

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 type 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 souhaitiez 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

Download CyberChef

ChaCha

Rabbit

SM4 Encrypt

SM4 Decrypt

GOST Encrypt

GOST Decrypt

GOST Sign

GOST Verify

GOST Key Wrap

GOST Key Unwrap

ROT13

ROT13 Brute Force

ROT47

ROT47 Brute Force

ROT8000

XOR

XOR Brute Force

Vigenère Encode

Vigenère Decode

To Morse Code

From Morse Code

Bacon Cipher Encode

Recipe

ROT13 Brute Force

Rotate lower case chars

Rotate upper case chars

Rotate numbers

Sample length100

Sample offset0

Print amount

Crib (known plaintext string)

STEP

BAKE!

Auto Bake

Input

Qb 1bh yvxr EB613 ?

Output

Amount = 1: Rc mcl zwys FCH13 ?
Amount = 2: Sd ndj axzt GDI13 ?
Amount = 3: Te oek byau HE113 ?
Amount = 4: Uf pfl czbv IFK13 ?
Amount = 5: Vg qgm dacr JGL13 ?
Amount = 6: Wh rhn edbx KHM13 ?
Amount = 7: Xi sio fcey LIN13 ?
Amount = 8: Yj tjp gdfz KJO13 ?
Amount = 9: Zk ukq hega NKP13 ?
Amount = 10: Al vlr ifhb OLQ13 ?
Amount = 11: Bm wes jgic PMR13 ?
Amount = 12: Cn xnt khjd QNS13 ?
Amount = 13: Do you like ROT13 ?
Amount = 14: Ep zpv ejlf SPU13 ?
Amount = 15: Fq aqw nkg TQV13 ?
Amount = 16: Gr brx olnh URW13 ?
Amount = 17: Hs csy pmol V SX13 ?
Amount = 18: It dtz qnpj WTY13 ?
Amount = 19: Ju esa roqk XUZ13 ?
Amount = 20: Ka fth rpsl YVA13 ?

- Chiffrement d'un message chiffré par Enigma

Download CyberChef

JWT Verify

JWT Decode

Citrix CTX1 Encode

Citrix CTX1 Decode

AES Key Wrap

AES Key Unwrap

Pseudo-Random Number Generator

Enigma

Bombe

Multiple Bombe

Typex

Lorenz

Colossus

SIGABA

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Recipe

Enigma

Model3-rotor

Left-hand rotorEKMFLGDQVZNTOWYHX ...

Left-hand rotor ring settingP

Left-hand rotor initial valueA

Middle rotorAJDKSIRUXBLHWTMCQ ...

Middle rotor ring settingW

Middle rotor initial valueK

Right-hand rotorBDFHJLCPRTXVZNYEI ...

Right-hand rotor ring settingN

Right-hand rotor initial valueR

ReflectorAY BR CU DH EQ FS GL IP JX ...

Plugboard

Strict output

STEP

BAKE!

Auto Bake

Input

Yes i like it !

Output

DLMVJ ZFZTR

- 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. On the left, the 'Recipe' panel contains a 'Magic' step with 'Depth' set to 3 and checkboxes for 'Intensive mode' and 'Extensive language support'. Below it is a 'Crib (known plaintext string or regex)' field. The 'Input' panel on the right contains the text '87cURD]hqrDfdR*AKW,'. The 'Output' panel at the bottom displays a table with the following data:

Recipe (click to load)	Result snippet	Properties
From_Base85('!-u')	Hello Root-Me !	Valid UTF8 Entropy: 3.19
	87cURD]hqrDfdR*AKW,	Matching ops: From Base85, From Hexdump Valid UTF8 Entropy: 4.64

- Chaîner 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. On the left, the 'Recipe' panel contains a 'From Hex' step with 'Delimiter' set to 'Auto'. Below it is a 'From Base64' step with 'Alphabet' set to 'A-Za-z0-9+/' and the checkbox 'Remove non-alphabet chars' checked. The 'Input' panel on the right contains a long hex string. The 'Output' panel at the bottom displays the text '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

