Cryptographie CTF

- Cette épreuve vous propose de déchiffrer un message chiffré avec la méthode inventée par Jules César. La clé est inconnue.

Cryptographie CTF

- Le message chiffré est :

  Rsëudwlrq q°42 : O'djhqw lqilowuë é Ehvdqarq, suëqrppë Udskdôo, grlw uëfxsëuhu oh eoë hw oh fbxu gh o'remhfwli g'lfl oh 15 drœw. Uhqghä-yrxv é fûwë gx judqg fkïqh, oé rç o'hdx hvw wuîv iudöfkh !

- Le flag est le prénom de l’agent infiltré mentionné dans ce message.

Cryptographie CTF

- Resolution

On va faire très simple, César, pour ses communications importantes à son armée, cryptait ses messages. Ce que l'on appelle le chiffrement de César est un décalage des lettres : pour crypter un message, A devient D, B devient E, C devient F ,.... Chaque lettre du message est remplacée par une autre lettre située un certain nombre de positions plus loin dans l'alphabet.

- Resolution

Alphabet de référence

Par exemple, avec une clé de 3 :

Lettre origibale	**lettre chiffrée**
A	**D**
B	**E**
X	**A**

- Resolution

J’espère que vous avez compris le principe, la lettre originale et la lettre chiffrée ont un décalage en fonction de la clé. La clé peut-être 3, 4, 5 ou plus.

Comment fonctionne la clé ?

- Resolution

Clé : 3

Lettre originale

A B C Y

Lettre chiffrée

D E F B

Nous restons dans le même principe

- Resolution

Voici comment se passe le chiffrement pour comprendre le déchiffrement. Formule :

$$C=(P+K) \bmod 26$$

P = position de la lettre originale

K = clé

C = position de la lettre chiffrée

En voici un exemple :

- Resolution

Exemple :

lettre originale : B

Clé : 3

lettre Chiffrée : E

Donc on fait ici B + 3lettres(clé) pour obtenir la sortie donc la lettre chiffrée. (E)

- Resolution

Le déchiffrement maintenant, ce qui nous intéresse dans ce CTF.
Formule : $P=(C-K) \bmod 26$

Exemple concret (à la main)

Premières lettres du message : Message chiffré : ERQMRXU

Clé : inconnue mais prenons par exemple 3

- Resolution

Chiffré		Clé	Clair
E		3	B
R		3	o
Q	Moins la clé	3	n
M		3	j
R		3	o
X		3	u
U		3	r

- Resolution

Sortie en claire : Bonjour

Tu vois ? Pour déchiffrer le message de César, il suffit de décaler les lettres dans l’autre sens.

NB : Le chiffrement de César est une excellente introduction à la cryptologie, mais il est aujourd'hui considéré comme un simple jeu d'enfant. Il ne doit absolument jamais être utilisé pour protéger des données réelles.

• Resolution

Calculs :

R – (clé=inconnue)

s – (clé=inconnue)

ë – S (clé=Inconnue)

Si vous avez la clé, il suffit de remplacer. Par exemple la clé est 3, ont fait donc R – 3 lettres, ça donne 0, lettre suivante s – 3 lettres, ça donne p, donc Op

CODE CHIFFRÉ

```
Rsëudwlrq q°42 : O'djhqw lqilowuë é Ehvdqarq, suëqrppë Udskdôo, grlw
uëfxsëuhu oh eoë hw oh fbxu gh o'remhfwli g'lfl oh 15 dræw. Uhqghä-yrxv é
fûwë gx judqg fkïqh, oé rç o'hdx hvw wuîv iudöfkh !
```

Si tu continues sans jamais t'arrêter, tu obtiens tout le texte, si la clé est bonne.

- Resolution

Comme tu l'as remarqué à la main ça sera hyper long, c'est pourquoi il est essentiel d'automatiser la tâche. Veuillez pratiquer votre compétence en programmation pour l'automatisation.

J'ai personnellement automatiser cette tâche de déchiffrement avec ce script python .

Trouver le script ici

https://github.com/dan-codeScript/cryptographie_c-sar.git

- Resolution

-$ python3 cesar.py

Opération n°42 : L'agent infiltré à Besançon, prénommé Raphaël, doit récupérer le blé et le cœur de l'objectif d'ici le 15 août. Rendez-vous à côté du grand chêne, là où l'eau est très fraîche !

- **FLAG = Raphaël**
- **J’ai bruteforcé la clé car il n’existe que 43 possibilités avec cette version étendue, la clé valide est 3.**

- Resolution

Failles!

NB : La sécurité d'un algorithme repose sur le nombre de clés possibles. Pour un alphabet classique, il n'y a que 26 décalages possibles (ou 43 dans la version étendue). Un ordinateur peut tester toutes ces combinaisons en une fraction de milliseconde.

Le chiffrement de César est une substitution "monoalphabétique", ce qui signifie qu'une lettre d'origine est toujours remplacée par la même lettre chiffrée (par exemple, tous les "e" deviendront des "h"). En français, la lettre "e" apparaît environ 17% du temps, suivie du "a", du "s", etc. Si l'on intercepte un long texte chiffré par César et qu'on compte les lettres, celle qui apparaît le plus souvent correspondra presque à coup sûr au "e". Cela permet de casser la clé mathématiquement en quelques secondes, sans même utiliser le bruteforce.

- Resolution

Structure mentale à retenir

Quand tu vois : « Chiffrement de César »

Tu dois penser immédiatement :

Alphabet → A=0 … Z=25,

Clé (décalage)

Modulo 26,

Soustraction pour déchiffrer,

Dan Maluma
Ingénieur CyberSécurité