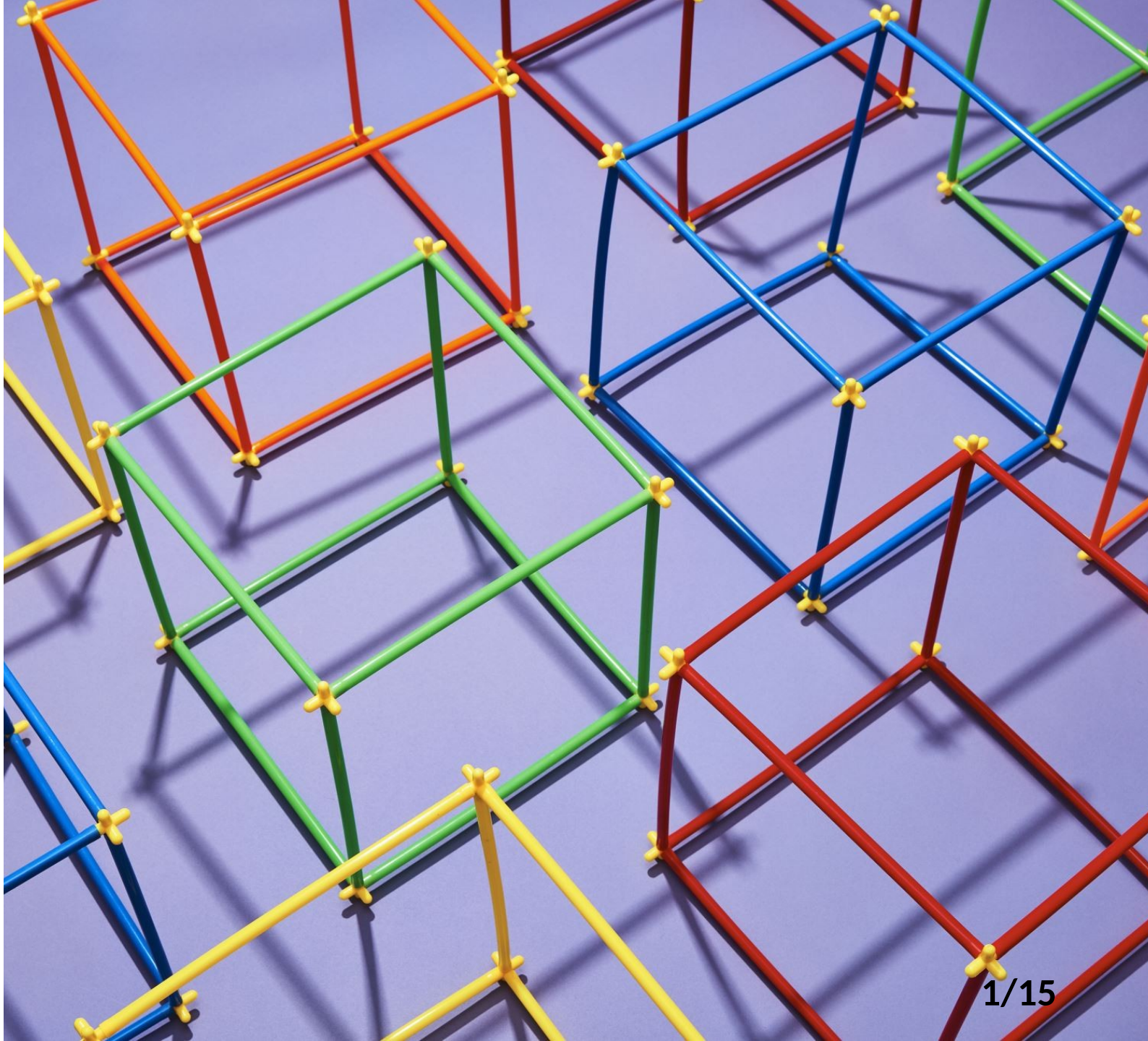
RANDOMNESS

Yağmur GÖKTAŞ

Discrete Computational Structures

20.11.2019 / WEDNESDAY



DEFINING RANDOMNESS

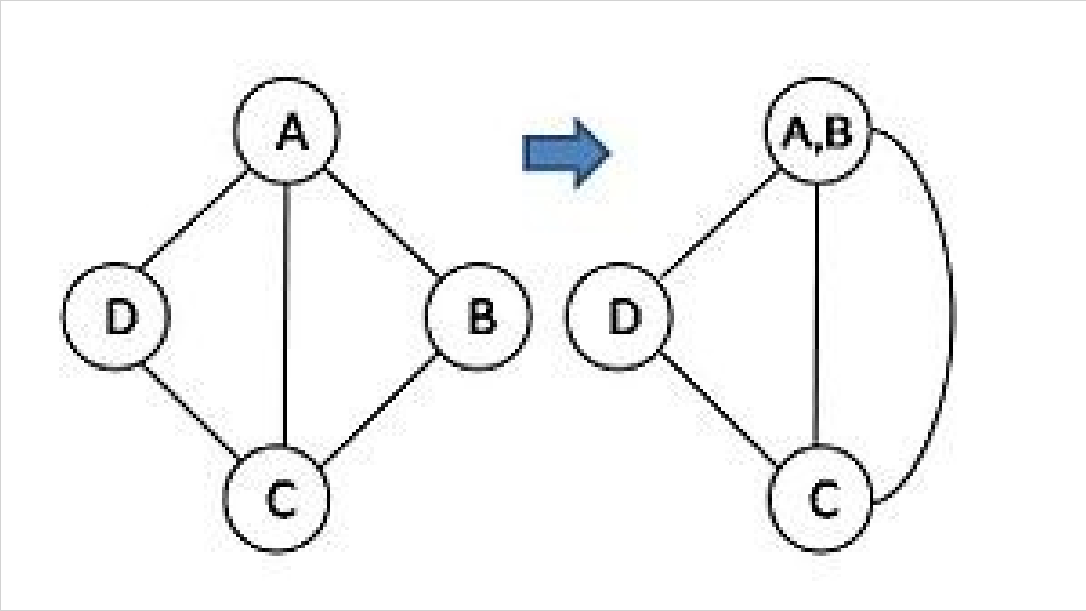
- Random sequence cannot conceal any rule that would enable us to recreate the sequence, while on the other hand, requiring the absence of all patterns within a sequence leads to a very restricting definition which is almost impossible to apply in practice.

RANDOMNESS IN COMPUTER SCIENCE

There are two main approaches to generating random numbers using a computer: Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs).

PSEUDO-RANDOM NUMBER GENERATORS

- PRNGs are algorithms that use mathematical formulae or simply precalculated tables to produce sequences of numbers that appear random. A good example of a PRNG is the linear congruential method.
-



LINEAR CONGRUENTIAL METHOD(OLDEST AND COMMON)

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

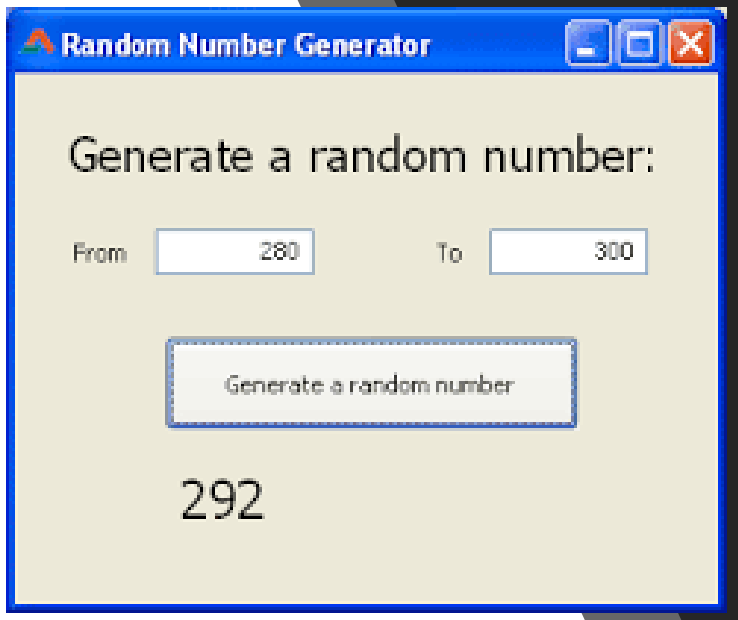
$\mathbf{X_{n+1} = (aX_n + c) \bmod m}$ where X is the sequence of pseudo-random values

m,0 < m - modulus

a, 0 < a < m - multiplier

c, 0 ≤ c < m - increment

x_0, 0 ≤ x_0 < m - the seed or start value



- PRNGs are *efficient*, meaning they can produce many numbers in a short time, and *deterministic*, meaning that a given sequence of numbers can be reproduced at a later date if the starting point in the sequence is known. Efficiency is a nice characteristic if your application needs many numbers, and determinism is handy if you need to replay the same sequence of numbers again at a later stage. PRNGs are typically also *periodic*, which means that the sequence will eventually repeat itself.

TRUE-RANDOM NUMBER GENERATORS

- In comparison with PRNGs, TRNGs extract randomness from physical phenomena and introduce it into a computer. The characteristics of TRNGs are quite different from PRNGs.

- First, TRNGs are generally rather *inefficient* compared to PRNGs, taking considerably longer time to produce numbers. They are also *nondeterministic*, meaning that a given sequence of numbers cannot be reproduced, although the same sequence may of course occur several times by chance. TRNGs have no period.

SAMPLE OF THE REAL-WORLD SOURCES OF TRUE RANDOMNESS

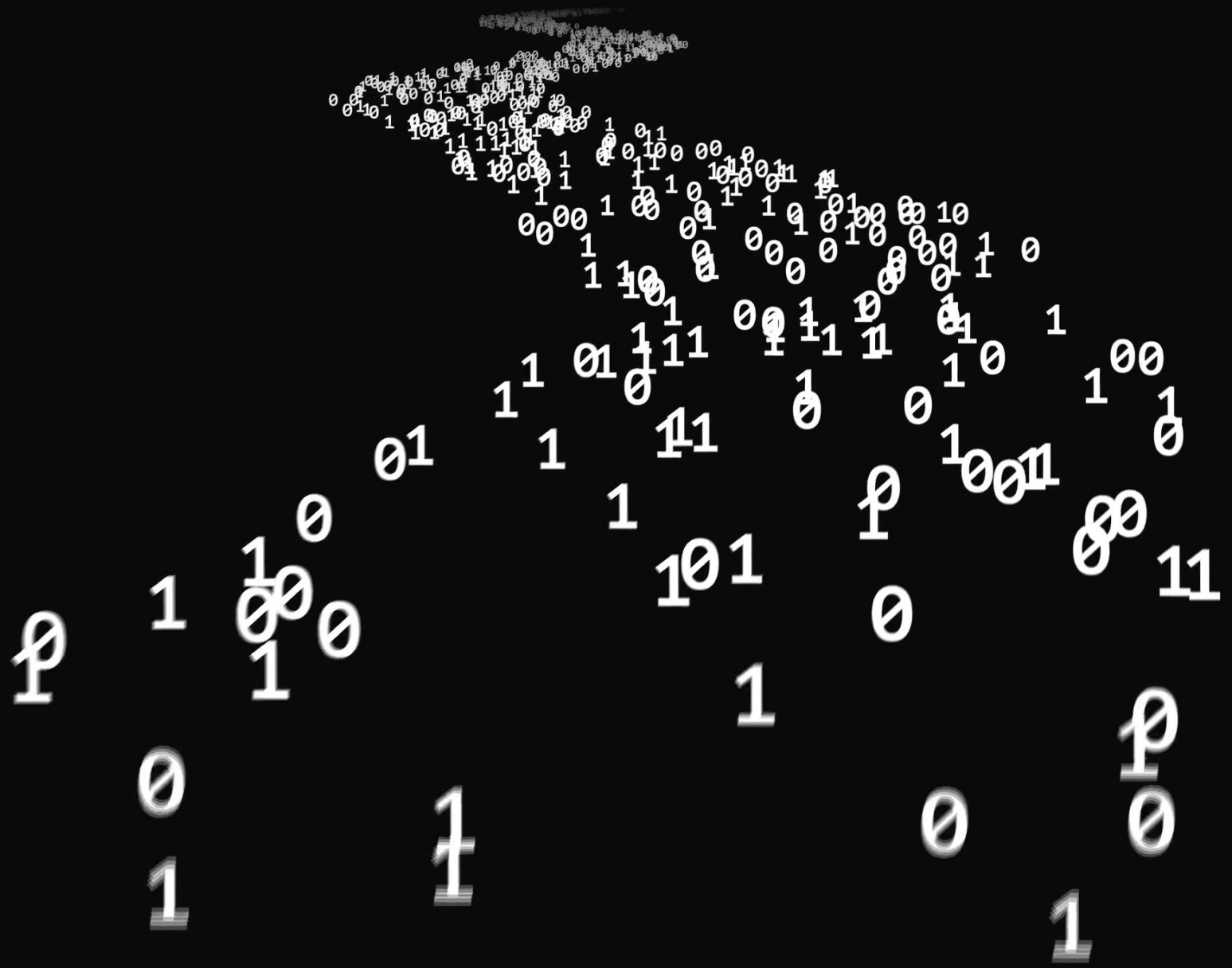
- Athmospheric Noise
- Dice
- Radioactivity
- Lasers
- Lava Lite

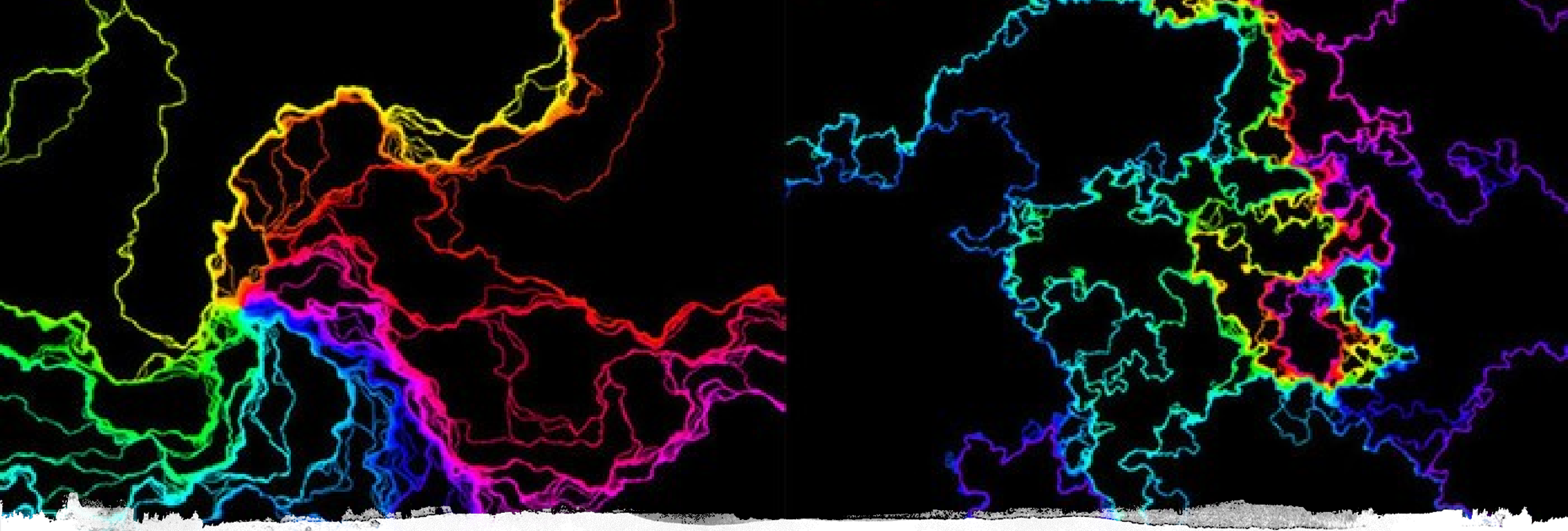
.

.

.

Characteristic	Pseudo-Random Number Generators	True Random Number Generators
Efficiency	Excellent	Poor
Determinism	Deterministic	Nondeterministic
Periodicity	Periodic	Aperiodic





RANDOMNESS IS THE KEY TO COMPUTER SECURITY

One of the best examples of randomness being used for good when it comes to computer security is your password. Passwords that tend to use the same format are easy to guess. That is why you are always told to mix it up when you create a password.

- Another good example of randomness when you are talking about computer security is how you set your system up. When a lot of system administrators set up their systems they will use the default names that already installed on the machines.

References

- https://sci-highs.com/what-is-randomness/
- https://www.sciencedirect.com/science/article/pii/B9780444518620500204
- https://www.quantamagazine.org/how-randomness-can-arise-from-determinism-20191014/
- https://www.random.org/randomness/