Сумський державний університет

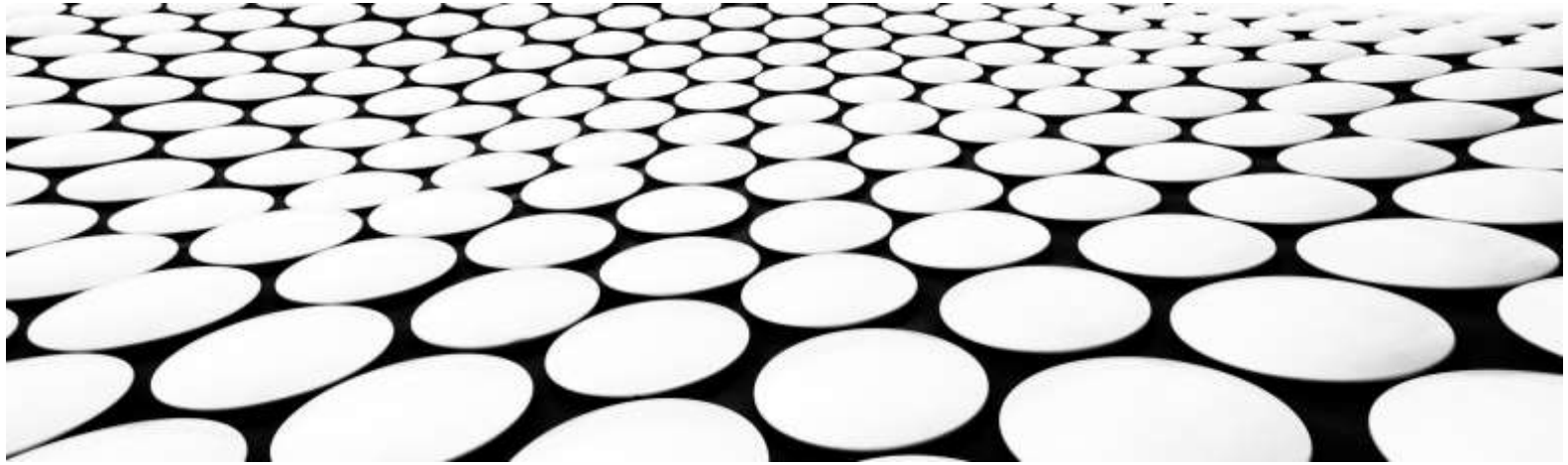
Кафедра кібербезпеки

ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ ТА ЇХ ЗАСТОСУВАННЯ В КІБЕРБЕЗПЕЦІ

АВТОРИ:

ЛАВРИК ТЕТЯНА ВОЛОДИМИРІВНА, ВИКЛАДАЧ КАФЕДРИ КІБЕРБЕЗПЕКИ

СОРОЧЕНКО МАКСИМ, ТОВОЛЖАНСЬКИЙ ЗАХАР , СТУДЕНТИ ДРУГОГО КУРСУ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»



ВСТУП

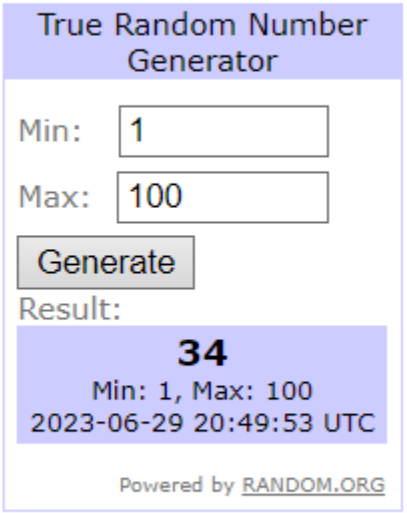
1. Приклади використання випадкових чисел.
2. Випадкові послідовності чисел.
3. Псевдовипадкові послідовності чисел.

RANDOM.ORG

What's this fuss about *true* randomness?

Perhaps you have wondered how predictable machines like computers can generate randomness. In reality, most random numbers used in computer programs are *pseudo-random*, which means they are generated in a predictable fashion using a mathematical formula. This is fine for many purposes, but it may not be random in the way you expect if you're used to dice rolls and lottery drawings.

RANDOM.ORG offers *true* random numbers to anyone on the Internet. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. People use RANDOM.ORG for holding drawings, lotteries and sweepstakes, to drive online games, for scientific applications and for art and music. The service has existed since 1998 and was built by Dr Mads Haahr of the School of Computer Science and Statistics at Trinity College, Dublin in Ireland. Today, RANDOM.ORG is operated by Randomness and Integrity Services Ltd.



ПРИКЛАДИ

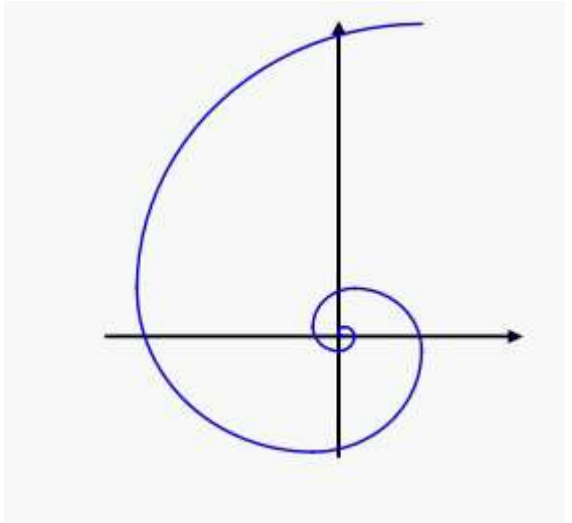
- ✓ Генерація стійких паролів (менеджери паролів - https://www.ukraine.com.ua/info/tools/passwdgenerate/).
- ✓ Генерація ключів для шифрування даних.
- ✓ Безпечне надсилання повідомлень в месенджерах (наприклад, Telegram).
- ✓ Безпека на пристроях Інтернету речей (Internet of Things, IoT).
- ✓ Розробка ігор.

ПОГРАЄМО!

ПРОДОВЖИТИ ПОСЛІДОВНІСТЬ …

1) 2 22 42 62 **82**

2) 1 1 2 3 5 8 13 21 **34** -
Послідовність Фібоначчі



3) 10 25 4 27 14 10 25 **4**

4) 6 1 8 11 26 5 28 **15 14 9 16 19 2**

ВИПАДКОВІ ТА ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ

Що таке випадкова послідовність чисел?

73 22 94 63 78

4 10 1 5 7

8 13 25 38 51

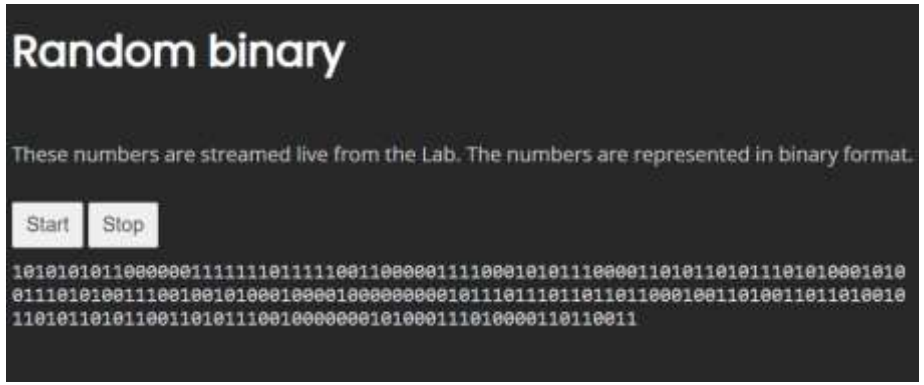
Яким чином отримати випадкову послідовність чисел?

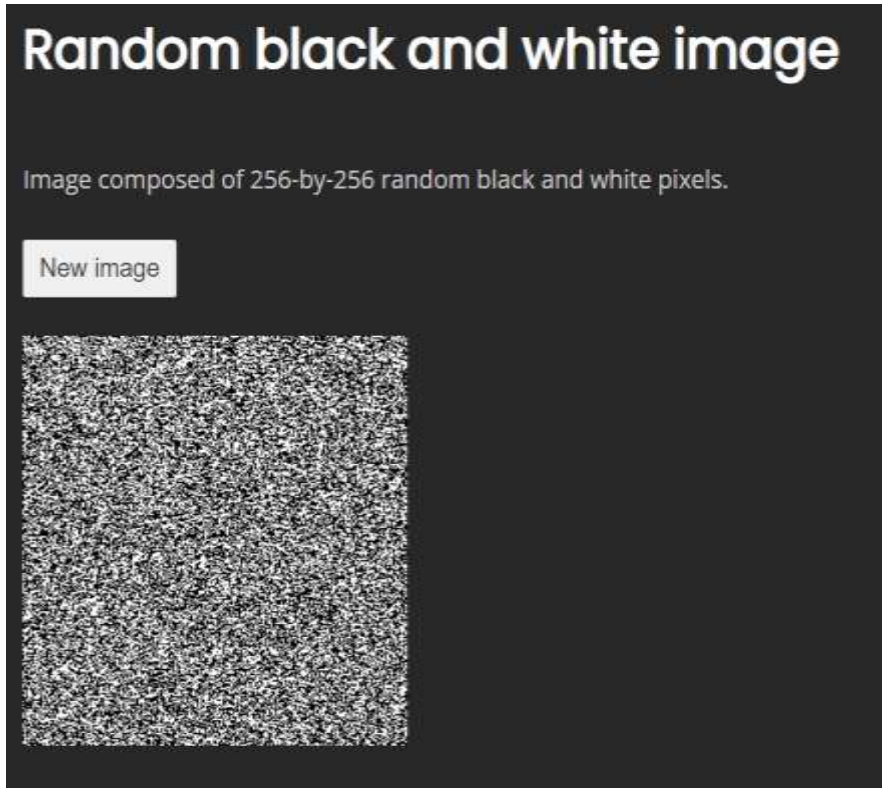
0 1 0 0 0 1,

де 0 — герб, 1 — вензель

ВИПАДКОВІ ТА ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ

Вимірюючи коливання у вакуумі можна генерувати випадкові числа в режимі реального часу з високою швидкістю https://qrng.anu.edu.au/





ВИПАДКОВІ ТА ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ

CloudFlare використовує стіну лавових ламп для генерації випадкових чисел за рахунок руху речовини в лавових лампах.

Лампи з проекту Lavarand

ВИПАДКОВІ ТА ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ

Що таке псевдовипадкова послідовність чисел?

5 16 0 4 78 5 16

Яким чином отримати псевдовипадкову послідовність чисел?

Приклад:

$X_{n+1} = X_n * 3 - X_n / 2$

$X_0 = 5$

$X_1 = 5 * 3 - 5/2 = 12{,}5$

$X_2 = 12{,}5 * 3 - 12{,}5/2 = 31{,}25$

$X_3 = 31{,}25 * 3 - 31{,}25/2 = 78{,}125$

ПІДВОДИМО ПІДСУМКИ

Дякуємо за увагу!