LETTRES SORBONNE UNIVERSITÉ

2019-2020

# M1SOL020

# Epistémologie de l'Informatique

## TD4

## Sécurité et Cryptographie

Gaël Lejeune, Sorbonne Université

Inspiré d'Agnès Delaborde 2015-2016

## Objectifs

- Comprendre les enjeux du cryptage
- Savoir représenter algorithmiquement une méthode de codage et de décodage

# 1 Méthodes de cryptage à clé secrète

## 1.1 Chiffrement par décalage : Chiffre de César

C'est un chiffrement par décalage ; chaque lettre de l'alphabet correspond à une autre lettre, selon un décalage de tout l'alphabet vers la droite ou la gauche.

| Clair | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Chiffré | 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 |

Table 1: Correspondance entre lettres en clair et lettres chiffrées (chiffrement 1)

### 1.1.1 Comprendre

- Dans le tableau 1, quelle est la clé permettant de déchiffrer le texte ?
- Connaissant la clé, que signifient ces textes ?
  - DYHFD HVDUP RULWX ULWHV DOXWD QW?
  - DO, HAM DF WDHVW
- Quelle est l'importance d'une **ponctuation inadéquate** ?
- Étudiez maintenant le chiffrement 2 (tableau 2), quelle est la clé ?

| Clair | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Chiffré | 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 |

Table 2: Correspondance entre lettres en clair et lettres chiffrées (chiffrement 2)

- Que signifie YTC AYCQYP dans ce chiffrement ?
- Connaissant la clé, comment pouvons-nous représenter algorithmiquement le décodage d'un texte ?

### 1.1.2 Coder le codage

Nous allons contribuer au codage en PYTHON une fonction permettant de chiffrer et de déchiffrer un texte selon une clé donnée. Par commodité on se limitera aux lettres majuscules. Utilisez le code ci-dessous:

```
def coder(message, cle):
  alphabet =['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']
  message_code = ""
  for caractere in message:
    position = alphabet.index(caractere)
    caractere_code = alphabet[position+cle]
    message_code+=caractere_code
  return message_code

message_a_coder = "BONJOUR"
cle = 5
message_bien_code = coder(message_a_coder, cle)

print("message :", message_a_coder)
print("cle :", cle)
print("message code :", message_bien_code)
```

- Le code fonctionne-t-il en mettant un clé valant 25? Comment corriger ?
- Comment peut-on créer une fonction de décodage ?

## 1.2 Chiffrement par substitution : Chiffre de Vigenère

Il s'agit d'un chiffrement polyalphabétique : une même lettre peut être remplacée par différentes lettres, selon la position de la lettre dans le message. (au contraire, le codage de César est mono-alphabétique).

- Utilisez le programme PYTHON ci-dessous (téléchargez la resource associée sur Moodle):

```
import json
f = open("Epistemo-TD4-vigenere.json")
dico_vigenere = json.load(f)
f.close()
message_base = "TOTO"#seulement des majuscules
cle = "TOKEN"#la clé n'a pas de signification
while len(cle)<len(message_base):
  cle+=cle
print("Message à coder : ",message_base)
print("Cle : ", cle)
message_code = ""
cpt = 0#va encoder la position où l'on est dans le message à
coder
for caractere in message_base:
  caractere_cle = cle[cpt]
```

```
    caractere_code = dico_vigenere[caractere][caractere_cle]
    message_code+=caractere_code
    cpt+=1
print("Message code : ", message_code)
```

- codez "BONJOUR" avec la clé "INFO" puis "SALUT" avec la clé "VRAI"
- Vérifiez le résultat en utilisant la table de Vigenère en annexe (tableau 3 page 4),
- Examinez dans un éditeur la ressource `Epistemo-TD4-vigenere.json` qui associe à chaque lettre, selon chaque clé, un équivalent codé. Comparez la avec le tableau 3
- Reconstituez l'algorithme de codage choisi, comment procéder autrement ?
- Que se passe-t-il si on choisit une clé de longueur 1 ?
- Avec le code fourni, peut-on choisir n'importe quel message à coder ?
- Quel est le problème de sécurité connu sur ce type de chiffrement ?

## 1.3 Chiffrement par substitution : Le Scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48‡8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;

### 1.3.1 Méthode de déchiffrage

- Déterminer la langue
- Analyse des fréquences des caractères de la langue en question
- Remplacer les caractères codés par des caractères de fréquence comparable
- Repérer des mots

### 1.3.2 Réalisation

Première approche ("5", "3", "‡", "†"... dans le code sont aussi fréquents que "a", "g", "o", "d"... en langue anglaise) :

agoodg0a))inthe2i)ho.)ho)te0inthede
¶i0))eat1ort:onedegree)andthirteen9i
nute)northea)tand2:north9ain2ran-h)e
¶enth0i92ea)t)ide)hoot1ro9the0e1te:eo
1thedeath)heada2ee0ine1ro9thetreeth
roughthe)hot1i1t:1eetout

Le texte après décodage complet (et ajout des espaces):

A good glass in the bishop's hostel in the de
vil's seat forty-one degrees and thirteen mi
nutes north east and by north main branch se
venth limb east side shoot from the left eye o
f the death's head a bee line from the tree th
rough the shot fifty feet out.

### 1.4 Le système du dictionnaire (chiffre du livre)

1 Et c'était bien exact : elle ne mesurait plus que vingt-cinq centimètres.
2 Son visage s'éclaira a l'idee qu'elle avait maintenant exactement la taille
3 qu'il fallait pour franchir la petite porte et pénétrer dans l'adorable jardin.
4 Néanmoins elle attendit d'abord quelques minutes pour voir si elle allait
5 diminuer encore : elle se sentait un peu inquiète a ce sujet: "car, voyez-
6 vous, pensait Alice, a la fin des fins je pourrais bien disparaître tout a fait,
7 comme une bougie. En ce cas, je me demande a quoi je ressemblerais." Et
8 elle essaya d'imaginer a quoi ressemble la flamme d'une bougie une fois
9 que la bougie est éteinte, car elle n'arrivait pas a se rappeler avoir jamais
10 vu chose pareille.
*Lewis Carroll (1865), Alice au pays des Merveilles. Edition du groupe "Ebooks libres et gratuits". Page 12*

- D'après le texte ci-dessus, construisez un message crypté à partir d'un code "numéro de ligne-numéro de caractère", où chaque symbole du code sera unique.
- Améliorez le cryptage avec une substitution homophonique, rédigez l'algorithme.

# 2 Cryptage à clé publique

- Limitation(s) des systèmes de chiffrement à clé privée ?
- Quel est alors l'apport de l'utilisation d'un système à clé publique ? (ex. RSA)

**Approfondissement**

- Chiffrement de César : `https://www.youtube.com/watch?v=g8RmT-CwTMo`
- Chiffrement de Vigenère : `https://www.youtube.com/watch?v=rUlqxHGKJ68`
- La machine Enigma : `https://www.youtube.com/watch?v=oGDPtm8pYPM`

| | 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 |

Table 3: Table de Vigenère , en colonne la lettre en clair, en ligne la clé, à l'intersection la lettre codée