Resolution CTF Cryptographie

https://hackropole.fr

Cryptographie CTF

- Cette épreuve vous propose de déchiffrer un message chiffré avec la méthode inventée par Blaise de Vigénère. La clé est FCSC.

Cryptographie CTF

- Le message chiffré est :

  ```
  CGqfltwj emgj clgfv ! Aqltj rjqhjsksg
  ekxuaqs, ua xtwk
  ```

  n'feuguvwb gkwp xwj, ujts f'npxkqvjgw nw tjuwcz

  ugwygjtfkf qz uw efezg sqk gspwonu. Jgsfwb-aqmu f

  Pspygk nj 29 cntnn hqzt dg igtwy fw xtvjg rkkunqf.

- `Le flag est le nom de la ville mentionnée dans ce message.`

Cryptographie CTF

- Resolution

On va faire très simple, le chiffrement de Vigenère est un chiffrement par substitution polyalphabétique qui utilise une clé répétée pour décaler chaque lettre du message, transformant chaque substitution en un chiffrement de César unique, où une lettre du message est chiffrée différemment selon la lettre de la clé qui lui correspond. Contrairement au César (une seule clé), ici : on utilise une clé composée de plusieurs lettres, chaque lettre de la clé correspond à un décalage différent.

- Resolution

Alphabet de référence

On numérote les lettres :

Lettre	Valeur
A	0
B	1
Z	25

- Resolution

J’espère que vous avez compris le principe, chaque lettre a une valeur, on commence de A qui a pour valeur 0 jusqu’à Z qui a pour valeur 25. Souvenez-vous on a commencé par 0.

Comment fonctionne la clé ?

- Resolution

Clé : FCSC

Lettre

F C S C

Valeur

5 2 18 2

Nous restons dans le même principe

- Resolution

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

C = (P + K) mod 26

P = lettre du texte clair

K = lettre de la clé

C = lettre chiffrée

En voici un exemple :

- Resolution

Exemple :

Texte clair : B (1)

Clé : F (5)

Chiffré : G (6)

Donc on fait ici 5 + 1 pour obtenir la sortie donc la lettre chiffrée.

- Resolution

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

Exemple concret (à la main)

Premières lettres du message : Message chiffré : G q f l t w j

Clé répétée : F C S C F C S

- Resolution

Chiffré	Valeur	Clé	Valeur	Clair
G	6	F	5	B
Q	16	C	2	o
f	5	S	18	n
L	11	C	2	j
T	19	F	5	o
w	22	C	2	u
j	9	S	18	r

- Resolution

Sortie en claire : Bonjour

Tu vois ? Ce n’est que de l’arithmétique modulaire.

Points très importants (pièges classiques) Ce qui NE consomme PAS la clé : Espaces, Ponctuation, Retours à la ligne, La clé avance uniquement sur les lettres A–Z / a–z

- Resolution

Calculs :

G (6) − F (5) = 1 → B

q (16) − C (2) = 14 → o

f (5) − S (18) = −13 → +26 = 13 → n

Bon

Gqfltwj emgj clgfv ! Aqltj rjqhjsksg ekxuaqs, ua xtwk n'feuguvwb gkwp xwj, ujts f'npxkqvjgw nw tjuwcz ugwygjtfkf qz uw efezg sqk gspwonu. Jgsfwb-aqmu f Pspygk nj 29 cntnn hqzt dg igtwy fw xtvjg rkkunqf.

Code chiffré

Si tu continues sans jamais t'arrêter, tu obtiens tout le texte.

- 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 connaissances en programmation.

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

Trouver le script ici

https://github.com/dan-codeScript/Vig-n-re-script

- Resolution

-$ python3 decrypt.py

Bonjour cher agent ! Votre prochaine mission, si vous l'acceptez bien sur, sera d'infiltrer le reseau souterrain ou se cache nos ennemis. Rendez-vous a Nantes le 29 avril pour le debut de votre mission.

FLAG = Nantes

- Resolution

Structure mentale à retenir

Quand tu vois : « Chiffrement de Vigénère »

Tu dois penser immédiatement :

Alphabet → A=0 … Z=25,

Clé répétée,

Modulo 26,

Soustraction pour déchiffrer,

Ignorer ponctuation/espaces

Dan Maluma
Juriste & Ir en Cybersécurité