \% M$$

- B и M – взаимно простые
- K – 1 кратно любому простому делителю M
- K – 1 кратно 4, если M кратно 4

Датчик Фибоначчи

Датчик Фибоначчи

$$R_i = R_{i-a} - R_{i-b}$$

Датчик Фибоначчи

$$R_i = R_{i-a} - R_{i-b}$$

- a, b – *лаги*

Датчик Фибоначчи

$$R_i = R_{i-a} - R_{i-b}$$

- a, b – *лаги*
- циклическая очередь значений

Датчик Фибоначчи

$$R_i = R_{i-a} - R_{i-b}$$

- a, b – *лаги*
- циклическая очередь значений
- $T = (2^{\max\{a, b\}} - 1) \cdot 2^l$

LFSR

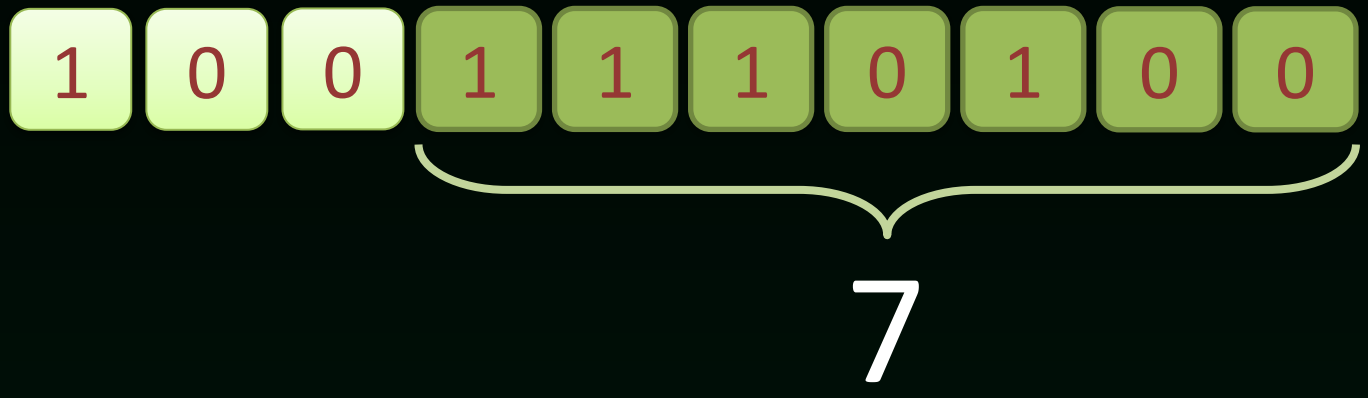
LFSR

$$R_i = (c_1 \times R_{i-1}) \oplus (c_2 \times R_{i-2}) \oplus \ldots \oplus (c_L \times R_{i-L})$$

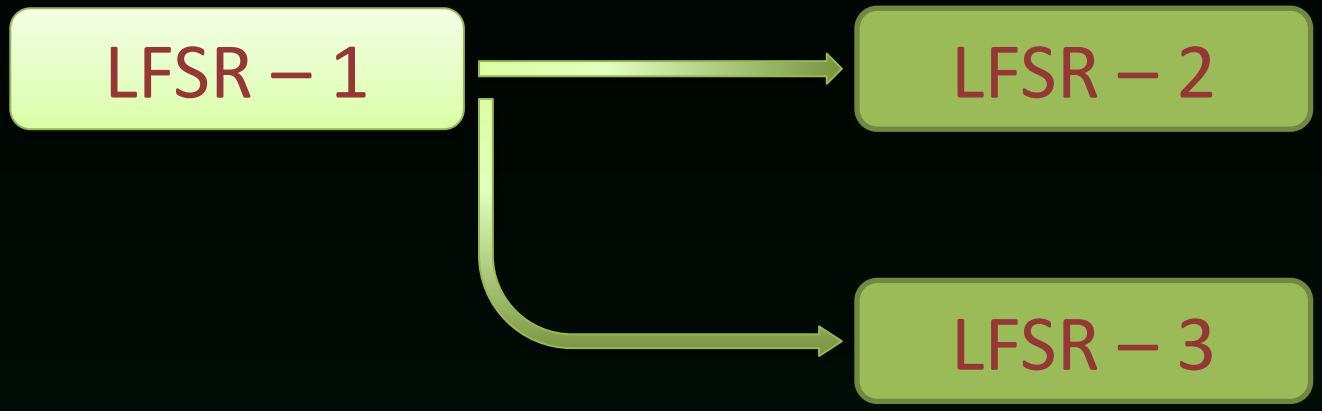
$$C(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_L x^L$$

LFSR

$x^3 + x + 1$

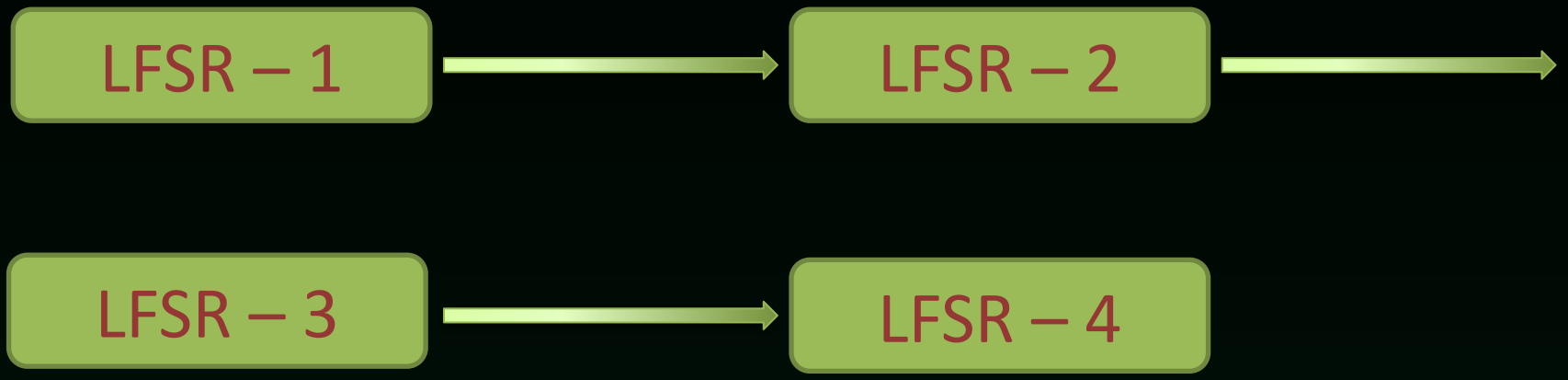


Стоп-пошел



⊕ = bit

Каскад Голлмана



Пороговый генератор

LFSR – 1

LFSR – 2

LFSR – 3

…

LFSR – K

Тестирование

Тестирование

NIST

pLab Project

DIEHARD

TEST-U01

Dieharder

Knuth’s

CRYPT-X

ENT

Тестирование

NIST

pLab Project

DIEHARD

TEST-U01

Dieharder

Knuth’s

CRYPT-X

ENT

NIST

NIST

Частотный побитовый тест

NIST

Частотный побитовый тест

Частотный блочный тест

NIST

Частотный побитовый тест

Частотный блочный тест

Последовательность одинаковых бит

NIST

Частотный побитовый тест

Частотный блочный тест

Последовательность одинаковых бит

Самая длинная последовательность единиц в блоке

NIST

Ранговый тест

NIST

Ранговый тест

Спектральный тест

NIST

Ранговый тест

Спектральный тест

Тест на шаблоны

NIST

Ранговый тест

Спектральный тест

Тест на шаблоны

Тест на пересекающиеся шаблоны

NIST

Ранговый тест

Спектральный тест

Тест на шаблоны

Тест на пересекающиеся шаблоны

Тест Маурера

NIST

Тест на линейную сложность

NIST

Тест на линейную сложность

Тест на периодичность

NIST

Тест на линейную сложность

Тест на периодичность

Тест приблизительной энтропии

NIST

Тест на линейную сложность

Тест на периодичность

Тест приблизительной энтропии

Тест кумулятивных сумм

DIEHARD

DIEHARD

Тест на парковку

DIEHARD

Тест на парковку

Тест сжатия

DIEHARD

Тест на парковку

Тест сжатия

Тест игры в кости

Криптостойкость

Криптостойкость

- Генерация ключей

Криптостойкость

- Генерация ключей
- Одноразовые случайные числа

Криптостойкость

- Генерация ключей
- Одноразовые случайные числа
- Одноразовые шифроблокноты

Криптостойкость

- Генерация ключей
- Одноразовые случайные числа
- Одноразовые шифроблокноты
- Генерация соли

Криптостойкость

- Тест на следующий бит

Криптостойкость

- Тест на следующий бит
- На основе блочного шифра

Криптостойкость

- Тест на следующий бит
- На основе блочного шифра
- На основе хеш-функции

Криптостойкость

- Тест на следующий бит
- На основе блочного шифра
- На основе хеш-функции
- Алгоритм Блюма — Блюма — Шуба

$$x_{n+1} = x_n^2 \bmod M$$

Криптостойкость

- Тест на следующий бит
- На основе блочного шифра
- На основе хеш-функции
- Алгоритм Блюма — Блюма — Шуба
- Алгоритм Блюма — Микали

Аппаратные генераторы

Аппаратные генераторы

- Lavarand

Аппаратные генераторы

- Lavarand
- Чипы в процессоре (3 Гб/сек)

по

ПО

- gLib – вихрь Мерсена

ПО

- gLib – вихрь Мерсена
- Java – Random, SecureRandom

ПО

- gLib – вихрь Мерсена
- Java – Random, SecureRandom
- C# - Random, Cryptography.RNG

ПО

- gLib – вихрь Мерсена
- Java – Random, SecureRandom
- C# - Random, Cryptography.RNG
- RFC 1750

Продолжи ряд 😊

1 0 0 1 1 0 1 0 0 1 0 0 0 1 1 0 1 1 1 0 0
1 0 1 1 0 1 1 0 0 0 1 0 1 1 0 0 1 1 0 0 1
0 0 1 0 1 0 0 1 ...