

Cyberchef

Description

CyberChef est un outil open source qui permet d'effectuer toutes sortes d'opérations allant du simple encodage, comme du Base64, jusqu'au chiffrement AES, DES, etc. Cet outil facilite la manipulation, la conversion et la compréhension de toutes ces données dans divers formats et à travers différentes méthodes. Il est largement utilisé dans les domaines de la cybersécurité, de la cryptographie (notamment pour du chiffrement, déchiffrement, hachage), de la stéganographie et d'autres domaines similaires.

Installation

Aucune installation n'est nécessaire pour utiliser l'outil CyberChef. Vous pouvez y accéder directement depuis un navigateur web en visitant le site officiel : <https://gchq.github.io/CyberChef/>

Cas d'utilisation

- **Cryptographie** : il permet de chiffrer et de déchiffrer des données, de générer des empreintes cryptographiques et d'effectuer diverses opérations de cryptographie.
- **Analyse de données** : il peut être utilisé pour analyser, supprimer et extraire des informations (comme des métadonnées par exemple) à partir de données brutes ou mal formatées.

Fonctionnalités principales

- **Plus de 250 opérations disponibles** : offre une large gamme d'opérations de transformation de données, telles que différents types d'encodage, la conversion hexadécimale, le hachage, la recherche et le remplacement, la compression, etc.
- **Mode interactif** : vous pouvez effectuer des opérations de manière interactive en utilisant une interface glisser-déposer intuitive.
- **Historique des opérations** : conserve un historique des opérations effectuées, ce qui facilite la relecture ou la modification des étapes précédentes.
- **Modularité** : vous pouvez créer et partager vos propres modules personnalisés pour étendre les fonctionnalités de CyberChef.

Exemple d'exploitation ou d'utilisation

Supposons que vous souhaitez déchiffrer un message codé à l'aide d'une substitution de type Code César dans une image avec CyberChef.

Dans l'interface de CyberChef, vous configurez l'opération **Substitution** de CyberChef pour utiliser la clé de déchiffrement appropriée, qui est le décalage du Code César. Il exécute ainsi l'opération de substitution sur l'image, ce qui entraîne le déchiffrement du message contenu dans l'image.

Une fois le message déchiffré, vous pouvez analyser le texte brut à la recherche d'informations ou d'indices. Il peut s'agir de mots-clés, de phrases significatives ou d'autres éléments pertinents. Si des informations sensibles ou des indices sont identifiés, vous pouvez ainsi les extraire du message déchiffré.

- Brute force de la méthode de chiffrement ROT13

The screenshot shows the CyberChef interface with the following configuration:

- Input:** Qb lhh yvrx EBG13 ?
- Recipe:** ROT13 Brute Force
- Options:** Rotate lower case chars (checked), Rotate upper case chars (checked), Rotate numbers (unchecked), Sample length: 106, Sample offset: 0, Print amount (checked).
- Crib (known plaintext string):** (empty)
- Output:** The output shows the decrypted message: "Amount = 1: Rc mcl zwys FCH13 ?" followed by 17 more lines of decrypted text.
- Buttons:** STEP, BAKE!, Auto Bake.

- Chiffrement d'un message chiffré par Enigma

The screenshot shows the CyberChef interface with the following configuration:

- Input:** Yes i like it !
- Recipe:** Enigma
- Options:** Model: 3-rotor, Left-hand rotor: EKMFNLGDQVZNTOWYHXA, Middle rotor: AJDKSIRUXBLHWTMCQ, Right-hand rotor: BDFHJLCPRTVZNYEI, Rotor settings: P, W, N, Reflector: AY BR CU DH EQ FS GL IP JX, Initial values: A, K, R.
- Output:** The output shows the encrypted message: DLMVJ ZFZTR.
- Buttons:** STEP, BAKE!, Auto Bake.

- Détection d'un encodage ou chiffrement

La méthode "magic" permet d'essayer de détecter l'encodage ou le chiffrement utilisé sur la chaîne de caractères passée à Cyberchef. Plus la chaîne est longue, plus grand est le pourcentage de réussite de l'opération de détection.

The screenshot shows the CyberChef interface with the following configuration:

- Input:** 87cURD]hqrDfdR*AKW,
- Recipe:** Magic (Depth 3), Intensive mode checked, Extensive language support unchecked.
- Output:**
 - Result snippet:** Hello Root-Me !
 - Properties:** Valid UTF8, Entropy: 3.19
 - Raw Bytes:** 87cURD]hqrDfdR*AKW,
 - Hexdump:** Matching ops: From Base85, From Hexdump
 - Entropy:** 4.04

- Chainer les méthodes

Une des fonctionnalités très intéressante de CyberChef est celle qui permet de chaîner les opérations. Vous pouvez glisser plusieurs opération (From/To) de différents chiffrements/encodages pour aboutir à un résultat. Dans l'exemple suivant, nous réalisons d'abord un décodage hexadécimal, puis en base64 :

The screenshot shows the CyberChef interface with the following configuration:

- Input:** 53 47 56 73 62 47 38 67 64 47 68 6C 63 60 55 67 4F 69 6B 67 49 51 3D 3D
- Recipe:**
 - From Hex:** Delimiter set to Auto.
 - From Base64:** Alphabet set to A-Za-zA-Z0-9+/=, Remove non-alphabet chars checked, Strict mode unchecked.
- Output:** Hello there :) !

Références

- <https://github.com/gchq/CyberChef>

Retour fiches outils

- [Cyber fiches outils](#)

From:
[/- Les cours du BTS SIO](#)

Permanent link:
[/doku.php/cyber/outils/cyberchef](#)

Last update: **2025/06/20 17:20**