

Sécurité des Applications

Septembre 2020 | **Serie 2**

Stéphane Küng

1 Administratif

Ce travail **individuel** doit être rendu avant la date indiquée sur le ScoreBoard au format **PDF** sur CyberLearn.

2 Exercices 2 - Randomness

2.1 Nuclear Warhead code generator

Le code suivant a été trouvé lors du démantèlement d'un ancien sous-marin d'une puissance étrangère.

```
1  // Nuclear Warhead code generator
2
3  #define NB_NUM 10
4  #define MIN_NUM 1
5  #define MAX_NUM 9
6
7  #include <stdio.h>
8  #include <stdlib.h>
9  #include <time.h>
10
11 int main(void){
12     puts("Nuclear Warhead code generator");
13
14     time_t now;
15     srand(time(&now));
16     printf("%s", ctime(&now));
17
18
19     while(1) {
20         puts("Press Any Key generate new code");
21         getchar();
22
23         for(int i=0; i<NB_NUM; i++){
24             printf("%d ",rand() % (MAX_NUM - MIN_NUM +1) + MIN_NUM);
25         }
26         printf("\n");
27
28     }
29     return 0;
30 }
```

La dernière console a pu être récupérée

Pouvez-vous déduire les prochains codes ?

2.2 CardGame

Etant chaque année dernier au concours de carte de la commune, vous décidez de prendre votre revanche cette année. Vous allez tenter de prédire les cartes des futurs tirages. En discutant avec l'organisateur, vous réussissez à lui récupérer le binaire des tirages de cartes. Il vous dit qu'il a été lancé pour la première fois **cette année**.

Les lignes intéressantes du binaire vous sont données.

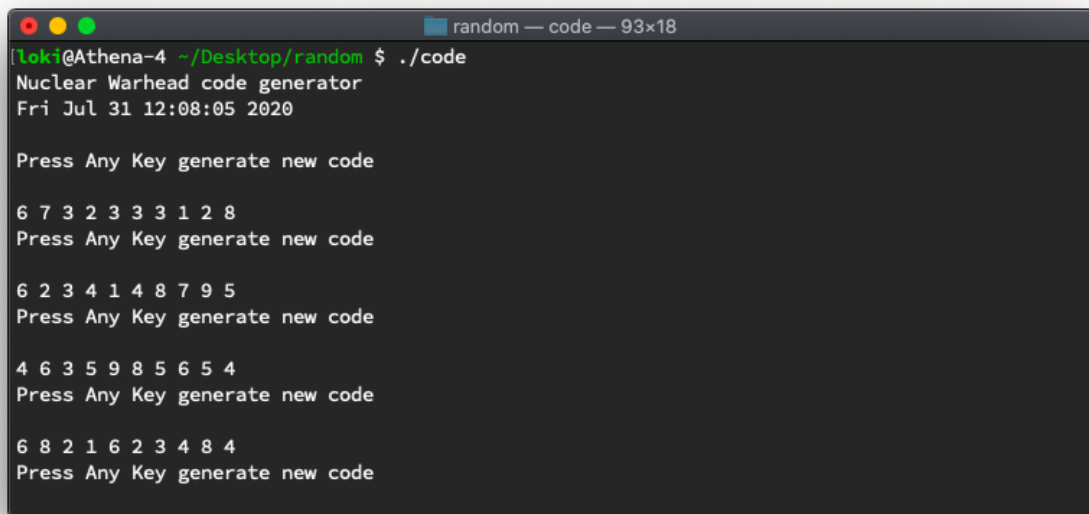
Connaissant les premiers tirages, pouvez-vous prédire les suivants ?

2.3 EuroMillions

Vous réussissez à récupérer le binaire officiel des tirages de la loterie EuroMillions.

Sachant que le jeu a été lancé au deuxième semestre 2019, prédisiez les prochains tirages.

2.4 Annexes



```
[Loki@Athena-4 ~/Desktop/random $ ./code
Nuclear Warhead code generator
Fri Jul 31 12:08:05 2020

Press Any Key generate new code

6 7 3 2 3 3 3 1 2 8
Press Any Key generate new code

6 2 3 4 1 4 8 7 9 5
Press Any Key generate new code

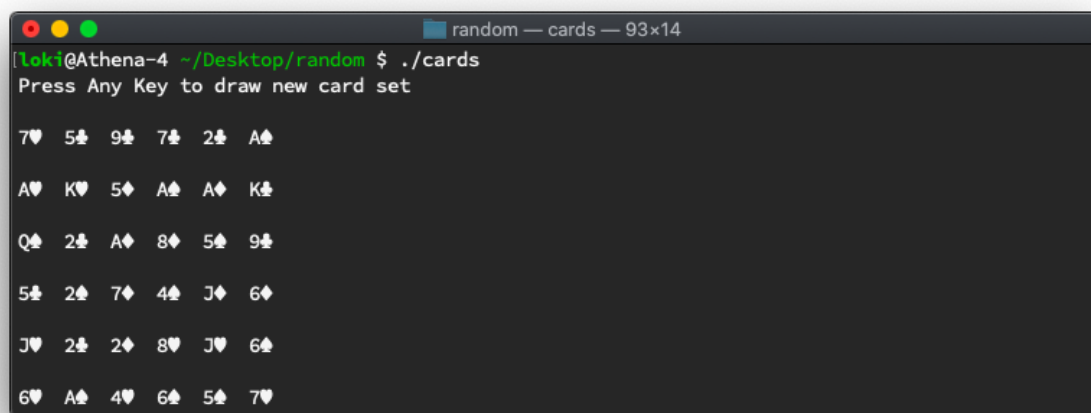
4 6 3 5 9 8 5 6 5 4
Press Any Key generate new code

6 8 2 1 6 2 3 4 8 4
Press Any Key generate new code
```

Figure 1: Exo 1 - Dernière console de bord

```
1 //...
2
3 const char* CardColors[] = {"♠", "♥", "♦", "♣"};
4 const char* CardValues[] = {"2", "3", "4", "5", "6", "7", "8", "9", "J", "Q", "K", "A"};
5
6 //...
7
8 CardValues[rand() % NS_ARRAY_LENGTH(CardValues)],
9 CardColors[rand() % NS_ARRAY_LENGTH(CardColors))];
10
11 //...
```

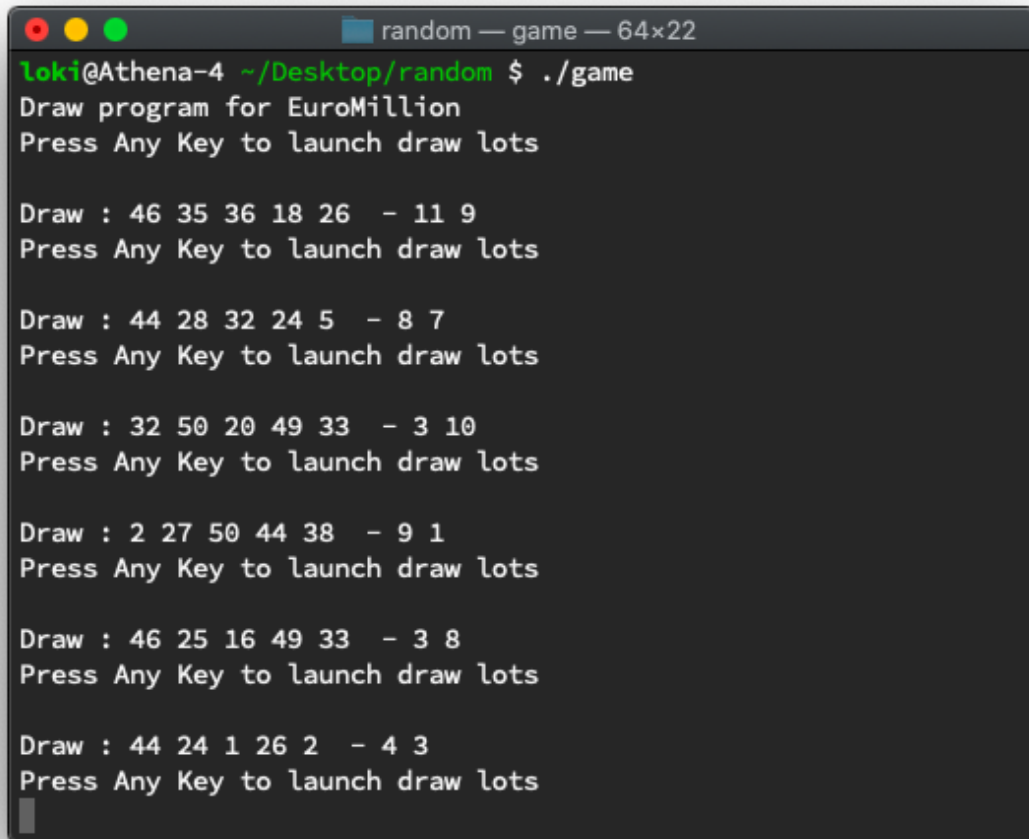
Figure 2: Exo 2 - Lignes de code



```
random — cards — 93x14
[loki@Athena-4 ~/Desktop/random $ ./cards
Press Any Key to draw new card set

7♥ 5♣ 9♣ 7♣ 2♣ A♣
A♥ K♥ 5♦ A♠ A♦ K♠
Q♠ 2♠ A♦ 8♦ 5♠ 9♠
5♣ 2♣ 7♦ 4♠ J♦ 6♦
J♥ 2♠ 2♦ 8♥ J♥ 6♠
6♥ A♠ 4♥ 6♠ 5♠ 7♥
```

Figure 3: Exo 2 - Derniers tirages

A terminal window titled "random — game — 64x22" with standard macOS window controls (red, yellow, green buttons). The prompt is "loki@Athena-4 ~/Desktop/random \$./game". The program outputs "Draw program for EuroMillion" and "Press Any Key to launch draw lots". It then displays six sets of random numbers, each preceded by "Draw :", followed by "Press Any Key to launch draw lots". The numbers are: 46 35 36 18 26 - 11 9; 44 28 32 24 5 - 8 7; 32 50 20 49 33 - 3 10; 2 27 50 44 38 - 9 1; 46 25 16 49 33 - 3 8; and 44 24 1 26 2 - 4 3. A cursor is visible at the bottom left.

```
loki@Athena-4 ~/Desktop/random $ ./game
Draw program for EuroMillion
Press Any Key to launch draw lots

Draw : 46 35 36 18 26 - 11 9
Press Any Key to launch draw lots

Draw : 44 28 32 24 5 - 8 7
Press Any Key to launch draw lots

Draw : 32 50 20 49 33 - 3 10
Press Any Key to launch draw lots

Draw : 2 27 50 44 38 - 9 1
Press Any Key to launch draw lots

Draw : 46 25 16 49 33 - 3 8
Press Any Key to launch draw lots

Draw : 44 24 1 26 2 - 4 3
Press Any Key to launch draw lots
```

Figure 4: Exo 3 - Derniers tirages d'EuroMillions