Qu'est-ce que la Cryptographie

[sommaire]

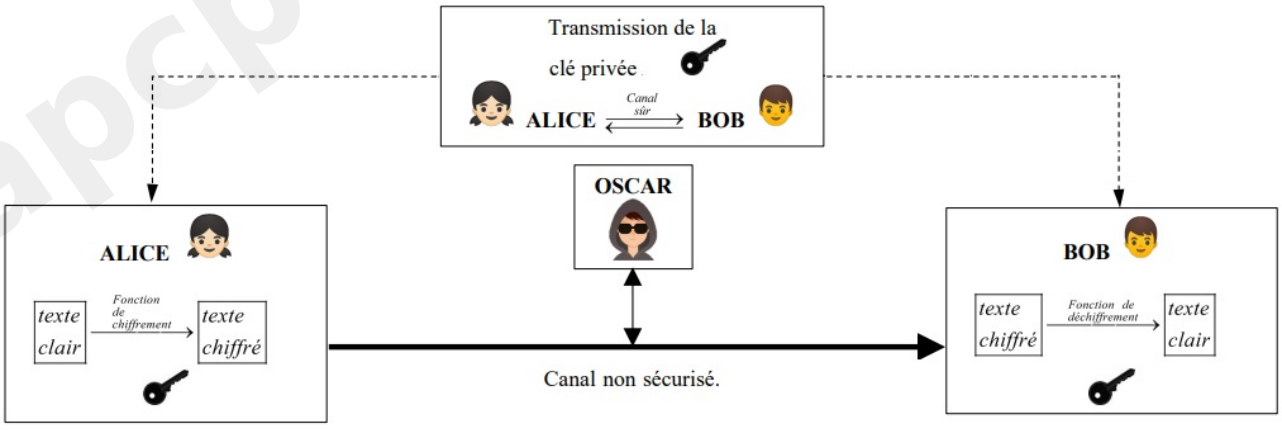
1. ## Objectifs

- Connaitre la Cryptographie

- ## Présentation

  - L'objectif fondamental de la **cryptographie** est de permettre à deux personnes, appelées traditionnellement **ALICE** et **BOB**, de communiquer au travers d'un canal non sécurisé de telle sorte qu'un opposant, **OSCAR** (le cryptanalyste) , ne puisse pas comprendre ce qui est échangé.
  - Le canal peut être par exemple une ligne de téléphone, une fibre optique ou tout autre réseau de communication.
  - L'information qu'**ALICE** souhaite transmettre à **BOB**, que l'on appelle texte clair, peut être un texte en français, une donnée numérique, ou n'importe quoi d'autre de structure arbitraire.
  - **ALICE** transforme le texte clair par un procédé de chiffrement en utilisant une clef prédéterminée et envoie le texte chiffré au travers du canal.
  - **OSCAR** peut intercepter le texte chiffré en espionnant le canal non sécurisé mais ne peut retrouver le texte clair. **BOB** qui connaît la clef, peut déchiffrer le texte et le récupérer.

    Schéma de principe



- ## Définitions de la cryptographie

- La `cryptographie` est une technique utilisée pour protéger les données et empêcher des tiers non autorisés d'accéder ou de modifier des informations précieuses pour leur propre bénéfice ou au détriment d'autrui.
- En général, la `cryptographie` est une technique d'écriture où un message chiffré est écrit à l'aide de codes secrets ou de clés de chiffrement. La `cryptographie` est principalement utilisée pour protéger un message considéré comme confidentiel.
- Cette méthode est utilisée dans un grand nombre de domaines, tels que la défense, les technologies de l'information, la protection de la vie privée, etc.
- La `cryptographie` est une méthode de protection des informations et des communications par l'utilisation de codes, de sorte que seuls les destinataires des informations puissent les lire et les traiter. Le préfixe "crypt-" signifie "caché" ou "coffre-fort" et le suffixe "-graphie" signifie "écriture".

Utilisation

- La `cryptographie` est indispensable pour échanger des informations confidentielles. Autrefois réservée aux utilisations militaires, la `cryptographie` s'étend maintenant aux échanges bancaires, aux informations médicales, aux transferts de données industrielles,...
- Les méthodes de `cryptographie` dites à clé secrète ont été utilisées dans la vie réelle depuis l'Antiquité jusqu'à la seconde guerre mondiale.
- Si celles que nous présentons dans ce cours sont très simples, il en existe d'autres beaucoup plus élaborées. Mais on s'est aperçu qu'aucune d'entre elles ne résiste bien longtemps face à la puissance de calcul apportée par les ordinateurs.
- C'est pourquoi elles ont été en général abandonnées et remplacées par des méthodes plus sûres et radicalement différentes, dites à clé publique, comme la méthode RSA, très largement utilisée sur internet pour la sécurité des transactions et des échanges.
- L'intérêt d'étudier quelques techniques anciennes est qu'elles font travailler sur le calcul modulaire en maths, et utiliser de nombreuses notions du programme en algorithmique.

Histoire de la cryptographie

- Le mot "**cryptographie**" est dérivé du grec kryptos, qui signifie "caché". L'origine de la cryptographie est généralement datée d'environ 2000 avant J.-C., avec la pratique égyptienne des hiéroglyphes.
- Ceux-ci consistaient en des pictogrammes complexes, dont la signification complète n'était connue que d'une élite.
- La première utilisation connue d'un cryptogramme moderne est celle de Jules César (100 av. J.-C. à 44 av. J.-C.), qui ne faisait pas confiance à ses messagers lorsqu'il communiquait avec ses

apcpedagogie.com

gouverneurs et ses officiers.
- C'est pourquoi il a créé un système dans lequel chaque caractère de ses messages était remplacé par un caractère situé trois positions avant lui dans l'alphabet romain.
- Ces derniers temps, la cryptographie est devenue le champ de bataille de certains des meilleurs mathématiciens et informaticiens du monde.
- La capacité de stocker et de transférer en toute sécurité des informations sensibles s'est avérée un facteur essentiel de succès dans la guerre et les affaires.

Vocabulaire

- La Cryptologie est la science des messages secrets. Elle se décompose en **deux disciplines** :
  - **La Cryptographie**, art de transformer un message clair en un message inintelligible par celui qui ne possède pas la clé de déchiffrement. Cependant, on utilise souvent le mot cryptographie comme synonyme de cryptologie.
  - **La Cryptanalyse**, art d'analyser un message chiffré afin de le décrypter quand on ne possède pas la clé de déchiffrement.
- **Chiffre** : anciennement code secret, par extension désigne aussi un algorithme utilisé pour le chiffrement ;
- **Chiffrer** : transformer à l'aide d'une clé de chiffrement un message en clair en un message chiffré, incompréhensible si on ne dispose pas de la clé de déchiffrement correspondante ;
- **Déchiffrer** : retrouver à l'aide de la clé de déchiffrement correspondante le message en clair d'origine à partir d'un message précédemment chiffré à l'aide d'une clé de chiffrement ;
- **Clé de chiffrement** : méthode permettant de chiffrer un message en clair ;
- **Clé de déchiffrement** : méthode associée à une clé de chiffrement et permettant de déchiffrer un message précédemment chiffré ;
- **Décrypter** : retrouver le message en clair correspondant à un message chiffré sans posséder la clé de déchiffrement ni la clé de chiffrement ;
- **Cryptogramme** : message chiffré (incompréhensible si on ne dispose pas de la bonne clé de déchiffrement).

Consignes générales

- On écrit les messages en lettres majuscules et sans accents. Ceci a pour but de simplifier le chiffrement et le déchiffrement des messages.
- Lorsque les messages sont constitués de plusieurs mots ou de plusieurs phrases, on conserve les espaces entre les mots et les signes de ponctuation. Le résultat est de faciliter encore le déchiffrement.

apcpedagogie.com

- Ce n’est pas conforme à la réalité, puisque dans la vraie vie, on veut au contraire compliquer au maximum le cryptogramme, pour empêcher l’adversaire de le décrypter, si possible...
- Plus un cryptogramme est long, plus il est facile à décrypter, car l’adversaire dispose de plus d’indices. Ceci explique pourquoi, dans les exercices, les messages à décrypter seront significativement plus longs que les messages à chiffrer ou à déchiffrer.
- On utilise la correspondance ci-dessous entre les lettres de l’alphabet {A, B, C, . . . , Z} et les nombres {0, 1, 2, . . . , 25}.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Source:http://www.irem.univ-bpclermont.fr/IMG/pdf/CryptoStageSIO.pdf

Types de cryptographie

- La cryptographie peut être symétrique ou asymétrique, selon le type de clé que vous utilisez.

- **La Cryptographie Symétrique**

  - La **cryptographie symétrique** Quoi Il est utilisé depuis le début de l'histoire et depuis très longtemps. Elle est également appelée cryptographie à clé privée ou cryptographie à une clé. Pour l'exécuter et pouvoir crypter et décrypter un message, une seule clé est utilisée que l'expéditeur et le destinataire doivent préalablement connaître. C'est le point faible de cette méthode, car la clé est plus susceptible d'être interceptée par un tiers lorsque l'expéditeur la transmet au destinataire.
  - Dans la **cryptographie symétrique**, une clé très difficile à deviner doit être utilisée, car les ordinateurs d'aujourd'hui peuvent deviner les mots de passe très rapidement. Pour cette raison, il faut considérer que les algorithmes cryptographiques étant publics, il faut garantir que leur force dépend de leur complexité interne et de la longueur de la clé utilisée, pour éviter les attaques par force brute.
  - Pour plus d'information consultez la page suivante:**cryptographie symétrique**

- **La Cryptographie Asymétrique**

  - Aussi connu sous le nom de cryptographie à clé publique. Cette méthode utilise deux clés, une publique et une privée; il n'est donc pas nécessaire de connaître un mot de passe au préalable. La clé publique peut être envoyée et portée à la connaissance de

n'importe qui, tandis que la clé privée est celle qui ne doit être partagée avec personne. Lorsqu'un expéditeur souhaite envoyer un message, il utilise la clé publique pour crypter le message et l'envoyer. Et seul le destinataire avec sa clé privée peut décrypter le message.

- La cryptographie asymétrique Il offre un niveau de sécurité extraordinaire, au point que même la personne qui a chiffré le message ne peut le déchiffrer sans la clé privée. C'est la méthode utilisée dans crypto-monnaies, et c'est une pièce fondamentale de la blockchain pour pouvoir effectuer des opérations et échanger des informations entre égaux en toute sécurité et sans avoir besoin de se faire confiance.
- Pour plus d'information consultez la page suivante:**cryptographie asymétrique**

Applications

- Dans la suite, on définira dans les fonctions qui le nécessitent la chaîne de caractères "abcdefghijklmnopqrstuvwxyz" qu'on appellera **alphabet**.
- **Q1.** Écrire une fonction **position(x)** d'argument un caractère **x** qui renvoie la position de **x** dans la chaîne de caractères alphabet. Cette fonction renverra
  - **-1** si **x** n'est pas élément de alphabet. Par exemple position('a') doit renvoyer 0, position('d') doit renvoyer 3, position('é') doit renvoyer -1

```
def position(x):
    alphabet="abcdefghijklmnopqrstuvwxyz"
    res=-1
    for i in range(26):
        if x==alphabet[i]:
            res=i
    return res
print(position('i'))
```

- **Q2.** On veut écrire une fonction **décalage(x, n)** qui renvoie le caractère obtenu du caractère **x** en le décalant de **n** dans la chaîne alphabet. On voudrait par exemple que décalage('d',3) renvoie 'g', décalage('z',3) renvoie 'c'. On voudrait aussi prendre en compte des décalages négatif (correspondant à un décalage vers la gauche) de sorte que par exemple décalage('g',-3) renvoie 'd' et décalage('c',-3) renvoie 'z'. Si i est la position du caractère **x** à décaler de n, la valeur i+n n'appartient pas nécessairement à l'intervalle [[0; 25]] des positions possibles des caractères dans la chaîne alphabet.
  - Quelle opération arithmétique permet de ramener cette valeur i+n dans l'intervalle [[0; 25]]?
  - Écrire une fonction **décalage(x,n)**.

apcpedagogie.com

```
alphabet="abcdefghijklmnopqrstuvwxyz"
def position(x):
    res=-1
    for i in range(26):
        if x==alphabet[i]:
            res=i
    return res

def decalage(x,n):
    i=(position(x)+n)%26 #position de la lettre decalee
    return alphabet[i]

print(decalage('a',-4))#Résultat est 'w'
```

- **Q3.** Écrire une fonction **codage(texte,n)** d'arguments un entier **n** et une chaîne de caractères texte qui renvoie la chaîne obtenue de texte par codage de César avec un décalage de **n** lettres (seuls les caractères minuscules de l'alphabet latin subissent une modification).
    - Tester la fonction codage sur un texte de votre choix.

```
def position(x):
    res=-1
    for i in range(int(len(x))):
        if x==x[i]:
            res=i
    return res

def decalage(x,n):
    i=(position(x)+n)% (int(len(x))) #position de la lettre decalee
    return x[i]

def codage(texte,n):
    code=""# chaine vide
    for i in range(len(texte)):
        if position(texte[i])==-1: #pas dans l'alphabet
            code=code+texte[i] # caractere non code
        else:
            code=code+decalage(texte[i],n)
            print(n)
    return code
print(codage("apcpedagogie",5))
```

apcpedagogie.com

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/quest-ce-que-la-cryptographie · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com