B0 - HUB

B-INN-000

Capture The Flag

Cyber Security & Cryptography

Le chiffrement

Les données sont souvent chiffrées pour les rendre illisibles afin qu'elles ne soient connues de tous.
Il existe plusieurs algorithmes qui permettent le chiffrement et le déchiffrement des données comme par exemple le **chiffrement RSA**. Ainsi, nos données peuvent être sécurisées !

Capture The Flag

Votre mission

Le Père Noël vous a embauché afin de vérifier si ses informations personnelles sont sécurisées afin qu'il garde son identité secrète. Même s'il a pris un abonnement **Nord VPN**, vous allez essayer de **déchiffrer** ses données afin d'avoir accès à ses informations personnelles.
Pour déchiffrer les données, vous allez devoir, **grâce au titre**, trouver l'algorithme de chiffrement adéquat pour trouver le mot de passe.

Vous allez devoir faire des recherches sur internet pour réussir. N'hésitez pas à vous entre-aider ou appeler un Cobra si vous avez besoin d'aide.

Pour vérifier vos mots de passe trouvés, vous avez a votre disposition un Google Form . N'oubliez pas de le remplir pour pouvoir valider vos réponses !

Bonus : Si vous trouvez les prénoms de tous les **Cobras** présents aujourd'hui, vous gagnerez un mot de passe au choix.

Qu'est-ce qu'un Capture The Flag ?

Un Capture The Flag (ou CTF) consiste à récupérer un flag c'est-à-dire une donnée cachée.
Pour ce sujet vous allez devoir **déchiffrer** une suite de caractères vous donnant un mot de passe. Ce mot de passe sera utile pour ce **Coding Club Chirstmas Camp**. Celui qui aura le plus de mots de passe gagnera une surprise !

Qu'est-ce qu'un dechiffrement de donnees ?

Le déchiffrement d'une donnée c'est rendre une donnée lisible qui a été auparavant rendu illisible par un algorithme de chiffrement de données.
Par exemple, la chaine de caractères "**Ifmmp**" deviendra, grâce au déchiffrement du code César (ou chiffrement par décalage) de clé 1 :

```
Terminal
~/B-INN-000> ./code-cesar 1 Ifmmp
» Hello
```

On dit donc que la donnée est rendu lisible.

DEBUT DE LA MISSION

1 - JULES CESAR

```
Terminal
~/B-INN-000> Zs ach rs doggs sgh Zihwb
```

2 - MESSAGE DIGEST

```
Terminal
~/B-INN-000> 8c9020ccb57a2577f0dc540837ba08ae
```

3 - C'EST LA BASE 8 OCTET

```
Terminal
~/B-INN-000> TGUgbW9IGRlIHBhc3NlIGVzdCBTYXBpbg==
```

4 - ASKIP

```
Terminal
~/B-INN-000> 76 101 32 109 111 116 32 100 101 32 112 97 115 115 101 32 101 115 116
32 82 101 118 101 105 108 108 111 110
```

5 - LE NOMBRE DE CHEH

```
Terminal
~/B-INN-000> Hash : 51559 368
Clé : 85720
```

6 - BIP BOUP

```
Terminal
~/B-INN-000> 01000011 01100001 01100100 01100101 01100001 01110101
```

7 - TUTUTU TUUUU TUTU

Terminal

```
~/B-INN-000> .-.. . / - -- - / -.. . / .-. .- ... ... . / . ... - / .-. . -. -. .
```

8 - TRIFIDE

Terminal

```
~/B-INN-000> BABABC BAABCBCAC ABBABC BCAAABCCBCCBCCBABC ABCCCBCAC
CACCCAAABBBABACABCAABCAA
```

9 - TRITHEME

Terminal

```
~/B-INN-000> Sempiternellement à perpétuité
Dans son royaume à perpétuité
```

10 - MESSAGE SECRET

Terminal

```
~/B-INN-000> Jours ensoleillés, douce lumière dorée,
Oiseaux chantent, mélodie légère éthérée.
Univers danse, étoiles dans la nuit constellées,
Éternité émerge, poésie du temps effleurée.
Tendresse des vagues, l'océan chante sa complainte.
```

11 - PAS LA BASE 2 NI LA BASE 10

Terminal

```
~/B-INN-000> 4c 65 20 6d 6f 74 20 64 65 20 70 61 73 73 65 20 65 73 74 20 4e 6f 75
72 72 69 74 75 72 65
```

LE SAVIEZ-VOUS ?

Le calendrier de l'Avent que l'on accroche tous dans nos maisons à partir du 1er décembre, est d'origine Allemande, et servait à faire patienter les enfants jusqu'à Noël. Par contre, pas de chocolats ou petits cadeaux à l'intérieur, mais plutôt des images religieuses, comportant une phrase de l'Evangile ou une incitation à la bonne action. Pas sûr que cela marche encore de nos jours…

12 - Code talker

```
Terminal
~/B-INN-000> NASH-DOIE-TSO DZEH TSIN-TLITI TLO-CHIN A-WOH LHA-CHA-EH AH-JAH
NE-ZHONI WOL-LA-CHEE KLESH KLESH AH-JAH DZEH DIBEH D-AH MOASI CHA WOL-LA-CHEE
NO-DA-IH KLESH DIBEH AH-JAH D-AH THAN-ZIE AH-JAH
```

13 - Des si mal !

```
Terminal
~/B-INN-000> 76 101 32 109 111 116 32 100 101 32 112 97 115 115 101 32 101 115 116
32 72 105 118 101 114
```

14 - UU code

```
Terminal
~/B-INN-000> begin 644 dcode_uuencode
%4V%N=&$
end
```

15 - Chat 256 !

A vous de chiffrer le mot “Buche” et de trouver l’algorithme correspondant !

Lisez bien le titre !

16 - Je suis a mon prime

```
Terminal
~/B-INN-000> 37 11 41 47 71 7 11 53 2 67 67 11 11 67 71 53 47 37 11 43 47 61 7
```

17 - Un poisson qui souffle

```
Terminal
~/B-INN-000> Hash : rd92XwCU6YVr5LBFHqS32g==
Clé : Poisson
```

18 - Detroit

```
Terminal
~/B-INN-000> 11/4/ /12/14/19/ /3/4/ /15/26/18/18/4/ /4/18/19/
/19/17/26/3/8/19/8/14/13
```

19 - Malaise pain

```
Terminal
~/B-INN-000> La pib da messa asb Vecencas
```

20 - Leet speak

```
Terminal
~/B-INN-000> >()W]><
```

21 - Parles-tu Javanais ?

```
Terminal
~/B-INN-000> LAVEMAVOTDAVEPAVASSAVEESTFAVAMAVILLE
```

22 - Quel temps fait-il aujourd'hui ?

```
Terminal
~/B-INN-000> +17°C +24°C +16°C +14°C +9°C +25°C +24°C +13°C +28°C +10°C +10°C
+24°C +24°C +10°C +9°C +23°C +11°C +14°C +20°C +25°C
```

23 - Wolseley

```
Terminal
~/B-INN-000> Hash : XNPWZSFIWEA
Clé : RUDOLF
```

24 - This is sparta !

```
Terminal
~/B-INN-000> Fnnl·eodicego·e
```

25 - B36

```
Terminal
~/B-INN-000> 915669005702 482 39308270
```

La mission n'est pas terminee !

Vous avez trouvé tous les mots de passe ?
Pour la réussir la mission, il suffit de répondre a une dernière énigme.Regardez chaque lettres des mots de passe trouvés.
Le premier nombre est le numéro de l'énigme et le second nombre est le caractère.
Voici donc le dernier mot de passe :

```
Terminal
~/B-INN-000> 6-1 1-1 4-6 10-4 11-1 23-1 17-1 5-3 9-2 22-2
```

Allez voir le **Père Noël** ou un **Cobra** avec ce code et vous gagnerez un cadeau !
Mais ce n'est pas fini !
C'est maintenant à vous d'implémenter quelques algorithmes de chiffrement en Python.

Conversion en Decimal

Tout d'abord, vous allez créer un fichier nommé `str_to_decimal.py`.
Vous allez ensuite créer une fonction `str_to_decimal(mot)` qui prend en paramètre une chaine de caractère `mot` et qui affiche les valeurs décimales des lettres de `mot`.

```
def str_to_decimal(mot)
```

Pour effectuer le chiffrement d'une chaine de caractères en décimal, vous allez devoir utiliser la fonction `ord()` qui permet de récupérer l'équivalent décimal d'un caractère.

Exemple :

```
Terminal
~/B-INN-000> ord(0)
» 48
```

A vous de coder !

Code Cesar

Maintenant que vous savez récupérer le décimal d'un caractère, vous allez devoir implémenter l'algorithme du Code César.
Le Code Cesar est un algorithme de chiffrement par décalage de n lettre (n étant une clé donnée.)

```
def code_cesar(message, decalage)
```

La fonction chiffre_cesar prend comme paramètre une chaine de caractères `message` et un entier `decalage` qui équivaut à notre clé. Cette fonction renvoie une chaine de caractères `message_chiffre` qui sera le message chiffré après modification.

Vous allez utiliser la fonction `chr()` vous permettant d'obtenir le caractère grâce à son équivalent en décimal.

Exemple :

```
Terminal
~/B-INN-000> chr(48)
» 0
```

A vous de coder !

Aller plus loin...

Si vous avez fini l'algorithme du Code César, alors vous pouvez implémenter d'autres algorithmes de chiffrement. En voici une liste :

- XOR
- RSA
- Leet Speak
- Binaire
- Il y en a plein, à vous d'en trouver !

Fin de mission

Grâce à votre expertise le Père Noël sait désormais qu'un abonnement Nord VPN ne suffit pas ;)
Peut-être qu'il vous appelera la prochaine fois pour lui régler ses failles informatique, qui sait ?
Si vous êtes arrivé jusqu'ici c'est que vous êtes trop fort(e) (ou alors que vous commencez un sujet par la fin ??).
Le monde de la cyber-sécurité est très vaste et en constante évolution, c'est pourquoi nous vous avons fait découvrir ce monde tout en s'amusant !