**Prosit 4 : Entre de mauvaises mains**

# Contexte :

Des gens ont usurpé l’identité des employés et on a un moyen de récupérer les mots de passes mais ils sont cryptés.

# Mot clés :

Chiffrement par substitution : Le chiffrement par substitution est une méthode de cryptage où chaque lettre d'un texte clair est remplacée par une autre lettre selon une règle spécifique. Le chiffrement César est un exemple célèbre de chiffrement par substitution.

Cryptographie : La cryptographie est l'art et la science de sécuriser des informations en les transformant en un format illisible, puis en les rendant lisibles uniquement pour les personnes disposant de la clé de déchiffrement appropriée.

Cryptanalyse : La cryptanalyse est l'analyse des systèmes de chiffrement dans le but de les casser ou de les décrypter sans avoir la clé de déchiffrement. C'est l'art de casser les codes.

Hashage : Le hashage est le processus de conversion de données (comme un mot de passe) en une valeur de hachage, généralement une chaîne de caractères alphanumériques, à l'aide d'une fonction de hachage. Le résultat est souvent utilisé pour vérifier l'intégrité des données.

Signature de mot de passe (MDP) : Une signature de mot de passe est une technique de stockage des mots de passe dans une base de données de manière sécurisée en utilisant des fonctions de hachage et des méthodes de salage pour protéger les informations sensibles.

Signature électronique : Une signature électronique est l'équivalent numérique d'une signature manuscrite. Elle est utilisée pour authentifier un document ou une transaction électronique, garantissant son origine et son intégrité.

Chiffrement César : Le chiffrement César est une technique de chiffrement par substitution où chaque lettre dans le texte clair est déplacée d'un certain nombre de positions dans l'alphabet. Il porte le nom de Jules César, qui l'aurait utilisé pour protéger des messages.

Chiffrement de Hill : Le chiffrement de Hill est une méthode de chiffrement qui utilise des matrices pour transformer le texte clair en texte chiffré. Il a été inventé par Lester S. Hill.

Enigma : Enigma était une machine de chiffrement mécanique utilisée par les forces armées allemandes pendant la Seconde Guerre mondiale. Elle était célèbre pour sa complexité et a été décryptée par les Alliés, ce qui a eu un impact significatif sur l'issue de la guerre.

# Problématique :

**Comment décrypter les 2 messages ?**

**Comment appliquer les méthodes de cryptage au mdp de l’entreprise ?**

# Contraintes :

Stagiaire

# Généralisation :

Différentes manières de crypter

# Livrables :

Procédure de cryptage des mots de passe de l’entreprise

Différences entre crypter, chiffrer, décrypter et déchiffrer

# Pistes de solution :

Chiffrement césar

6d… clé hashage

Mdp + clé + fonction = mdp hashé

Hugo = non dernière question

Emile = Clé en hexadécimal ?

Kerbéros pour forcer le changement de mdp

# Plan d’action :

Déchiffrer la phrase

Méthode de chiffrage

# Réalisation du plan d’action :

J’ai réalisé un petit script python me permettant de decoder du chiffrement césar :

def generer\_decryptions\_cesar(phrase\_chiffree):

decalages\_possibles = range(26)

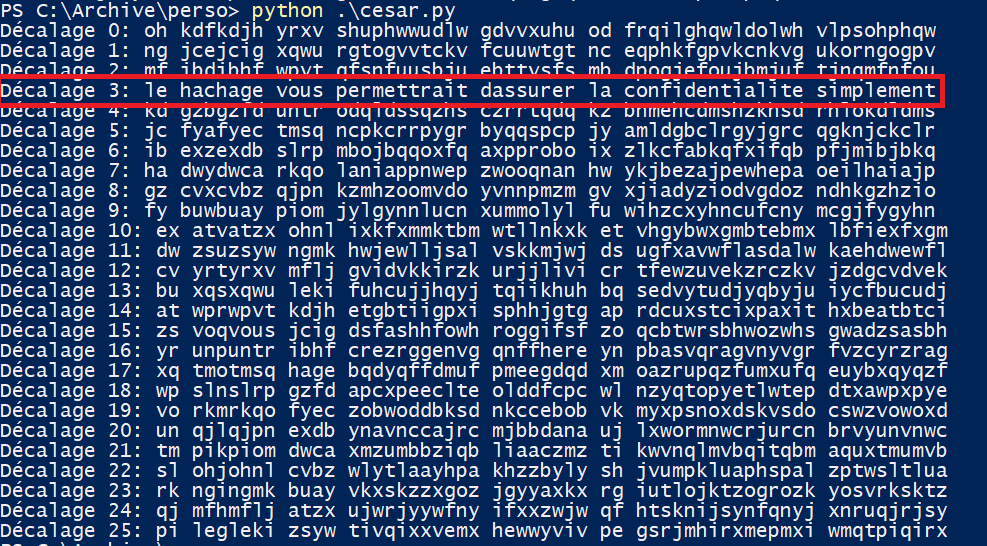
for decalage in decalages\_possibles:

dechiffre = dechiffrer\_cesar(phrase\_chiffree, decalage)

print(f"Décalage {decalage}: {dechiffre}")

generer\_decryptions\_cesar("oh kdfkdjh yrxv shuphwwudlw gdvvxuhu od frqilghqwldolwh vlpsohphqw")

Qui me ressort :



On a donc bien un chiffrement césar simple avec un décalage de 26-3 = 23.

J’ai ensuite essayé de faire quelque chose de la chaine de caractère :

**6d1523b39a9904958cada602dc52c7d4**

Il semblerait que ce soit un mot de passe haché, le principe du hashage de mot de passe est d’utilisé une fonction de hashage à sens unique comme MD5, SHA-1, SHA-256, bcrypt, Scrypt, Argon2… et une clé de hashage ce qui permet de stocker le mot de passe de manière crypté.

Une image contenant texte, Rectangle, capture d’écran, diagramme

Description générée automatiquement

On ne peut par donc construction pas retrouver le mot de passe original une fois qu’il a été hashé. On pourrait essayer avec un dico de mot de passe hashé de comparé notre hash pour retrouver le message en clair, cependant comme on ne connait pas l’algo qui a été utilisé pour hashé, c’est pratiquement impossible.

## Différences entre crypter, chiffrer, décrypter et déchiffrer

Chiffrer : Chiffrer signifie prendre des données en clair (non chiffrées) et les convertir en un format illisible (chiffré) en utilisant un algorithme et une clé de chiffrement. Le but du chiffrement est de protéger les données contre les accès non autorisés en rendant leur contenu illisible sans la clé de déchiffrement appropriée.

Crypter : "Crypter" est un anglicisme qui est souvent utilisé à la place de "chiffrer". Les deux termes ont la même signification en pratique.

Décrypter : Décrypter est l'opération inverse du chiffrement. Cela implique la prise de données chiffrées et l'utilisation de la clé de déchiffrement pour les ramener à leur état d'origine (en clair). Seules les personnes disposant de la clé appropriée sont censées être en mesure de décrypter les données.

Déchiffrer : "Déchiffrer" est un synonyme de "décrypter" et est utilisé de manière interchangeable. Il fait référence à l'action de rendre des données chiffrées lisibles en utilisant la clé de déchiffrement.

## Procédure de cryptage des mots de passe de l’entreprise

Les employés doivent suivre les directives de création de mots de passe fortes, qui comprennent :

Des mots de passe d'au moins 12 caractères.

Une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.

Éviter d'utiliser des informations personnelles faciles à deviner (comme les noms ou les dates de naissance).

Les mots de passe ne doivent pas être stockés sous forme de texte brut. Au lieu de cela, ils doivent être stockés de manière sécurisée, par exemple dans une base de données sécurisée ou un gestionnaire de mots de passe (keepass).

Les mots de passe stockés doivent être chiffrés à l'aide d'un algorithme de chiffrement sécurisé, tel que bcrypt ou Argon2. Le chiffrement doit être effectué avec des paramètres de coût appropriés pour ralentir les attaques par force brute.

Les clés de chiffrement utilisées pour protéger les mots de passe chiffrés doivent être stockées en lieu sûr, de préférence dans un coffre-fort de clés ou un système de gestion des clés sécurisé. L'accès aux clés de chiffrement doit être strictement contrôlé et limité aux personnes autorisées.