



Des lampes à lave pour sécuriser Internet

Thibault Meunier
Research Engineer
Cloudflare



Colissimo



Votre colis  arrive ce jour. Il sera remis contre code 383747. RDV sur sms.laposte.fr/AFCj9.

Create New World

Seed for the world generator

4206996

Leave blank for a random seed

Generate Structures: ON

World Type: Default

Villages, dungeons etc.

Bonus Chest: OFF

Import Settings

Done

Create New World

Cancel

RUGBY WORLD CUP FRANCE 2023

CHAPEAU 1

UE DU SUD

LE-ZÉLANDE

LETERRE

DE GALLES

CHAPEAU 2

IRLANDE

AUSTRALIE

FRANCE

JAPON

CHAPEAU 3

ÉCOSSE

ARGENTINE

FIDJI

ITALIE

CHAPEAU 4

OCÉANIE 1

EUROPE 1

AMÉRIQUES 1

ASIE / PACIFIQUE 1

CHAPEAU 5

AFRIQUE 1

EUROPE 2

AMÉRIQUES 2

VAINQUEUR DU TOURNOI FINAL

#RWC2023



RANDOM.ORG

Search RANDOM.ORG

Search

True Random Number Service

Advisory: Historical results for the Third-Party Draw Service are currently unavailable. We are working on bringing them back.

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,

True Random Number Generator

Min: 1

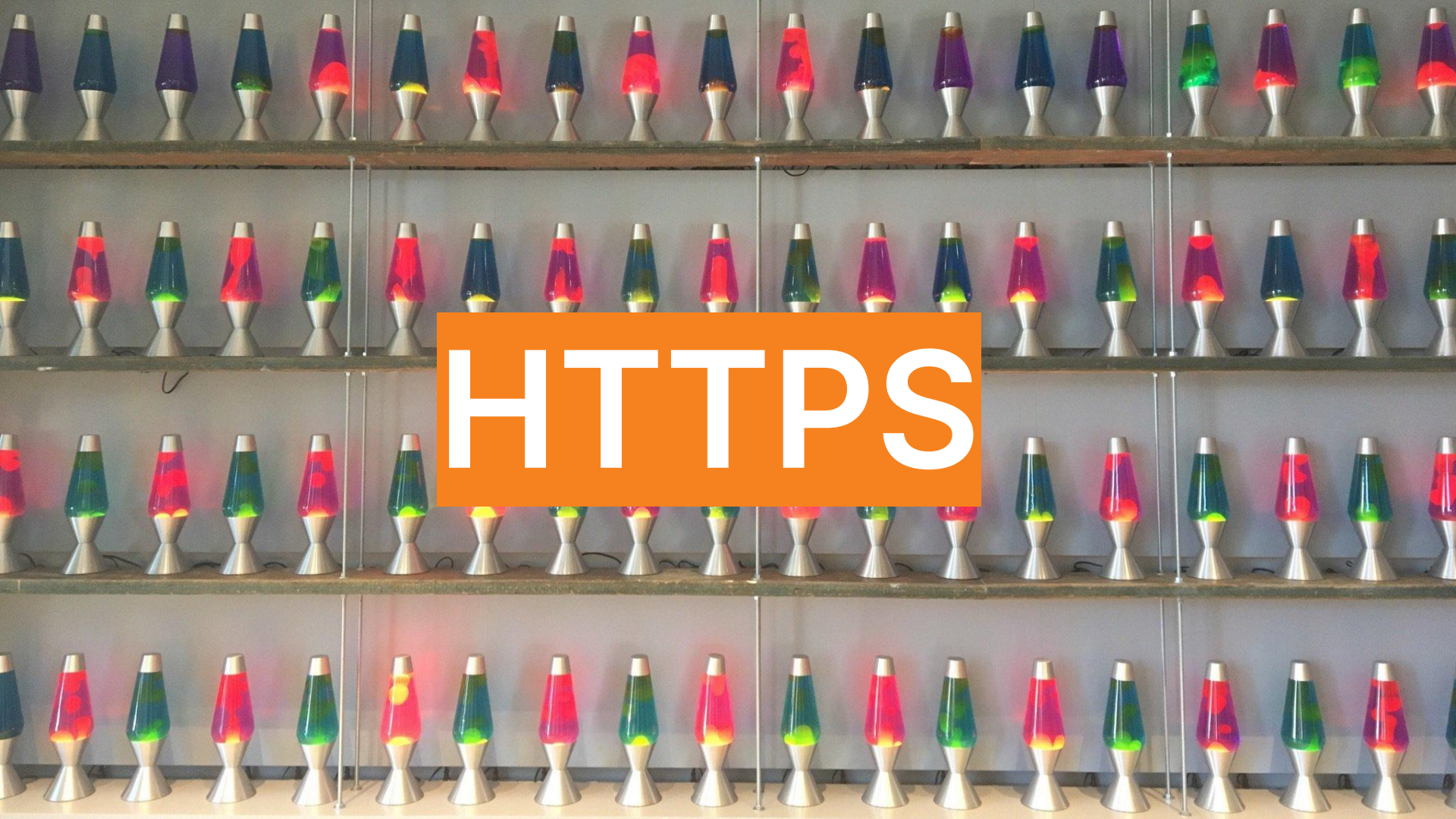
Max: 100

Generate

Result:

Powered by RANDOM.ORG



The image features a dense grid of approximately 100 lava lamps arranged in four rows and many columns. Each lamp is a classic teardrop shape with a silver-colored metal base and a clear glass body. Inside the glass, there are various combinations of bright colors like red, blue, green, and yellow, which are separated into distinct, rounded blobs. The lamps are illuminated from within, causing the colors to glow. The lamps are sitting on a light-colored wooden surface, and the background is a plain, light-colored wall. In the center of the image, there is a large, solid orange rectangle. Overlaid on this rectangle is the text "HTTPS" in a bold, white, sans-serif font. The text is centered both horizontally and vertically within the orange box.

HTTPS

Agenda

- 1 Base de chiffrement
- 2 Génération de l'aléatoire
- 3 Du code
- 4 Aller plus loin

Base de chiffrement

Le drop de TLS

cheveu, x...	2737
chez...	1040
chi...	438
chiffr, e, e, r, s...	1315
choi, x; si, e, r, s, t...	2249
choler, a; ique, s...	1091
chose, s...	486
chrétien, ne, s...	2437
chu...	1510
ci, r, s...	2379
cieu, x, se, s, m ^t ...	917
circonscri, t, e; re; ption, s...	271
circonspect, e, s; ion...	992
circonstanc, e; ié, e, s...	1707
circul, e, r; aire, s...	2398
cit, e, e, r; ation, s...	515
citoyen, s...	1710
civilis, e, e, r, s; ation...	2881
cl...	1143
cla, i, r, e, s, m ^t ; rté...	1811
clameur, s...	2594
class, e, e, r, s...	57
clandestin, e, s, m ^t ...	901

commerc, e; ial, e, s;iaux...	2303
comm, ettre; is, e, s, ion, s...	110
commissa, ire, s...	1326
commissaire, s de police...	2841
commissaire, s de surveillance administrative...	94
commun, e, s, m ^t ...	11 1247
communa, l, e, s; u, x...	2318
communi, qu, e, e, r; cation, s...	510
communiquer...	2861
compagn, e, e, r; ie, s...	1073
compar, aître; u, e, s...	115
compat, ib, le, ilité, s...	2342
compét, ent, e, s; ence...	729
compétit, eur, s...	149
complém, ent, aire, s...	2986
complet, e, e, r, s, m ^t ...	1717
compli, qu, e, e, r; cation, s...	224
complicité...	2004
complot, e, e, r, s...	1017
compos, e, e, r; ition, s...	81
compr, en, d, re; is, e, s...	1265
compréhensi, b, le, s, ilité...	2008
comprom, ettre; is, e, s...	380



Alice



Bob



Alice



Bob



Alice



Bob



Eve

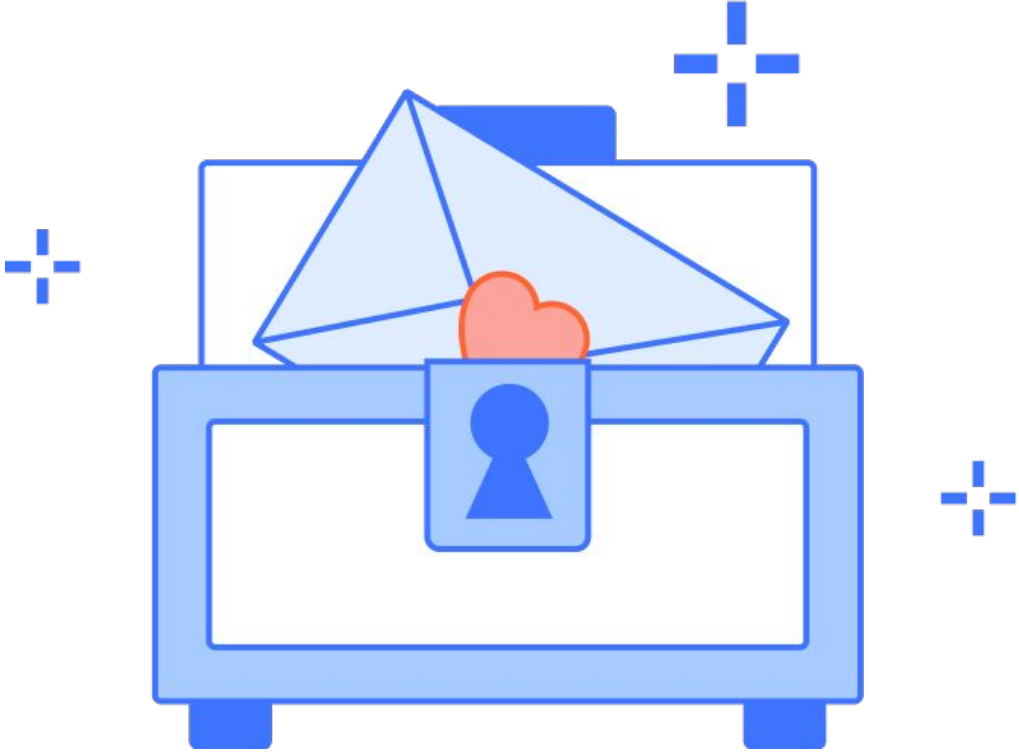


Alice



Bob





Comment partager la clé?



Des clés secrètes



Alice



Bob

Alice met son cadenas

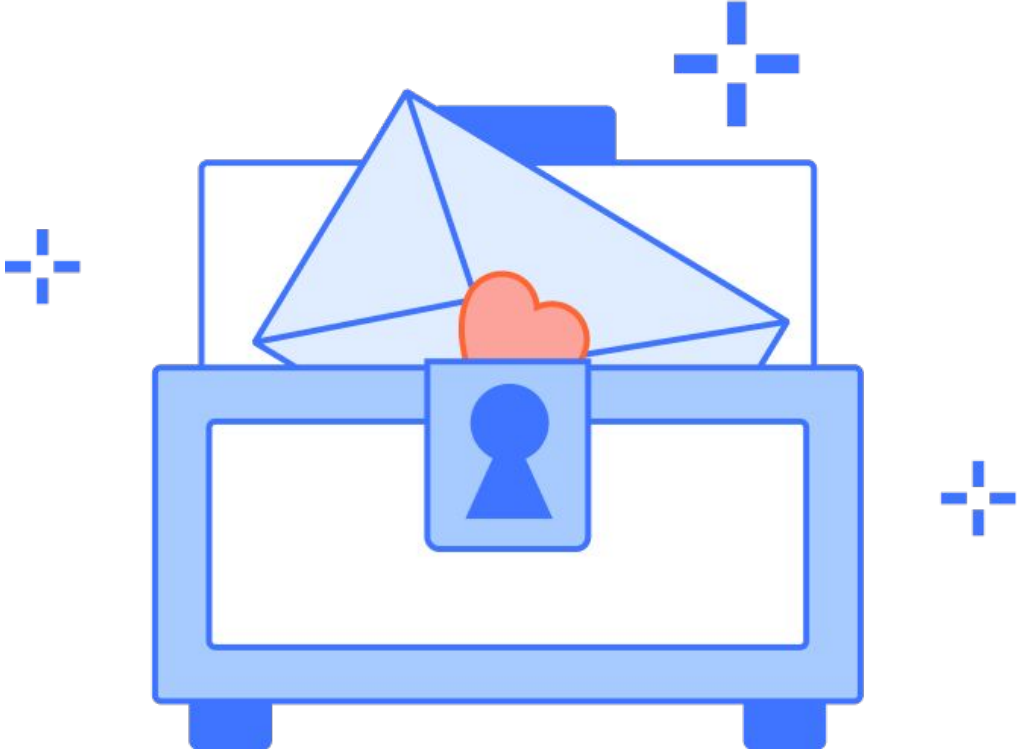


Bob rajoute le sien



Alice enlève son cadenas



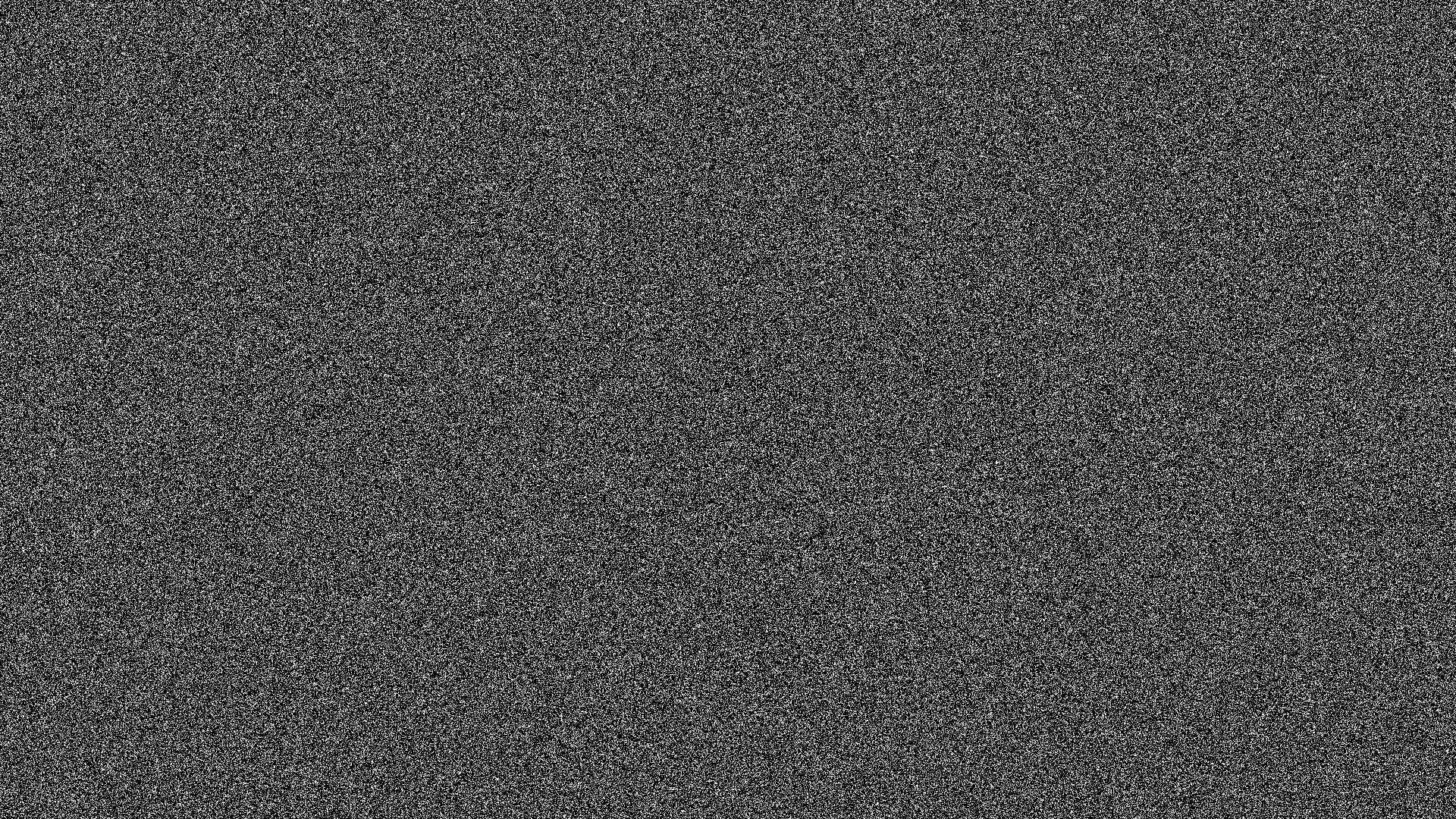


Des clés uniques

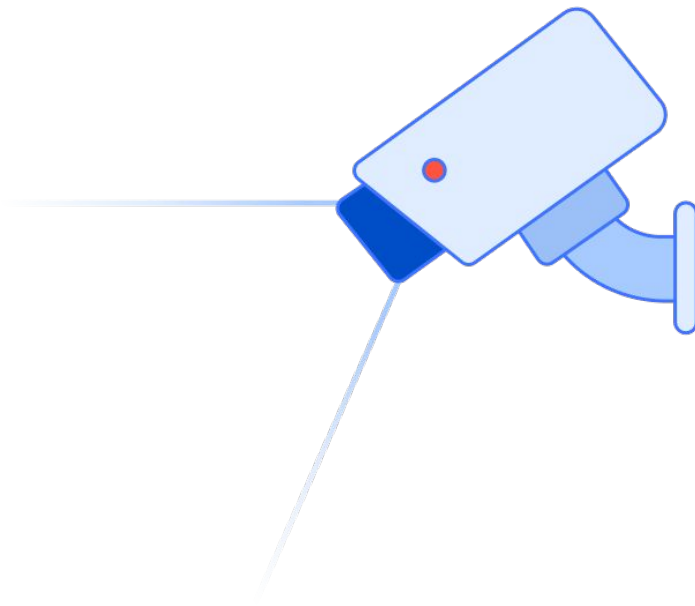


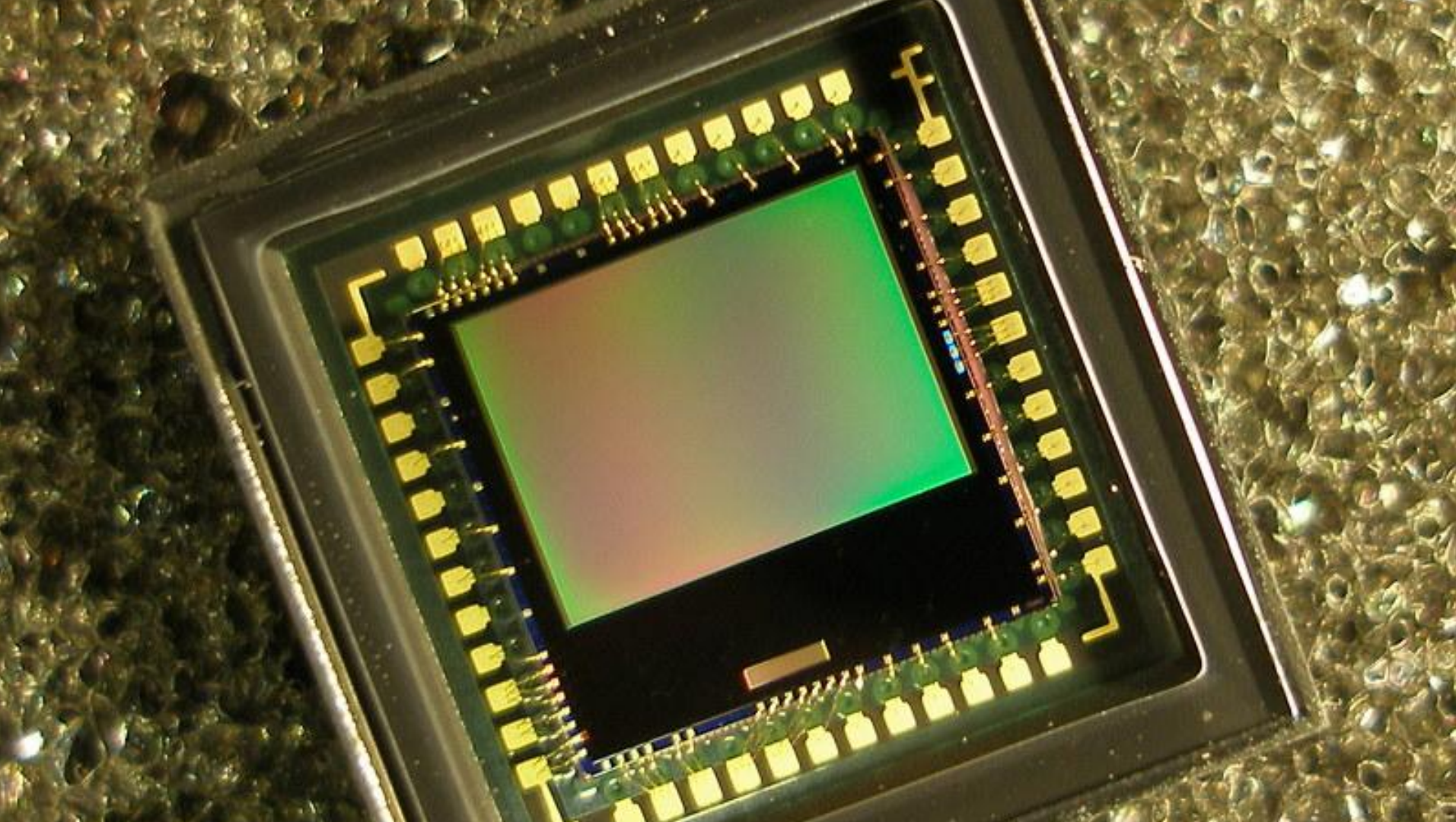
Génération d'aléatoire

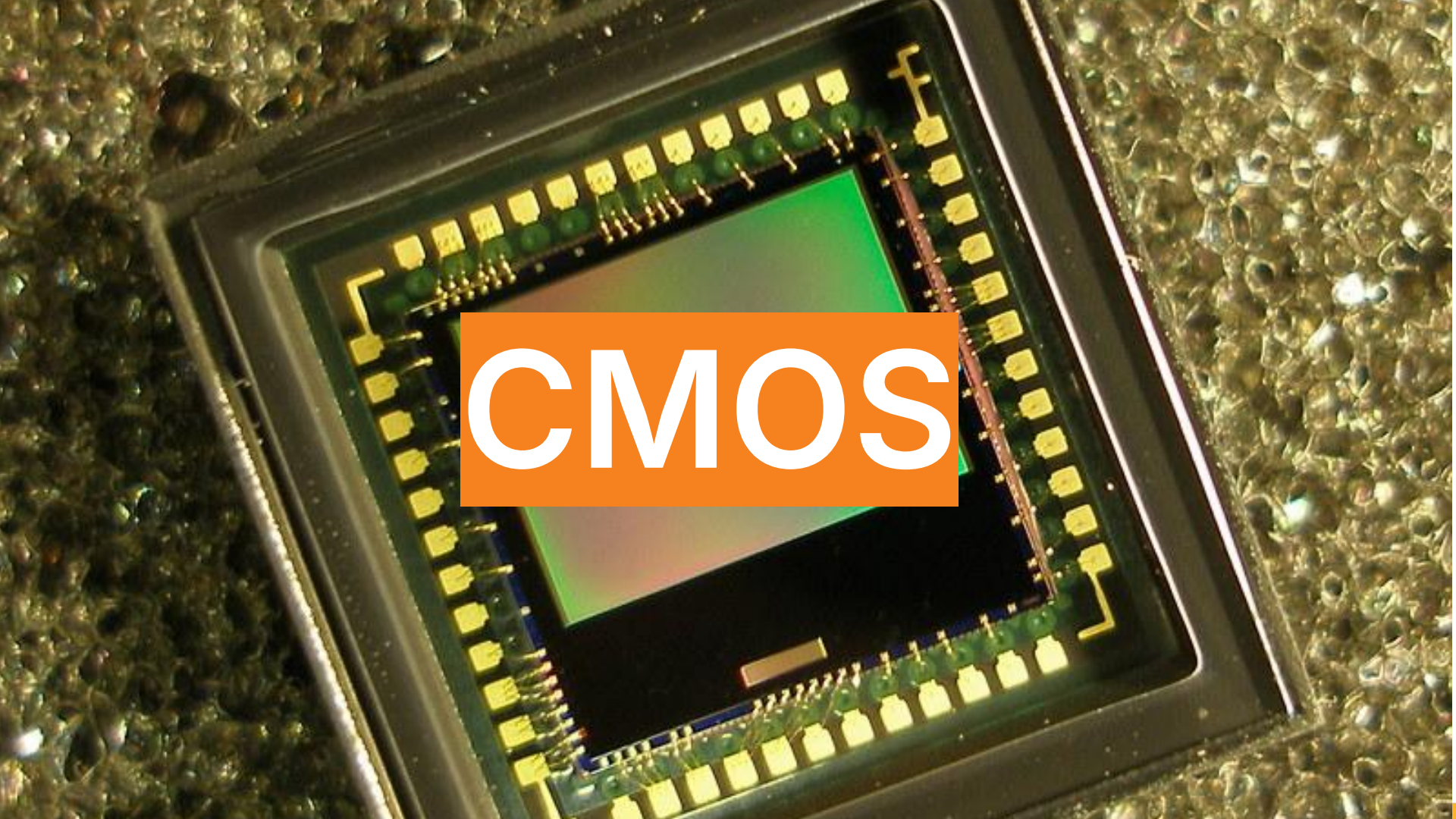
Faites du bruit



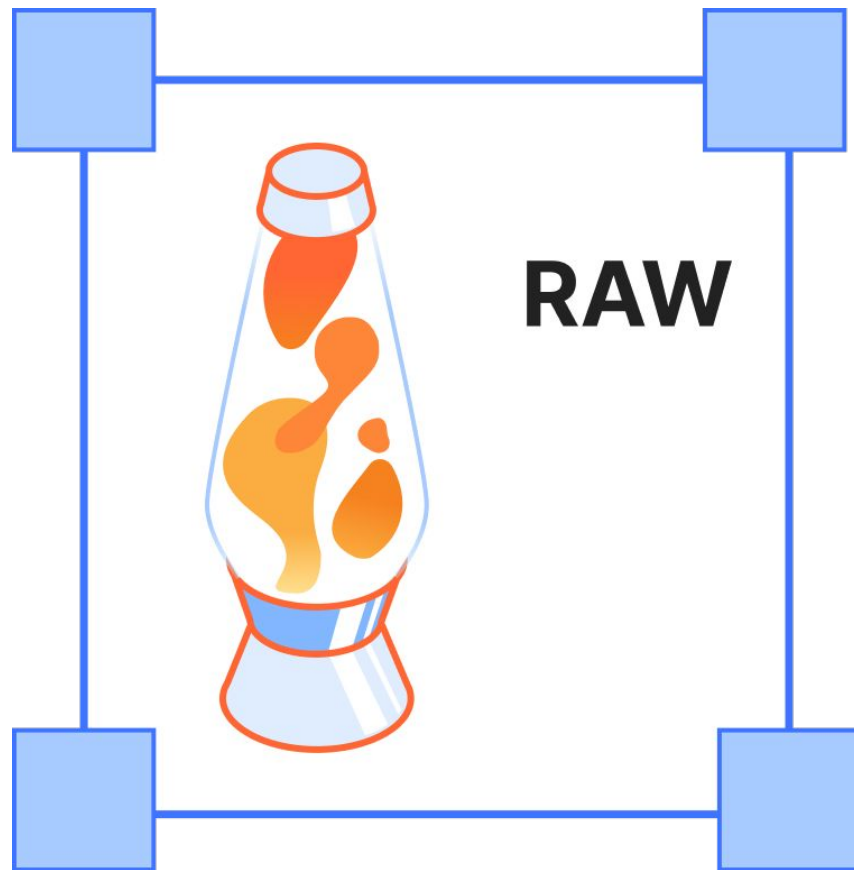


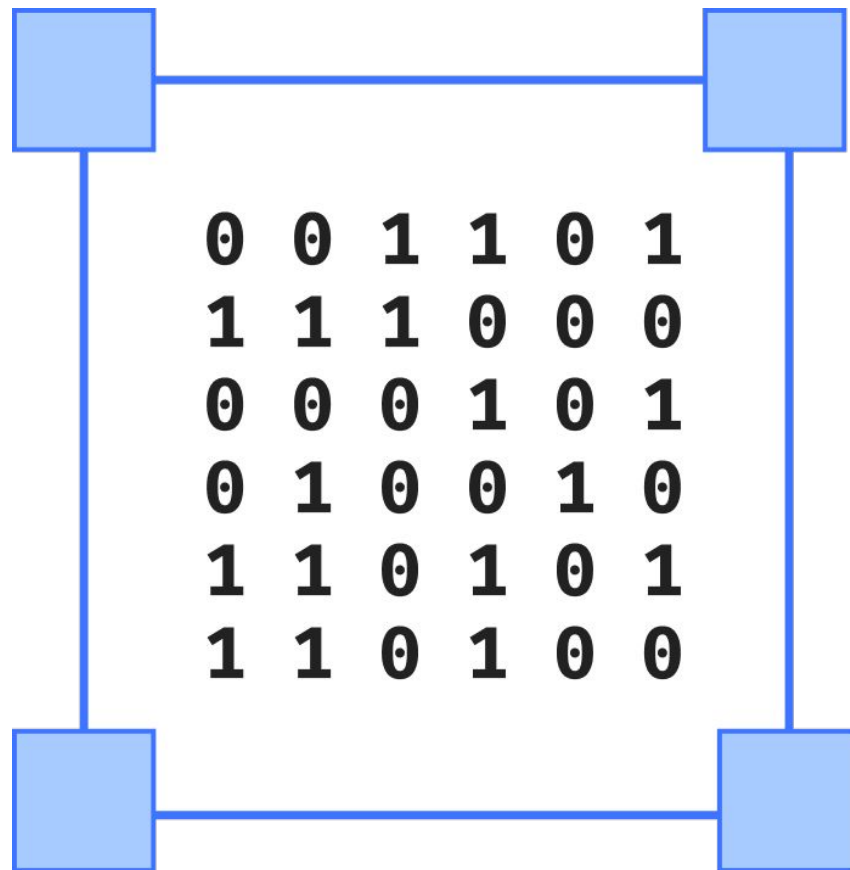






CMOS







Générer de nouveaux nombres

Utilisation d'un CSPRNG

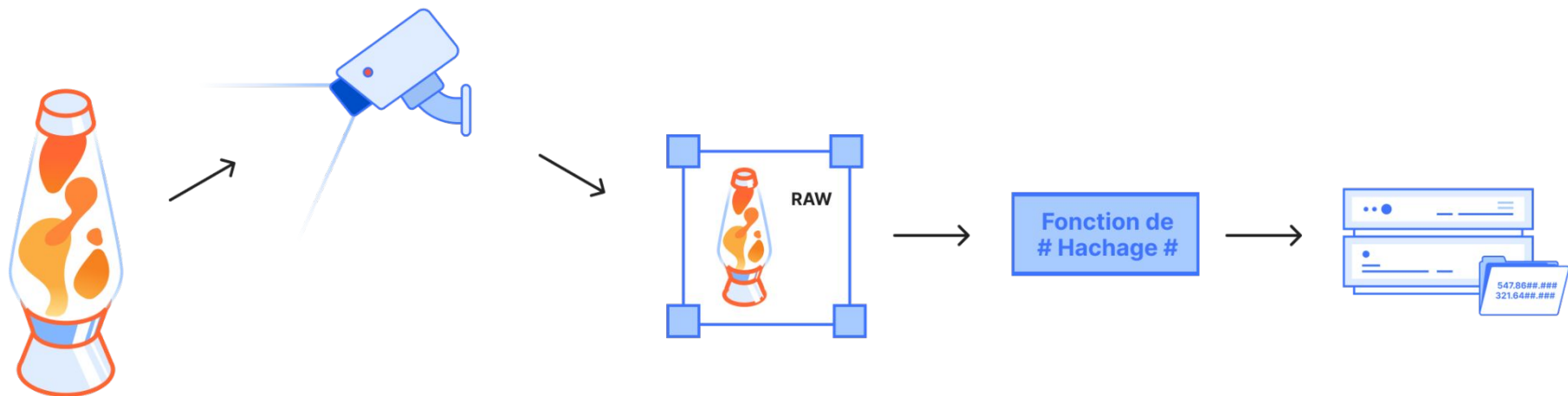
*Cryptographically secure
pseudorandom number generator*

Par exemple

[RFC 7539](#) - ChaCha20 and Poly1305



Vue d'ensemble



Initialisation terminée



Du code

10010010000001

Récupérer l'entropie

```
$ curl 'https://drand.cloudflare.com/public/latest'
{
  round: 5420711,
  signature:
"954e9fd69dd933fd84926b4be5f722e04901dc6860c09f4838e60ac11601696932278219e4ba9c27396
77de62e446cb5140bb29dedf0e115eb0506fc863a0d79eacf063cce0efcca3c962caeb6f0c545a30ad08
60817dfd6f82c70b18a77fa17",
  previous_signature:
"b162fea7e6edaff963b9bf1069e22f9531bc571eae8ccece3b7739735c7128c711f752c981fcef17760
8995b0e17b1c60820974df3fc477c2c015d113e5da7f2e4b8dd0f1b97a94bc0ef04e6cb3cfee4deba88e
1ac75d7f61fefde13ffbcf6b4",
  randomness: "db582af3e4a690fc9598cef8afa0241affc05a548787fd8513ef24f9f60d74db"
}
```

En une seule ligne de commande

```
$ cargo install dee
Ignored package **dee v0.0.16** is already installed

$ dee remote add quicknet "https://drand.cloudflare.com/52db..."
quicknet

$ dee rand -u quicknet
8998bdb919b2c5eb5f5a688f24532f523f486eaf7b6b481cf6354b4ac059e16d
```

Sur votre machine

Bash

```
RANDOM=$(dee get --format json | jq -r '.randomness')  
echo "$RANDOM $RANDOM $RANDOM"
```

Python

```
import random  
random.seed(int("dee-randomness", 16))  
print(random.random())  
print(random.random())  
print(random.random())
```


Aller plus loin

C'est pour vous à la maison

En résumé

Internet repose sur des **clés secrètes**

Ces clés doivent être **imprévisible**

L'aléatoire est donc au coeur de la sécurité en ligne



Plus de ressources

Aléatoire

[Tirer parti du chaos dans les bureaux de Cloudflare](#) - Cloudflare (Blog)

[La ligue d'entropie](#) - Cloudflare (Blog)

[The Randomness crisis threatening the Internet](#) - Be Smart (Video)

[How the Minecraft seed was found](#) - SalC1 (Video)

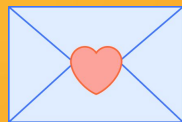
Securité Internet

La fin du cadenas - [Chrome](#) & [Safari](#) (Article)

[crypto/tls](#) - Mainteneurs Go (Code)

[Diffie Hellman](#) - Wikipedia (Article)

Merci



thibmeu.com



thibmeu



thibmeu.com/pdf/lava-lamps.pdf