

Défi c0d1ngUP Chiffrement Cybermen-Daleks

c0d1ngUP team¹

c0d1ngUP² est un **challenge de programmation**, qui s'adresse autant aux débutants qu'aux programmeurs plus expérimentés. Il se présente sous la forme d'épreuves et d'énigmes dont la résolution nécessite **programmation, réflexion et inventivité**. Chaque participant **utilise les outils et langages de programmation de son choix** : seule importe la résolution effective de l'énigme.

La première édition a eu lieu en 2014. Exception faite de 2020, il y a eu une édition par an, généralement en mars. Le challenge se déroule en présentiel, à Poitiers, sur une journée. Cependant, depuis 2021, il est également possible de participer au concours en mode distanciel (quelques défis en moins, tableau des scores adapté...). Le niveau des épreuves est varié, et chaque participant peut, indépendamment de son niveau, trouver des énigmes à résoudre tout en s'amusant.

Les participants peuvent concourir **individuellement ou en équipe de deux** et sont segmentés en différentes catégories qui n'entrent pas en concurrence. Durant la journée, chaque concurrent peut suivre en direct le nombre de points et le classement de tous les participants du concours. Après 7 heures d'intense activité, les résultats sont donnés et les meilleurs de chaque catégorie récompensés.

1. Emmanuel Laizé (université de Poitiers, UP), Freddy Légé (UP), Laurent Signac (UP), Benoit Tremblais (UP), Loïc Restoux, Caroline Tartary.

2. <https://codingup.fr>.

c0d1ngUP poursuit plusieurs objectifs : **promouvoir et démystifier la programmation** auprès du plus grand nombre, **informer les futurs étudiants** sur les filières universitaires qui ouvrent sur les métiers du développement et enfin, permettre aux personnes intéressées par la programmation de **se rencontrer et de mettre à l'épreuve leur savoir-faire**.

Les problèmes les plus faciles peuvent être résolus par des collégiens avancés en programmation (à l'aide d'outils de programmation par blocs comme Scratch). Les plus difficiles donnent du fil à retordre à la plupart des challengers (le temps est limité, et il y a généralement entre 20 et 25 problèmes).

Dans cette nouvelle rubrique, nous proposerons aux lecteurs de 1024 certains de ces problèmes, plutôt parmi les difficiles (donc *a priori* hors de portée des collégiens). Les énoncés seront présentés avec seulement quelques modifications cosmétiques mineures. Des liens seront fournis pour accéder aux fichiers parfois nécessaires à la **résolution effective** du problème (on rappelle que les challengers ne doivent pas produire leur code, mais seulement résoudre effectivement le problème). Dans le bulletin 1024 suivant, nous donnerons quelques *éléments de résolution* agrémentés si possible des idées ou programmes (fonctionnels) que vous aurez pu nous faire parvenir.

Nous présentons ici un problème de 2023, l'année du thème *Docteur Who*³. C'est inhabituel, l'énoncé de ce challenge contient aussi du code C.

Chiffrement Cybermen-Daleks

Le Docteur a besoin d'un cryptanalyste, et c'est à vous qu'il a fait appel. Il semble que les Cybermen et les Daleks utilisent un nouveau système de chiffrement pour communiquer. Vous avez pu mettre la main sur la méthode de chiffrement dans un dépôt GitInvaders et vous disposez maintenant de fonctions de chiffrement écrites en C :

```
#include <string.h>
#include <assert.h>
#define BLKSIZE1 5
#define BLKSIZE2 5
#define MODULE 33554432L

char alp[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZ. ,:!?";

unsigned long int pgcd(unsigned long int a,
                      unsigned long int b) {
    if (b == 0) return a;
    return pgcd(b, a % b);
}
```

3. Chaque année a son thème, souvent tiré de la pop culture, et avec lequel nous prenons généralement quelques libertés... que les fans absolus ne s'en offusquent pas.

```

int letter_num(char c) {
    switch(c) {
        case '.': return 26;
        case ' ': return 27;
        case ',': return 28;
        case ':': return 29;
        case '!': return 30;
        case '?': return 31;
        default: return c - 'A';
    }
}

char num_letter(int n) {
    return alp[n];
}

void crypt1_blk(char blk[], char key[], char res[]) {
    for (int i = 0; i < BLKSIZE1; i++) {
        res[i] = num_letter(letter_num(blk[i]) ^
                                letter_num(key[i]));
    }
}

void crypt2_blk(char blk[], unsigned long int key,
                char res[]) {
    unsigned long int n = 0;
    for (int i = 0; i < BLKSIZE2; i++) {
        n = n * 32 + letter_num(blk[i]);
    }
    n = (n * key) % MODULE;
    for (int i = BLKSIZE2 - 1; i >= 0; i--) {
        res[i] = num_letter(n % 32);
        n = n / 32;
    }
}

void crypt(char message[], char key1[], int key2,
           char res[]) {
    assert (strlen(message)
            % (BLKSIZE1 * BLKSIZE2
              / pgcd(BLKSIZE1, BLKSIZE2)) == 0);
    assert (pgcd(key2, MODULE) == 1);
    assert (strlen(key1) == BLKSIZE1);
    assert (key2 >= 0 && key2 < MODULE);

    for (int i = 0; i < strlen(message); i += BLKSIZE1) {
        crypt1_blk(&message[i], key1, &res[i]);
    }
    for (int i = 0; i < strlen(message); i += BLKSIZE2) {
        crypt2_blk(&res[i], key2, &res[i]);
    }
}

```

Les Daleks et les Cybermen ont certainement une paire de clés communes (key1 et key2 du code C) et chiffrent leurs messages avec ces clés.

Le Tardis a aussi pu intercepter deux messages :

- Cybermen aux Daleks (le message fait une seule ligne de 70 caractères, les blancs y sont représentés par ce symbole «`␣`») :



```
:RMOP,DOCC,QTUY,QMHWVA_L_DCUUGYMHN_QUQXWK!  
KJGL?FRD_EL,OJQMOXUIYSDOBMQF
```

- Réponse des Daleks (10 caractères) : MA.AYTBUAY

Il y a fort à parier que la dernière réponse des Daleks est : EXTERMINER

Serez-vous capable de décrypter le message et d'informer le Docteur du plan machiavélique qui se trame? Validez le défi avec le message des Cybermen.

Vous pouvez nous faire parvenir votre méthode, vos astuces de résolution, vos remarques, accompagnées de la solution au défi (ici, la réponse au défi est simplement le message décrypté des Cybermen), à l'adresse suivante : <mailto:codingup.team+1024@gmail.com>. Dans le prochain bulletin, nous proposerons une synthèse de notre solution et de celles qui nous seront parvenues à temps.

Données accessibles en ligne

- Code C de la méthode de chiffrement⁴
- Message des Cybermen⁵
- Réponse des Daleks⁶

4. <https://codingup.socinfo.fr/1024/24/pb/chiffrement.c>.

5. <https://codingup.socinfo.fr/1024/24/pb/message1.txt>.

6. <https://codingup.socinfo.fr/1024/24/pb/message2.txt>.