

2024
2025

Travaux Pratiques n°3

Cryptologie

LARCHER STEPHANE



Travaux Pratiques n°3

Cryptologie

Table des matières

| | |
|--|----------|
| <i>Exercice I - Méthode de Vignère</i> | <i>2</i> |
| <i>Exercice II – Indice de Friedman.....</i> | <i>3</i> |
| <i>Exercice III - Indice de Friedman</i> | <i>4</i> |
| <i>Exercice IV – Chiffre de Playfair</i> | <i>5</i> |
| <i>Exercice V – Chiffre de Playfair</i> | <i>6</i> |

Exercice I - Méthode de Vignère

Je vous propose de déchiffrer un message chiffré avec la méthode inventée par Blaise de Vignère. La clé est FCSC et le message chiffré est :

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

Exercice II – Indice de Friedman

Je vous propose de trouver le *Flag* à partir de données de sortie et du code source utilisé de trouver les données d'entrée :

i. Données en sortie :

« d91b7023e46b4602f93a1202a7601304a7681103fd611502fa684102ad6d1506ab
6a1059fc6a1459a8691051af3b4706fb691b54ad681b53f93a4651a93a1001ad3c40
06a825 »

ii. Code source utilisé :

```
import os
from Crypto.Util.number import long_to_bytes
from Crypto.Util.strxor import strxor

FLAG = open("flag.txt", "rb").read()

key = os.random(4) * 20
c = strxor(FLAG, key[:len(FLAG)])
print(c.hex())
```

Exercice III - Indice de Friedman

Le texte suivant résulte du chiffrement d'un texte français (traduit de l'anglais) par une substitution monoalphabétique.

« v ubcfb osu ymoqsuu n cxqfj dqmfnu ub vjcfqu juz amqjmruz zmsscfusb bqflu
auoquz hfszbms zwfba ju wusbms qusbqu ncsz ju vmo z uddmqvcfb n uxfbuq ju xusb
wcoxcfz fj eczzc qcefnuwusb jc emqbu xfbquu no ijm v nuz wcfzmsz nu jc xfvbmfuq ecz
czzul qcefnuwusb vueusncsb emoq uweuvauq kou z usrmoddqu us wuwu buwez kou jof
os bmoqifjjms nu emozzfuqu ub nu zciju ju acjj zusbcfb ju vamo vofb ub ju xfuog bcefz c
j osu nu zuz ugbquwfbuz osu cddfvau nu vmojuoq bqme xczbu emoq vu nuejmfuwusb
fsbuqfuq ubcfb vjmouu co woq ujju quequzusbcfb zfwejuwusb os usmqwu xfzcru jcqru
nu ejoz n os wubqu ju xfzcru n os amwwu n usxfqms kocqcsbu vfsk csz c j uecfz zu
wmozbcvau smfqu cog bqcfbz cvvusbouz ub iucog hfszbms zu nfqfruc xuqz j uzvcjfuq fj
ubcfb fsobfju n uzzcpuq nu equsnqu j czvuszuq wuwu cog wufjjuoquz uemkouz fj
dmsvbfmsscfb qcquwusb cvboujjuwusb n cfjjuoqz ju vmoqcsb ujuvbqfkou ubcfb vmoeu
ncsz jc ymoqsuu v ubcfb osu nuz wuzoquz n uvmsmwfu eqfzuz us xou nu jc zuwcfsu nu
jc acfsu »

Décrypter le texte

Exercice IV – Chiffre de Playfair

- i. Prenons la clé "OPENAI" et créez la grille (5x5)
- ii. Message à déchiffrer : "HELLO WORLD" (remarquez qu'il y a des espaces ...)

Exercice V – Chiffre de Playfair

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de Playfair sur un texte en langue française (traduit de l'anglais) dans lequel les espaces ont été supprimées :

celoafvzlslvfenovlflebibaebvxaevfrybkrapuakroeuclyxv
mxuicgvavlulcvrurmvasvmgoeavxmiatfaeugholvtevreoezd
luvevluixyezcvvesiavmzvesloezlbeaixaufslmzhomoljeprf
vlmoljlfeicfxvlecasvtevrermalmiqvoeucesalmzxmesrgvl
rmlsuffvvzebqvarzevasvlvtevlvuclypelvroamevodvouckx
osvmmzaucearcvrafoevxafthbxaevkgbouflyluecavkgoelcay
cgvllfaurmfcxklsevkioelscgamoeavxmllaayobxvmvflufgnea
ovulliceozcsvkvomvsmvfllevivavlklaeaseescvvldeaebv
mzrmklayucabymxmecyoqreckrfeyzaevgbivlmovzebnovflvtev