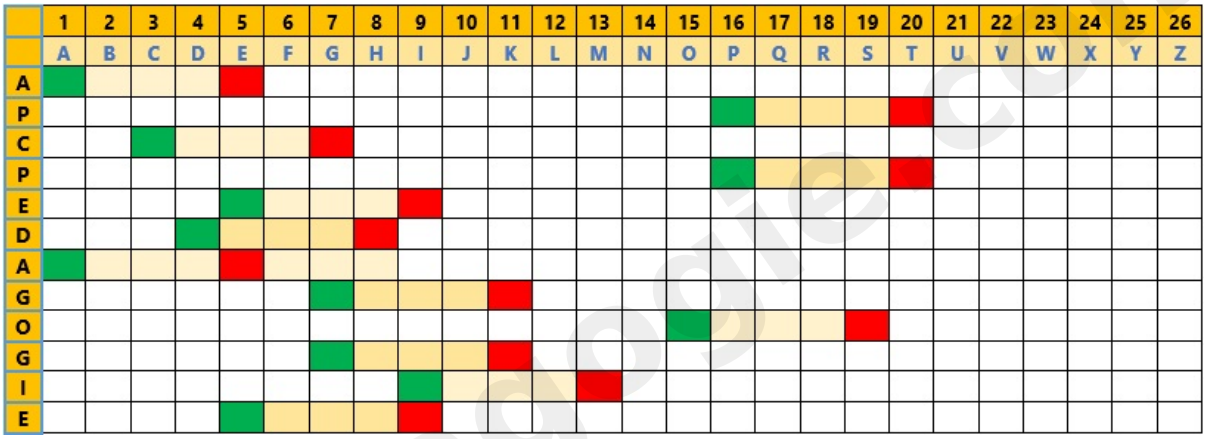
Techniques de cryptographie

1. Objectifs

- Découvrir les techniques de cryptographie

2. Présentation

- La `cryptologie` et la `stéganographie` sont deux procédés visant à protéger des messages afin d'assurer notamment la confidentialité des échanges ou des données.



3. Techniques de cryptographie au cours de l’histoire

- Contrairement à ce que l’on peut penser, la cryptographie n’est pas seulement une technique moderne, ni un produit de l’ère informatique. En effet de tout temps, les hommes ont ressenti le besoin de cacher des informations confidentielles.

- **Cryptage de César**

  - Le `cryptage de César` (empereur romain) est le tout premier code de cryptage qui ait existé.
  - L'un des systèmes les plus anciens et les plus simples est le codage par substitution mono alphabétique (ou alphabets désordonnés). Il consiste à remplacer chaque lettre par une lettre différente.
  - Il existe donc grâce à cette technique 26 façons de coder un message, ce qui fait que ce système a été longtemps utilisé par les armées pendant l’antiquité.

apcpedagogie.com

- Ce procédé très fiable à l'époque est tout de même problématique car il nécessite que les interlocuteurs se souviennent tous deux de la clef.
- De plus, il est évident que la sûreté de ce codage est quasi nulle et qu'il pourrait être déchiffré par n'importe quelle personne qui y mettrait le temps nécessaire.
- C'est un algorithme à translation ou substitution ou à décalage mod 26
- Le chiffre de César ou code de César est un chiffrement par décalage : une des méthodes connues d'encryptage la plus simple et la plus connue. Elle consiste en une substitution de lettres par une autre plus loin dans l'alphabet.
- Par exemple, si l'on utilise un décalage de 4, **A** serait remplacé par **E**, **B** deviendrait **F**, et ainsi de suite.

> ***Texte clair*** *= APCPEDAGOGIE* ***Clé*** *= k = 4* ***Cryptogramme*** *= ETGTIHEKSKMI*

- **Cryptage de Vigenère**

- Pour palier à la faiblesse du code de César, Le diplomate Français du 16ème siècle Blaise de Vigenère eu l'idée d'utiliser un chiffre de César, mais avec un décalage qui change de lettre en lettre grâce à une clé (un mot de longueur arbitraire).
- Pour coder un message, on décale chaque lettre du message par le même décalage qui fait passer la lettre a à la lettre correspondante de la clé écrite sous le message (et répétée autant de fois que nécessaire).
- Le code de Vigenère est un cryptosystème symétrique, ce qui signifie qu'il utilise la même clé pour le chiffrement et le déchiffrement. Il possède la particularité d'être poly-alphabétique, c'est à dire qu' une lettre peut être remplacée par plusieurs autres.
- Mathématiquement, on considère que les lettres de l'alphabet sont numérotées de 0 à 25 (A=0,B=1,C=2 ...). La transformation lettre par lettre se traduit par: Crypté = (Texte + Clé) modulo 26.
- On effectue l'addition de deux caractères puis on trouve le numéro correspondant à la lettre codée. Le modulo nous assure que notre résultat sera compris entre 0 et 25.

- **Carré de Vigenère ou tableau de Vigenère .**

  - Le tableau est constitué des alphabets écrits 26 fois dans des rangées différentes, chaque alphabet décalé cycliquement vers la gauche par rapport à l'alphabet précédent, correspondant aux 26 chiffres de César possibles .

- À différents stades du processus de chiffrement, le chiffrement utilise un alphabet différent de l'une des lignes.
- L'alphabet utilisé à chaque point dépend d'un mot-clé répétitif.
- La table permet de crypter rapidement de manière graphique tout texte utilisant ce chiffre sans recours aux notions de congruences, complexes à manipuler pour les néophytes. Elle met donc à portée de tous un système relativement avancé.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Pour coder un message, on choisit une clé qui sera un mot de longueur arbitraire. On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé. Pour coder, on regarde dans le tableau l'intersection de la ligne de la lettre à coder avec la colonne de la lettre de la clé.

- **Exemples**

  - **Exemple01**: On veut coder le texte "**LA CRYPTOGRAPHIE**" avec la clé "**APCPEDAGOGIE**". On commence par écrire la clé sous le texte à coder :

Message	L	A	C	R	Y	P	T	O	G	R	A	P	H	I	E
Clé	A	P	C	P	E	D	A	G	O	G	I	E	A	P	C

  - Pour coder la lettre **L**, la clé est donnée par la lettre **A**. On regarde dans le tableau l'intersection de la ligne donnée par le **L** de la première colonne (en

bleu), et de la colonne donnée par le **A** de la première ligne (en orangé) On trouve L. Puis on continue.

- Pour coder la lettre **A**, la clé est donnée par la lettre **P**. On regarde dans le tableau l'intersection de la ligne donnée par le **A** de la première colonne (en bleu), et de la colonne donnée par le **P** de la première ligne (en orangé) On trouve L. Puis on continue.

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11-2	A	A	B	C	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
3	C	C	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
15	E	E	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
9	G	G	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
13	H	H	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
14	I	I	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	k	k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
1	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
8	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
12-6	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
10-4	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
7	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
5	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Le texte chiffré est :**LPEGCSTUUXITHXG**
- Cet algorithme de cryptographie comporte beaucoup de points forts. Il est très facile à utiliser, et le déchiffrement est tout aussi facile si on connait la clé.
- Il suffit, sur la colonne de la lettre de la clé, de rechercher la lettre du message codé. A l'extrémité **gauche de la ligne, on trouve la lettre du texte clair**.

4. Cryptosystèmes actuels

5. Applications

- **Application:01**

  - **Énoncé**

- Un des plus anciens systèmes de cryptographie (aisément déchiffrable), le système de César qui consiste à décaler les lettres d'un message pour le rendre illisible. Ainsi, les **A** deviennent des **B**, les **B** des **C**, etc. Et les **Z** deviennent des **A** avec un décalage de 1
- **Exemple**
  - Si "**chaineacrypter**"="APCPEDAGOGIE" et la clé est 4, alors la chaine "**chaineCrypte**" crypté qui sera affichée est "ETGTIHEKSKMI"
- Écrivez un programme (Python ou php) qui demande à la foi une chaine "**chaineacrypter**" et une clé "**cle**" à l'utilisateur et qui la code dans une chaine "**chaineCrypte**" selon ce principe (**César**).
- Le même programme doit permet à l'utilisateur de décrypter une chaîne de caractère
- Écrire un script Python qui chiffre (ou déchiffre selon le choix de l'utilisateur) une chaîne de caractères entrée au clavier avec une clé (i.e.un décalage) choisi aussi par l'utilisateur. On définira les fonctions chiffrer et déchiffrer.

- **Solution**

  - **Python**

    Cryptage

```
chaineacrypter=input("Saisir une chaine non vide")
cle=int(input("Saisir un nombre entre 1 et 26"))

acrypter=chaineacrypter.upper()
lg=len(acrypter)
chaineCrypte=""

for i in range(lg):
    if acrypter[i]==' ':
        chaineCrypte+=' '
    else:
        asc=ord(acrypter[i])+cle
        chaineCrypte+=chr(asc+26*((asc<65)-(asc>90)))

print (chaineCrypte)
```

    Décryptage

apcpedagogie.com

```
chaineCrypte=input("Saisir une chaine non vide")
cle=int(input("Saisir un nombre entre 1 et 26"))

lg=len(chaineCrypte)
chaineClair=""

for i in range(lg):
    if chaineCrypte[i]==' ':
        chaineClair+=' '
    else:
        asc=ord(chaineCrypte[i])-cle
        chaineClair+=chr(asc+26*((asc<65)-(asc>90)))

print (chaineClair)
```

- **Php**

- **Application:02**

  - **Énoncé**

    - **1.** Qu'apporte le **chiffrement de vigénère** en matière de sécurité par rapport à une simple substitution alphabétique ?
    - **2.** En utilisant le chiffre de Vigen`ere avec la cl´e = ”VIGENERE”, chiffrer le message "**VRAIMENT ETONNANT CECI**".

  - **Solution**

    - **1.** Vigénère apporte un plus car une même lettre peut être chiffrée différemment dans le texte ce qui complique l'analyse statistique. Vigènere est donc plus solide.
      - **Remarque**: il y a des attaques connues contre Vigènere: déterminer d'abord la taille de la clef puis faire des attaques statistiques. Cf TD.
    - **2.** message chiffrée = "**QZGMZIEXZBURAEEXXMIM**"

- **Application:03**

  - **Énoncé**

apcpedagogie.com

- Écrivez un programme (Python ou php) qui demande à la foi une chaine "**chaineacrypter**" et une clé "**cle**" à l'utilisateur et qui la code dans une chaine "**chaineCrypte**" selon le principe de Vigénère.
- Le même programme doit permet à l'utilisateur de décrypter une chaîne de caractère

- **Solution**

  - **Python**

    Cryptage

```
def vigenere(c, cle):
    indice_cle = 0
    msg_code = ""

    for i in range(0, len(c)):
        if 'A' <= c[i] <= 'Z':
            msg_code +=  chr((((ord(c[i]) - ord('A')) +
(ord(cle[indice_cle]) - ord('A'))) % 26) + ord('A'))
            indice_cle =  (indice_cle + 1) % len(cle)
            print(ord(c[i]))
        else:
            msg_code +=  c[i]
    return msg_code
chaine_a_crypter=input("Donnez la chaine de caractere")
chaine_a_crypter=chaine_a_crypter.upper()
cle=input("Donnez la chaine de caractere")
cle=cle.upper()
print(vigenere(chaine_a_crypter, cle))
```

    Décryptage

```
def decode_vigenere(c, cle):
    indice_cle = 0
    msg_code = ""

    for i in range(0, len(c)):
        if 'A' <= c[i] <= 'Z':
            msg_code +=  chr((((ord(c[i]) - ord('A')) -
(ord(cle[indice_cle]) - ord('A'))) % 26) + ord('A'))
            indice_cle =  (indice_cle + 1) % len(cle)
        else:
```

apcpedagogie.com

```
            msg_code +=  c[i]
    return msg_code
chaine_a_decrypter=input("Donnez la chaine de caractere")
chaine_a_decrypter=chaine_a_decrypter.upper()
cle=input("Donnez la chaine de caractere")
cle=cle.upper()
print(decode_vigenere(chaine_a_decrypter, cle))
```

- **Php**

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/techniques-de-cryptographie · téléchargé le 08/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com