

TP1- Cryptographie Classique

Exercice 1 :



Rechercher un outil

★ RECHERCHE SUR DCode PAR MOTS-CLÉS :
Tapez par exemple 'scrabble'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

Mode Force Brute : les 26 décalages (pour l'alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) sont testés et triés du plus probable au moins probable.

↑↓	↑↓
→10 (←16)	Quoique ce detail ne touche en aucune maniere au fond meme de ce que nous avons a raconter, il n'est peut-etre pas inutile, ne fut-ce que pour etre exact en tout, d'indiquer ici les bruits et les propos qui avaient couru sur son compte au moment ou il etait arrive dans le diocese.

CODE CÉSAR
Cryptographie › Chiffrement par Substitution › Code César

DÉCHIFFREMENT DU CODE CÉSAR

★ MESSAGE CHIFFRÉ PAR CODE CÉSAR (?)

Aeysaao mo nodksv xo dyemro ox kemexo wkxsobo ke pyxn
wowo no mo aeo xyec
kfyxc k bkmyxdob, sv x'ocd zoed-odbo zkc sxedsvo, xo ped-
mo aeo zyebo odbo
ohkmd ox dyed, n'sxnsaeob sms voc lbesdc od voc zbyzyc
aes kfksoxd myebe

Tester tous les décalages possibles (alphabet de 26 lettres A-Z)

► DÉCHIFFRER AUTOMATIQUEMENT

DÉCHIFFREMENT MANUEL ET PARAMÈTRES

★ DÉCALAGE/CLÉ (NOMBRE) : 3

☒ UTILISER L'ALPHABET FRANÇAIS (26 LETTRES DE A À Z)
☐ UTILISER L'ALPHABET FRANÇAIS ET DÉCALER AUSSI LES CHIFFRES 0-9
☐ UTILISER L'ALPHABET LATIN DU TEMPS DE CÉSAR (23 LETTRES, NI J, NI U, NI W)
☐ UTILISER LA TABLE ASCII (0-127) COMME ALPHABET
☐ UTILISER UN ALPHABET PERSONNALISÉ (CARACTÈRES A-Z0-9 SEULEMENT)

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

► DÉCHIFFRER

Voir aussi : Chiffre ROT (Rotation) – Chiffre par Décalages

Il existe le site dcode qui peut faire des tests en force brute et deviner le décalage exact, sinon manuellement on peut remarquer que la lettre "o" est la lettre la plus fréquente ce qui devrait correspondre à la lettre "e" dans l'alphabet français, et on réalise donc un décalage de 10 sur toutes les lettres et on obtient ce texte :

Quoique ce detail ne touche en aucune maniere au fond meme de ce que nous avons a raconter, il n'est peut-etre pas inutile, ne fut-ce que pour etre exact en tout, d'indiquer ici les bruits et les propos qui avaient couru sur son compte au moment ou il etait arrive dans le diocese.

Exercice 2 :

1. De quel type de chiffrement est la machine Enigma ?

La machine Enigma utilise un chiffrement par substitution, où chaque lettre est remplacée par une autre. Ce qui rend le message compliqué à déchiffrer, c'est que la substitution change à chaque frappe de touche.

2. Calculer le nombre de clés possibles dans une machine Enigma avec choix parmi cinq rotors et qui utilise six fiches

Pour une machine Enigma avec cinq rotors parmi lesquels on en choisit trois, et avec six fiches connectées sur le tableau de connexion, il y a environ 68 quintillions (10^{30}) de combinaisons possibles. Cela signifie qu'il y a énormément de façons différentes de configurer la machine pour chiffrer ou déchiffrer un message.

3. Quelles sont les techniques de cryptanalyse qui ont permis de casser le chiffrement d'Enigma ?

Le chiffrement d'Enigma a été cassé grâce à plusieurs méthodes. D'abord, les opérateurs faisaient parfois des erreurs qui donnaient des indices aux cryptanalystes. Ensuite, les analystes devinaient des mots qui pouvaient être dans le message chiffré, ce qui les aidait à trouver la clé. Des machines spéciales ont aussi été créées pour tester rapidement des millions de combinaisons possibles. Enfin, les Alliés ont capturé des machines Enigma et des documents, ce qui a beaucoup aidé à comprendre comment casser le code.

Exercice 3 :

1. Chiffrez le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "SECURITE":

« Introduction a la cryptographie appliquee »

On peut le réaliser en utilisant l'outil dcode comme suit :



On utilise dcode et on obtient le message chiffré suivant : Arvlfnglmqh r tt gjcrnfokehlky rxipauwyv

On peut de même le réaliser de manière manuelle comme suit :

Clair	I	N	T	R	O	D	U	C	T	I	O	N
Clé	S	E	C	U	R	I	T	E	S	E	C	U
Décalage	18	4	2	20	17	3	19	4	18	4	2	20
Chiffré	A	R	V	L	F	L	N	G	L	M	Q	H

Clair	A	/	L	A
Clé	R	/	I	T
Décalage	17	/	3	19
Chiffré	R	/	T	T

Clair	C	R	Y	P	T	O	G	R	A	P	H	I	E
Clé	E	S	E	C	U	R	I	T	E	S	E	C	U
Décalage	4	18	4	2	20	17	3	19	4	18	4	2	20
Chiffré	G	J	C	R	N	F	O	K	E	H	L	K	Y

Clair	A	P	P	L	I	Q	U	E	E
Clé	R	I	T	E	S	E	C	U	R
Décalage	17	3	19	4	18	4	2	20	17
Chiffré	R	X	I	P	A	U	W	Y	V

On retrouve ainsi le même résultat.

2. Le texte suivant a été obtenu en appliquant le chiffrement de Vigenère sur un texte en langue française dans lequel les espaces ont été supprimées :

Pour répondre à cette question, nous avons appliqué le test de Kasiski sur le texte chiffré :

ZBPUEVPUQSDLZGLLKSOU SVPASFPDDGGAQWPTDGPTZWEEMQZRDJTDDEF EKEFERDPRRCYND
GLUAOW
CNBPTZZRBVPSSFPASHPNCOTEMHAEQRFERDLRLWWERTLUSSFIKG OEUSWOTFDGQSYASRLNR
ZPPDH
TTICFRCIWURHCEZRPMHTPUWIYENAMRDBZYZWELZUCAMRPTZQSEQCFGDRFRHRPATSEPZGFN
AFFIS BPVDBLISRPLZGNEMSWAQOXPDSEEHBEKSDPTDTTQSDDDGXURWNIDBDDDLNCS D

Nous avons utilisé le logiciel <https://fr.planetcalc.com/8550/>

Test de Kasiski

Texte codé

```
ZBPUEVPUQSDLZGLLKSOUSVPASFDDGGAQWPTDGPTZWEEMQZRDJTDDEFEKEFERDPRRCYNDGLUAOW  
CNBPTZZRBPSSFPASHPNCOTEMHAEQRFERDLRLWWERTLUSSFIKGOEUSWOTFDGQSYASRLNRZPPDH  
TTICFRCIWURHCEZRPMTUWIYENAMRDBZYWELZUCAMRPTZQSEQCFGDRFRHRPATSEPZGFNAFFIS  
BPVDBLISRPLZGNEMSWAQXPDSSEHBEEKSDPTDTTQSDDDGXURWNIDBDDPLNCSD
```

CALCULER

Précision de calcul
Chiffres après la virgule décimale : 2

Longueurs de clefs probables



Longueur de la clef	Distances correspondantes
4	80 %
14	13.33 %
33	6.67 %

Selon le résultat obtenu, la longueur de clé 4 était le plus probable. Nous avons donc testé cette clé sur le logiciel dcode et nous avons obtenu le texte suivant :



Rechercher un outil

★ RECHERCHE SUR dCODE PAR MOTS-CLÉS :
Tapez par exemple 'cesar'

★ PARCOURIR LA [LISTE COMPLÈTE DES OUTILS](#)

Résultats

Vigenere ?
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

↑↓	↑↓
	ANEUFHEURES LASALLE DUTHEATRE DES VARIETES AIT ENCORE VIDE QUELQUES PERSONNES AUBAL
	CONETALORCHESTRE ATTENDAIENT PERDUS PARMILS FAUTEUILS DE VELOURS GRENAT DANS LE PETIT JOUR DULUSTRE ADEMIFEU X UNE OMBRE NOYAIT LA GRANDE TACHE ROUGE DURIDE AUE TPAS UN BRUIT
ZOLA	NE VENAIT DELASCENELARAMPEE TEINTELESPUITRES DES MUSICIENS DE BANDES

CHIFFRE DE VIGENÈRE

Cryptographie > Chiffre Poly-Alphabétique > Chiffre de Vigenère

DÉCHIFFREMENT DE VIGENERE

★ MESSAGE CHIFFRÉ PAR VIGENERE ?

```
EBERDPRKCTNDGLOUOW  
CNBPTZZRBPSSFPASHPNCOTEMHAEQRFERDLRLWWERTLUSSFIKGOEUSWO  
TFDGQSYASRLNRZPPDH  
TTICFRCIWURHCEZRPMTUWIYENAMRDBZYWELZUCAMRPTZQSEQCFGDRF  
RHRPATSEPZGFNAFFIS  
BPVDBLISRPLZGNEMSWAQXPDSSEHBEEKSDPTDTTQSDDDGXURWNIDBDDPLNCSD
```

PARAMÈTRES

★ LANGUE DU MESSAGE CLAIR : Français

★ ALPHABET : ABCDEFGHIJKLMNOPQRSTUVWXYZ

► DÉCHIFFRER AUTOMATIQUEMENT

MÉTHODE DE DÉCHIFFREMENT

☐ AVEC LA CLÉ/LE MOT-CLÉ DE CHIFFREMENT : 3

☒ AVEC LA LONGUEUR/TAILLE DE LA CLÉ, NOMBRE DE LETTRES : 4

☐ AVEC SEULEMENT UN MORCEAU DE LA CLÉ : CL?

☐ EN CONNAISSANT UN MOT DU TEXTE CLAIR : CODE

☐ CRYPTANALYSE DE VIGENERE (TEST DE KASISKI)

► DÉCHIFFRER

Soit, avec les espaces :

A NEUF HEURES LA SALLE DU THEATRE DES VARIETES ETAIT ENCORE VIDE QUELQUES
PERSONNES AU BALCON ET A L'ORCHESTRE ATTENDAIENT PERDUES PARMIS LES FAUTEUILS DE
VELOURS GRENAT DANS LE PETIT JOUR DU LUSTRE A DEMI FEUX UNE OMBRE NOYAIT LA
GRANDE TACHE ROUGE DU RIDEAU ET PAS UN BRUIT NE VENAIT DE LA SCENE LA RAMPE
ETEINTE LES PUPITRES DES MUSICIENS DE BANDES

2. Le texte suivant a été obtenu en appliquant le chiffrement de Vigenère sur un texte en langue française dans lequel les espaces ont été supprimées :

gmyxzoocxziancxktanmyolupjrtgxwshctzluibuic

yzwxyqtvqxzukibkotuxkagbknmimmzzyajvjzampqyz

loinoiqknaumbknknvkaiakgwtnilvvzvqydmvjcximr

vzkilxzqtomrgqmdjrzyazvzmmyjgkoaknkuiaivknvvy

Il nous a été demandé d'utiliser l'indice de coïncidence pour trouver la clé probable et ainsi déchiffrer ce message.

L'indice de coïncidence est une méthode qui permet de, par son indication, avoir une idée sur la répartition des lettres dans le texte chiffré, et ainsi trouver la langue du texte en clair.

Nous avons utilisé dcode pour trouver l'indice de coïncidence du message

<https://www.dcode.fr/indice-coincidence> et nous avons trouvé un indice de 0.050

Rechercher un outil

★ RECHERCHE SUR DCODE PAR MOTS-CLÉS :
Tapez par exemple 'sudoku'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

gmyxzoocxziancxktanmyolupjrtgxwshctzluibuic

↑↓

L	IC
L=3	IC ≈ 0.07598 ± 0.011
L=6	IC ≈ 0.07605 ± 0.013
L=15	IC ≈ 0.07354 ± 0.016
L=9	IC ≈ 0.07433 ± 0.021
L=2	IC ≈ 0.05168 ± 0.023
L=12	IC ≈ 0.07173 ± 0.024

INDICE DE COÏNCIDENCE
Cryptographie > Cryptanalyse > Indice de Coïncidence

CRYPTANALYSE AVEC L'INDICE DE COÏNCIDENCE

★ MESSAGE À ANALYSER

gmyxzoocxziancxktanmyolupjrtgxwshctzluibuic
yzwxyqtvqxzukibkotuxkagbknmimmzzyajvjzampqyz
loinoiqknaumbknknvkaiakgwtnilvvzvqydmvjcximr
vzkilxzqtomrgqmdjrzyazvzmmyjgkoaknkuiaivknvvy

★ CARACTÈRES ☐ LETTRES A-Z UNIQUEMENT
☐ TOUS LES CARACTÈRES (MÊME NON IMPRIMABLES)
☒ TOUS SAUF ESPACES (ET ASSIMILÉS)

▶ CALCULER L'IC

▶ CALCULER LES LONGUEURS DE CLÉ PROBABLES

▶ CALCULER LE NOMBRE PROBABLE D'ALPHABETS UTILISÉS

Voir aussi : Reconnaître un Chiffrement – Analyse des Fréquences

Exercice 4 :

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement affine sur un texte en langue française dans lequel les espaces ont été supprimées :

ntjimpumgxpgtstgqpgtxpnchumtputgfsftgthnngxnchumwx
ootrtumhpyctgktjqtjchfooxujqhgztumxpotjxotfoqtohr
xumhzutwftgtopfmntjmpuatmfmshodpfrxpjjtqtghbxuj

Après avoir appliqué le déchiffrement affine, nous obtenons ce texte :

cestunroudeverdureouchanteuneriviereaccrochantfo
llementauxherbesdeshailionsdargentoulesoleildelam
ontagnefiereluitcestunpetitvalquimoussederayons

Avec les espaces :

C'est un trou de verdure où chante une rivière, accrochant follement aux herbes des haillons d'argent où le soleil de la montagne fière luit. C'est un petit val qui mousse de rayons.

Exercice 5 :

Le chiffrement "one-time pad" repose sur l'utilisation d'une clé unique pour chaque message. Cependant, dans ce cas, la même clé a été utilisée pour chiffrer deux messages distincts, ce qui fragilise le chiffrement. L'objectif est de retrouver les textes clairs possibles à partir des deux chiffrés donnés : "HQQYAJT" et "RJAJPWG".

One-Time Pad enciphering

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

E 4 K 10

N 13 E 4

I 8 Y 24

G 6 W 22

M 12 O

A 0 R

plain text: ENIGMA

keyword: KEYWORD

On se rend sur ce site : <https://github.com/OpenTaal/opentaal-wordlist/blob/master/wordlist.txt>

et on télécharge les documents txt qui vont nous servir pour le corpus.

Le programme fonctionne en trois étapes principales :

1. Conversion des caractères en indices : La fonction `char_to_index` permet de convertir chaque caractère du texte chiffré en un index numérique correspondant à sa position dans l'alphabet. Par exemple, 'A' est converti en 0, 'B' en 1, etc.
2. XOR entre les caractères : Le chiffrement "one-time pad" utilise l'opération XOR entre le texte clair et la clé pour générer un chiffré. Étant donné que la même clé a été utilisée pour deux textes différents, en effectuant un XOR entre les deux chiffrés, on obtient la différence entre les deux textes clairs.
3. Recherche dans le corpus : Une fois la différence entre les deux textes clairs calculée, le programme recherche dans un corpus de mots français (qui doit être préalablement défini) tous les couples de mots susceptibles d'être les textes clairs à l'origine des chiffrés.

```
PS C:\Users\rahmo\Documents\Git\EFREI-Crypto-MI\TP 1 - Cryptographie Classique> py .\Exercice5.py
Différence des deux chiffrés : [22, 25, 16, 17, 15, 5, 21]
Corpus chargé avec 1000 mots.
Mot: AAFITNK -> Déchiffré: WZVCHIF
Mot: AAIBAAR -> Déchiffré: WZYQPFE
Mot: AAIBARE -> Déchiffré: WZYQPUR
Mot: AAITJES -> Déchiffré: WZYCGBH
Mot: AALBEEK -> Déchiffré: WZBQLBF
Mot: AALBEKE -> Déchiffré: WZBQLPR
```

Et on rajoute les logs pour vérifier que le programme marche bien.