

02 Walkthrough

Apprenant	Date	Sujet	Nom du CTF
Michel MEIRESONNE	25/01/2023	Cryptographie Résolution	Base-Ball

Résolution

TkhNMkI7SWwgZmF1dCBhd9pcibkZSBib25uZXMGYmFzZXN9

Déterminer le type de chiffrement

Sur [Dcode](#) on peut identifier rapidement le type.

The screenshot shows the Dcode interface. At the top, there's a search bar with the text 'Rechercher un outil'. Below it, a message says '★ RECHERCHE SUR DCODE PAR MOTS-CLÉS : TkhNMkI7SWwgZmF1dCBhd9pcibkZSBib25uZXMGYmFzZXN9'. There's also a link to 'PARCOURIR LA LISTE COMPLÈTE DES OUTILS'. A sidebar on the left lists tools: 'Code Base64 (ymfzzty0)', 'Précision et Rappel (11)' (with items like 'Vous ne trouvez pas ?', 'Vous cherchez à déchiffrer un message ? Essayez le détecteur de chiffrement !', 'Parcourez la liste de tous les outils dCode', and 'Décrivez vos besoins: écrivez-nous !'), and 'Reconnaitre un Chiffrement' (with a note about identifying cipher types). The main area has a section titled 'RECONNAITRE UN CHIFFREMENT' under 'Cryptographie > Reconnaître un Chiffrement'. It includes a 'Real-Time Feedback' box with the text 'Like a spell checker, SonarLint squiggles coding issues and enables you to code better.' and a 'Sonar' button with an 'Open' button. Below this is a 'IDENTIFIER UN MESSAGE CODÉ' section with a message input field containing 'TkhNMkI7SWwgZmF1dCBhd9pcibkZSBib25uZXMGYmFzZXN9', a 'INDICES/MOTS-CLÉS (FACULTATIF)' input field, and a '► ANALYSER' button. A note at the bottom says 'Voir aussi : Analyse des Fréquences – Indice de Coïncidence'.

Résolution en ligne

Il existe plusieurs sites pour déchiffrer, par exemple

- [Cyberchief](#)
- [Dcode](#)
- [Online-toolz](#)

Ici on le fait avec CyberChef

The screenshot shows the CyberChef interface with the following layout:

- Operations** sidebar:
 - Favourites
 - To Base64
 - From Base64
 - To Hex
 - From Hex
 - To Hexdump
 - From Hexdump
 - URL Decode
 - Regular expression
 - Entropy
 - Fork
 - Magic
- Recipe** panel:
 - STEP
 - BAKE! button
 - Auto Bake checkbox
- Input** panel: Empty.
- Output** panel:
 - time: 1ms
 - length: 36
 - lines: 1

- **avec Magic**

- Si le type de chiffrement est indéterminer

Dans la partie Opération on chercher Magic, puis la fait glisser vers Recipe.

The screenshot shows the CyberChef interface with the following layout:

- Operations** sidebar:
 - magic
 - Magic**
 - Image Brightness / Contrast
 - Detect File Type
 - Scan for Embedded Files
- Recipe** panel:
 - Magic
 - Depth: 3
 - Intensive mode checkbox
 - Extensive language support checkbox
 - Crib (known plaintext string or regex) input field
- Input** panel: Empty.
- Output** panel:
 - time: 7ms
 - length: 2
 - lines: 1

Nothing of interest could be detected about the input data.
Have you tried modifying the operation arguments?

- **avec From base64**

- Si il a trouver que c'est du base64

Dans la partie Opération on chercher From Base64, puis la fait glisser vers Recipe.

The screenshot shows the Cryptpad interface with a 'From Base64' recipe selected. The input field contains the encoded string 'TkNMk17SWwgZmF1dCBhd9pcibkZSBib25uZXMyMfzZXN9'. The output field shows the decrypted message: 'NHM2I{Il faut avoir de bonnes bases}'.

Puis on colle le chiffré

TkhNMk17SWwgZmF1dCBhd9pcibkZSBib25uZXMyMfzZXN9

dans Input.

Le message déchiffré s'affiche dans Output

NHM2I{Il faut avoir de bonnes bases}

avec From base64

The screenshot shows the Cryptpad interface with a 'From Base64' recipe selected. The input field contains the encoded string 'TkNMk17SWwgZmF1dCBhd9pcibkZSBib25uZXMyMfzZXN9'. The output field shows the decrypted message: 'NHM2I{Il faut avoir de bonnes bases}'.

avec Magic

The screenshot shows the Cryptpad interface with a 'Magic' recipe selected. The input field contains the encoded string 'TkNMk17SWwgZmF1dCBhd9pcibkZSBib25uZXMyMfzZXN9'. The output table shows three results:

Recipe (click to load)	Result snippet	Properties
<code>From_Base64('A-Za-z0-9+=',true,false)</code>	NHM2I{Il faut avoir de bonnes bases}	Valid UTF8 Entropy: 4.23
<code>From_Base64('A-Za-z0-9+=',true,false)</code>	NHM2I{Il faut avoir de bonnes bases}	Valid UTF8 Entropy: 4.23
<code>From_Base64('A-Za-z0-9+\\",true,false)</code>	NHM2I{Il faut avoir de bonnes bases}	Valid UTF8 Entropy: 4.23

Le déchiffrement en lignes de commande

On utilise la commande

```
echo -ne TkHNmk17SWwgZmF1dCBhd9pcIBkZSBib25uZXMyMfzZXN9 | base64  
# Flag{drapeau d'initiation}
```

Bonus

Source: <https://www.dcode.fr/code-base-64>

Qu'est-ce que l'encodage Base64 ?

Base64 est un codage informatique utilisant 64 caractères pour encoder n'importe quelle chaîne binaire avec du texte (il est notamment utilisé pour les emails).

Pourquoi utiliser la Base64 ?

Un message codé en Base64 contiendra uniquement des caractères ASCII imprimables
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+=

Cette propriété permet de transmettre n'importe quelles données sur des systèmes originellement prévus pour ne transmettre que du texte (sans avoir à se soucier de l'encodage initial ni de la manière dont les caractères apparaîtront sur l'écran du destinataire du message)

Qu'est-ce que Base64URL ?

Base64URL est une variante de Base64 adaptée aux URL (http). Les caractères 62 + et 63 / peuvent poser des problèmes dans les URL, les remplacer alors par respectivement - et _. De plus, le = est quant à lui supprimé.

Quand Base64 a-t-il été inventé ?

La Norme RFC 2045 qui officialise Base64 date de 1996