EPI

Progression sur la Cryptologie

EPI L'histoire des secrets ou les secrets de l'Histoire

Sommaire :

Introduction

La cryptologie, qui signifie la science du secret, regroupe la cryptographie et la cryptanalyse. C'est une science qui est apparue à la naissance de l'écriture et qui s'est développée avec l'apparition de grands empires toujours en lutte pour leurs frontières : la transmission sûre d'informations est devenue une priorité toujours plus importante pour les gouvernements et les individus. Cette science continue encore à progresser avec des codes toujours plus sécurisant. Il y a eu de grandes avancées notamment dans les années 1970.

La cryptographie consiste à crypter un message, c'est-à-dire le rendre illisible pour toutes les personnes excepté le destinataire du message.

La cryptanalyse cherche à décrypter un message sans en connaître la clé de chiffrement. On dit alors qu'on tente de « casser » le chiffrement.

La cryptologie a été très utile durant les différentes guerres. Par exemple, la machine Enigma cryptait des messages secrets pour l'Allemagne nazie et les Alliés, notamment Alan Turing, tentaient de les décrypter.

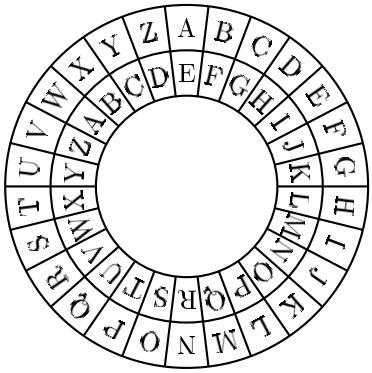
Cette science est aussi utilisée dans notre vie de tous les jours, afin d'assurer la confidentialité des communications et notamment la sécurité de toutes les transactions bancaires (utilisation des smartphone, paiement par carte bleue (RSA)...).

Nous allons découvrir trois méthodes de cryptage, la méthode de César, le chiffrement affine, qui sont deux méthodes de substitution monoalphabétique et le chiffre de Vigenère, qui est une méthode substitution polyalphabétique.

I Code de César

Méthode :

Le texte crypté s'obtient en remplaçant chaque lettre du texte clair par la lettre qui est située trois rangs plus loin.
La longueur du décalage constitue la clé du chiffrement.



Référence historique :

La méthode a été utilisée par Jules César pour certaines de ses correspondances secrètes, notamment militaires.

I.1 TP 1 : Méthode de César

I.1.a) Papier/crayon

Exercice n° 1 — Messages secrets

1. Décrypte le message « ELHQ MRXH », crypté avec la méthode de César.
2. Dans cette question la clé de chiffrement est 17.
   (a) Crypte le message « ESSAI ».
   (b) Décrypte le message « RJJVQ JZDGCV » .

I.1.b) Avec le tableur

Construire, avec le tableur de LibreOffice un tableau permettant de crypter et de décrypter un message avec une clé donnée.

Indications :

— Voici un exemple de feuille dans laquelle les trois dernières lignes sont remplies automatiquement par les formules :

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
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

Clé	3							
Message clair	E	X	E	R	C	I	C	E
Nombre	4	23	4	17	2	8	2	4
Nombre crypté	7	0	7	20	5	11	5	7
Message Crypté	H	A	H	U	F	L	F	H

— « =MOD(A1 ;A2) » renvoie le reste de la division euclidienne de A1 par A2. Ce qui est nécessaire pour avoir des nombres toujours compris entre 0 et 25.

— « =RECHERCHE(B5 ;$B2 :$AA2 ;$B1 :$AA1) » récupère la valeur dans B5 puis recherche dans la plage B2 :AA2 cette valeur. Une fois la valeur trouvée, elle renvoie la valeur correspondante de la plage B1 :AA1. Ici $ sert à pouvoir étirer la formule sans que le numéro de colonne ne change.

Exercice n° 2

A l'aide du tableur :

1. Crypter le message « JADORELESMATHS », avec la clé 21.
2. Décrypter le message « XZNVMIZMVXJIOZKVNYZNVGVYZ », avec la clé 21.

Exercice n° 3 — **Bonus**

1. Crypter un message avec la clé de votre choix.
2. Recopier ce message et indiquer votre clé de chiffrement dans le Bloc-notes de l'ordinateur et enregistrer sur le réseau dans le serveur « Commun Classes (H :) ».
3. Décrypter les messages de vos camarades.

I.2 TP Scratch

I.2.a) Liste des TP

2. Associer un nombre à une lettre et une lettre à un nombre.
3. Avec une liste de l'alphabet, transformer une lettre avec une clé de 3, utilisation du modulo. Attention au décalage le « a » est l'élément 1 de la liste alors qu'on le code avec 0.
4. Copier le message clair dans une liste pour pouvoir le transformer.
5. Mettre une variable clé.
6. Décrypter un message.
7. Analyse de la fréquence.

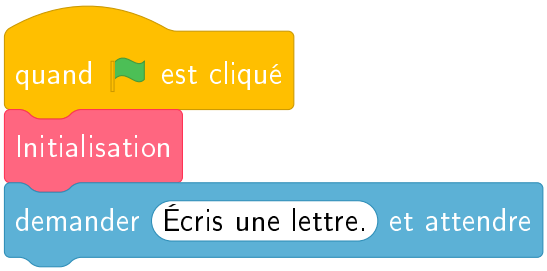
I.2.b) TP 2 : Associer lettre et nombre

1. Écrire un programme Scratch demandant à l'utilisateur une lettre et retournant son nombre associé.

Indications :

- On pourra créer une liste alphabet et un bloc initialisation comme ci-dessous :

- On pourra se servir de : élément no de chose dans alphabet
  ou position de chose dans alphabet
  selon les versions de Scratch.
- On pourra débuter le programme principal ainsi :



- Pour utiliser la réponse on pourra utiliser réponse.

2. Vérifier que pour « a », le programme nous répond « 0 ».
3. Écrire un programme Scratch demandant à l'utilisateur un nombre et retournant la lettre associée.

Indication :

On pourra se servir de : élément 1 de alphabet

4. Vérifier que pour « 0 », le programme nous répond « a ».

I.2.c) TP 3 : Crypter une lettre

En se servant du TP précédent, écrire un programme codant une lettre avec la méthode de César et une clé de chiffrement de 3.

Le programme doit demander une lettre à l'utilisateur et lui répondre la lettre située 3 rangs plus loin.

Indications :

- La lettre « a » doit être associée à « 0 » .
- On pourra se servir de ( ) modulo ( ) qui renvoie le reste de la division euclidienne du premier argument par le deuxième.
  Par exemple, comme $7 = 3 \times 2 + 1$, (7) modulo (3) renvoie 1.

I.2.d) TP 4 : Crypter un message avec la clé 3

1. Créer une nouvelle liste que l'on pourra nommer message clair, dans laquelle on recopiera le message clair.
2. Écrire un programme demandant un message à crypter et le recopier dans la liste message clair.

Indication :

On pourra s'inspirer du bloc initialisation qui vide les listes mais surtout qui recopie l'alphabet dans la liste alphabet.

3. Compléter le programme pour qu'il crypte avec la méthode de César et une clé de chiffrement de 3 le message clair donné par l'utilisateur.

Indications :

- Pour simplifier le programme principal, on pourra créer un bloc copie du message qui s'occupe de recopier le message à crypter dans la liste message clair.
- On pourra recopier la réponse de l'utilisateur dans une variable message à crypter pour ensuite le recopier dans la liste message clair.
- On pourra se servir des programmes des TP précédents ; dans lesquels :
  - on prend une lettre ;
  - on lui associe le nombre correspondant ;
  - on ajoute à ce nombre la clé (en utilisant ( ) modulo ( )) ;
  - on associe à ce nouveau nombre la lettre correspondante.
- On pourra avoir besoin de longueur de message à crypter, qui permet de connaître le nombre de lettres du message.

Exercice n° 4

Crypter le message « TESTONSCEPROGRAMMEPOURVOIRSILFONCTIONNEBIEN » .

Indication :

Vous devez trouver :

Message crypté

WHVWRQVFHSURJUDPPHSRXUYRLUVLOIRQFWLRQQHELHQ

I.2.e) TP 5 : Crypter un message avec une clé quelconque

Écrire un programme demandant à l'utilisateur un message à crypter et la clé de chiffrement et répondant le message crypté.

Indications :

On pourra se servir des programmes des TP précédents ; dans lesquels la clé de chiffrement était 3. Ici la clé doit être une variable clé donnée par l'utilisateur.

Exercice n° 5

Crypter le message « TESTONSCEPROGRAMMEPOURVOIRSILFONCTIONNEBIEN », avec la clé 19 .

Indication :

Vous devez trouver :

Message crypté

MXLMHGLVXIKHZKTFFXIHNKOHBKLBEYHGVMBHGGXUBXG

I.2.f) TP 6 : Décrypter un message

Écrire un programme demandant à l'utilisateur un message crypté et la clé de chiffrement et répondant le message clair.

Indication :

On pourra reprendre le TP précédent, recopier le programme et le modifier légèrement.

Exercice n° 6

Décrypter le message « WDZIZIOZIYPGZKMJAVZXMDOZIAMVIXVDN » qui a été crypté avec la clé de chiffrement 21.

Exercice n° 7

Bonus

1. Crypter un message avec la clé de votre choix.
2. Recopier ce message et indiquer votre clé de chiffrement dans le Bloc-notes de l'ordinateur et enregistrer sur le réseau dans le serveur « Commun Classes(H :) ».
3. Décrypter les messages de vos camarades.

I.2.g) TP 7 : Cryptanalyse

La cryptanalyse cherche à décrypter un message sans en connaître la clé de chiffrement. On dit alors qu'on tente de « casser » le chiffrement.

Référence historique :

L'un des premiers outils de la cryptanalyse est l'analyse des fréquences.
Les premières traces écrites de cette technique sont l'œuvre d'Al-Kindi (astronome, médecin, mathématicien et linguiste né en 801 à Bagdad). On a retrouvé en 1987, à Istanbul, une copie de son traité « Manuscrit sur le déchiffrement des messages cryptographiques » où il décrit la technique pour décrypter un message, suffisamment long, dont on connaît la langue :

- compter le nombre de fois où chaque lettre apparaît dans le texte à décrypter,
- classer ces lettres selon leur fréquence d'apparition dans ce texte,
- comparer avec les fréquences l'apparition des lettres dans un texte de la langue.

On sait, par exemple, que les lettres qui apparaissent le plus souvent dans les textes écrits en français sont : E, S, A, I, N ...

Exercice n° 8

Nous avons intercepté un message crypté sans la clé de chiffrement à vous de retrouver le message clair.

Message crypté

LHNOXGMIHNKLTFNLXKEXLAHFFXLWXJNBITZXIKXGGXGMWXLTEUTMKH
LOTLMXLHBLXTNQWXLFXKLJNBLNBOXGMBGWHEXGMLVHFITZGHGLWX
OHRTZXEXGTOBKXZEBLLTGMLNKEXLZHNYYKXLTFXKLTIXBGXEXLHG
MBELWXIHLXLLNKEXLIETGVAXLJNXVXLKHBLWXETSNKFTETWKHBM
LXMAHGMXNQETBLLXGMIBMXNLXFXGMEXNKLZKTGWXLTBEXLUETGV
AXLVHFFXWXLTOBKHGLMKTBGXKTVHMXWXNQVXOHRTZXNKTBEXVHFF
XBEXLMZTNVAXXMOXNEXENBGTZNXKXLBUXTNJNBEXLMVHFBJNXXM
ETBWENGTZTVXLHGUXVTOXVNGUKNEXZNXNEXETNMKXFBFXXGUHBM
TGMEBGYBKFXJNBOHETBMEXIHXMXXLMLXFUETUEXTNIKBGVXWXLG
NXXLJNBATGMXETMXFIXMXXMLXKBMWXETKVAXKXQBEXLNKEXLHET
NFBEBXNWXLANXXLLXLTBEXLWXZXTGMEXFIXVAXGMWXFTKVAXKVA
TKEXLUTNWXETBKX

Indications :

- On pourra importer un nouveau sprite « Laptop » du réseau dans le serveur « Commun Classes (H :) », dans lequel il y a un programme demandant à l'utilisateur une lettre et qui calcule la fréquence d'apparition de cette lettre. On aura peut-être besoin d'adapter le programme.
- On pourra utiliser les fréquences d'apparition des lettres dans un texte écrit en français avec ce lien Wikipedia

II TP 8 : Chiffrement affine

Exercice n° 9 — **Une fonction affine**

Soit f la fonction qui définie par $x \mapsto 3x + 5$.

1. Calculer l'image du nombre 2 par f.
2. Calculer $f(20)$.
3. Calculer l'antécédent du nombre 35 par f.
4. Que vaut x si $f(x) = 15$?

Méthode :

Le chiffrement affine consiste à associer à un nombre entier entre 0 et 25, x, un unique nombre qui est son image (ramenée entre 0 et 25) par la fonction affine définie par $x \mapsto ax + b$.
Le couple (a, b) constitue la clé.

II.1 Papier/crayon

Exercice n° 10 — **Cryptons**

Prenons comme clé $a = 3$ et $b = 5$. Cryptons le message suivant : « VIVE LES MATHS »

Remarque :

Pour décrypter un code, il faut prendre l'opposé de b et trouver un inverse du nombre a « modulo 26 ». C'est à dire un nombre dont le produit avec a donne un multiple de 26 augmenté de 1.

Exemples :

- Si $a = 3$, on remarque que $9 \times 3 = 27$ et $27 - 26 = 1$. Ainsi 9 est un inverse de 3 modulo 26.
- Si $a = 5$, on remarque que $21 \times 5 = 105$ et $105 - 4 \times 26 = 1$. Ainsi 21 est un inverse de 5 modulo 26.

Inverses modulo 26

n	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	26
n^{-1}	1	∅	9	∅	21	∅	15	∅	3	∅	19	∅	∅	∅	7	∅	23	∅	11	∅	5	∅	17	∅	25	∅

Proposition :

Un nombre possède un inverse modulo 26 si, et seulement si ce nombre et 26 sont premiers entre eux.

Démonstration : *admise.*

□

Exercice n° 11 — **Décryptons**

Prenons comme clé $a = 3$ et $b = 5$.
Décryptons le message suivant :« QDQRMRHUVSLKDVSH »

Remarque :

Si on prend $a = 1$, on retrouve la méthode du code de César.

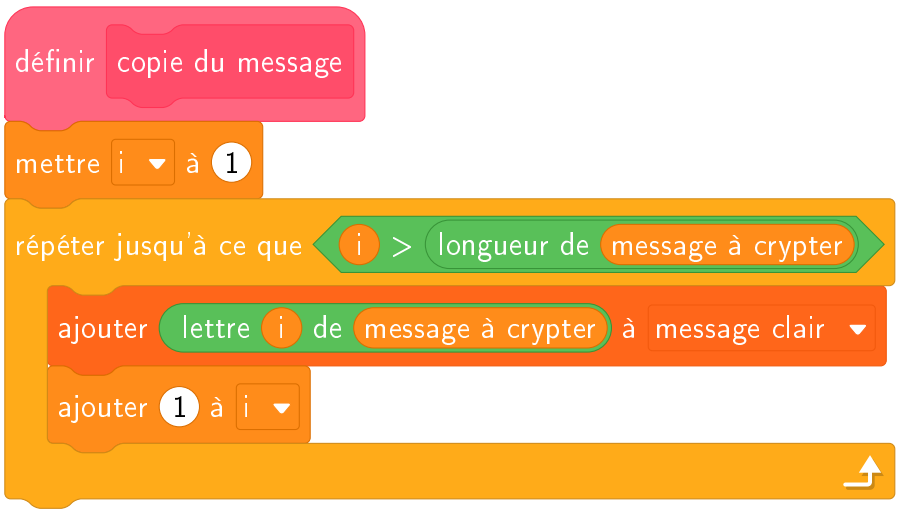
II.2 TP Scratch

II.2.a) Crypter

1. Écrire un programme demandant à l'utilisateur un message clair à crypter, la clé a et la clé b de chiffrement et répondant le message crypté.

Indications :

On pourra se servir des programmes des TP précédents, notamment en prenant les blocs :

- 

- Le bloc « Codage de César » peut nous servir de base, il faudra le modifier pour l'adapter au chiffrement affine (c'est un cas particulier quand $a = 1$ et $b =$ clé de César) :

2. Vérifier les solutions des deux exercices précédents, avec $a = 3$ et $b = 5$:
« VIVE LES MATHS » et « QDQRMRHUVSLKDVSH »

II.2.b) Décrypter

1. Écrire un programme demandant à l'utilisateur un message crypté, l'inverse de la clé a et la clé b de chiffrement et répondant le message clair.

Indication :
Nous pourrons reprendre le code du TP précédent et l'adapter légèrement.

2. Grâce au fichier texte sur le réseau envoyer des messages cryptés aux autres élèves. Préciser le prénom de l'expéditeur et les clés utilisées.

III TP 9 : Le chiffre de Vigenère

Référence historique :
Blaise de Vigenère est un cryptographe français du XVIème.
Le chiffre de Vigenère est le premier et le plus célèbre des chiffrements polyalphabétiques.
Ce système est resté invaincu pendant presque 300 ans.

Méthode :

Comme pour le code de César, le **chiffre de Vigenère** consiste à appliquer un décalage à chaque lettre du message en clair. Cependant cette fois, la longueur du décalage varie en fonction de la position dans le message initial.

Plus précisément, on choisit une clé, un mot (ici : « MATHS »), qu'on écrit autant de fois que nécessaire sous le message à coder. Le décalage de chaque lettre est déterminé par le rang dans l'alphabet de la lettre correspondante dans la clé.

Par exemple, pour coder « PYTHAGORE », on procède ainsi :

Message clair	P	Y	T	H	A	G	O	R	E
Nombre clair	15	24	19	7	0	6	14	17	4
Clé répétée	M	A	T	H	S	M	A	T	H
Décalage	12	0	19	7	18	12	0	19	7
Nombre crypté	1	24	12	14	18	18	14	10	11
Message crypté	B	Y	M	O	S	S	O	K	L

Remarque :

Avec cette méthode, on constate qu'une même lettre peut être cryptée par des lettres différentes. Deux lettres identiques dans le message crypté ne correspondent pas forcément à la même lettre dans le message clair. On ne peut donc plus utiliser la fréquence pour « casser » le code.

III.1 Papier/Crayon

Exercice n° 12 — **Crytpons**

Crypter le message clair « THEOREME » avec la clé « CRYPTO ».

Exercice n° 13 — **Décrytpons**

Décrypter le message « TGMXEWYGTSGIP » avec la clé « EPI ».

III.2 Avec le tableur

Construire, avec le tableur de LibreOffice un tableau permettant de crypter et de décrypter un message avec une clé donnée, avec la méthode du chiffre de Vigenère.

Indication :

On pourra utiliser le TP sur le tableur avec le méthode de César.

Conclusion

Il existe de nombreuses méthodes pour crypter un message soit en utilisant des clés privées, c'est à dire que si on connaît la clé on peut déchiffrer le message (comme les méthodes présentées ici César, Chiffrement affine, chiffre de Vigenère) ; soit en utilisant des clés publiques, comme la méthode RSA, qui permet, par exemple, de sécuriser les paiements par cartes bleues.

La méthode RSA (Ronald Rivest, Adi Shamir et Leonard Adleman) est une méthode connue et publique. Elle est néanmoins, pour l'instant, « incassable » en un temps raisonnable.

Par exemple si Alice veut envoyer un message secret à Bob. Celui-ci dispose d'une clé publique qu'il peut diffuser à tous et d'une clé privée qu'il garde exclusivement pour lui. Alice crypte le message avec la clé publique. Bob est le seul à pourvoir calculer, en un temps raisonnable, et donc à connaître la clé privée pour décrypter le message envoyé par Alice.

Bob peut aussi signer avec sa clé privée pour prouver que c'est bien lui qui envoie le message. Alice aura juste à décrypter avec la clé publique.

La cryptologie fait progresser et progresse avec les connaissances mathématiques (les nombres premiers par exemple) et informatiques (les capacités de calculs par exemple).

Annexes

3ème

Année 2021/2022
Calculatrice autorisée

Devoir en Temps Libre
pour le

Nom : .....
Prénom : .....
Classe : .....

Le contrôle sera rédigé sur une copie double et l'énoncé doit être rendu avec la copie.
La présentation et l'orthographe doivent être soignées et seront prises en compte dans le barème.

Exercice n° 1 :

Polybe, un historien grec (vers 200 - 125 av. J.-C.), est à l'origine du premier procédé de chiffrement par substitution. C'est un système de transmission basé sur un carré de 25 cases. Chaque lettre peut être ainsi représentée par un groupe de deux chiffres : celui de sa ligne suivi de celui de sa colonne. Ainsi : "E" = 15, "U" = 51, "N" = 34 ...
Le W n'est pas utilisé. Au besoin, on emploie le V à sa place.
Voir ci-contre.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

▷ Quel est le message codé par 3215 41433521154444155143 ?

Exercice n° 2 :

Mais ce codage est peut-être un peu simple. On décale alors l'alphabet avec un mot de passe... Par exemple, si le mot de passe est ELECTRICITE, on commence à remplir le carré avec les lettres de ce mot, en ne gardant que la première occurrence de chaque lettre, ce qui donne E L C T R I, puis on complète le tableau avec les lettres inutilisées dans l'ordre alphabétique.
Voir ci-contre.

	1	2	3	4	5
1	E	L	C	T	R
2	I	A	B	D	F
3	G	H	J	K	M
4	N	O	P	Q	S
5	U	V	X	Y	Z

▷ Quel est le message codé par 21334212 411215 avec le mot de passe GEORGESAND ?

Exercice n° 3 :

Durant la Première Guerre Mondiale, ce type de codage a été utilisé par les Allemands pour faire passer des message secrets à leurs troupes. Ils ont rajouté une 6ème ligne et une 6ème colonne pour pouvoir faire tenir les chiffres en plus des lettres. Il choisissait aléatoirement l'emplacement du A chaque jour.
Voir ci-contre.

	1	2	3	4	5	6
1	W	X	Y	Z	0	1
2	2	3	4	5	6	7
3	8	9	A	B	C	D
4	E	F	G	H	I	J
5	K	L	M	N	O	P
6	Q	R	S	T	U	V

Le code a été « craqué » par un scientifique et militaire français, Paul Painlevé.

▷ Quel est le message codé par 354455355552336463 364163 31442115 ?

EPI L'histoire des secrets ou les secrets de l'Histoire

3ème

Année 2021/2022
Calculatrice autorisée

Devoir en Temps Libre
pour le

Nom : .....
Prénom : .....
Classe : .....

Le contrôle sera rédigé sur une copie double et l'énoncé doit être rendu avec la copie.
La présentation et l'orthographe doivent être soignées et seront prises en compte dans le barème.

Méthode :

Pour crypter un texte, nous choisissons d'utiliser la décomposition en facteurs premiers des nombres.
Par exemple prenons la clé (2 ; 3 ; 5), observons donc le message « 8 201 250 ; 8 192 ».
$8\,201\,250 = 2^{\mathbf{1}} \times 3^{\mathbf{8}} \times 5^{\mathbf{4}}$ et $8\,192 = 2^{\mathbf{13}} \times 3^{\mathbf{0}} \times 7^{\mathbf{0}}$.
D'après le tableau classique de correspondance entre lettres et nombres :

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
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

On a « BIENAA ». Ici le 0 représente le A ou le vide en fonction du sens, donc nous lirons « **BIEN** ».

Exercice n° 1 :

En utilisant la clé (2 ; 3 ; 5), décrypte le message « 800 ; 28 343 520 000 ».

Exercice n° 2 :

En utilisant toujours cette clé (2 ; 3 ; 5), crypte le message « GENIAL ».

Exercice n° 3 :

Selon toi, quel peut être l'inconvénient de ce type de cryptage ?

Proposition de plan

Nous vous proposons un plan pour la présentation orale de cet EPI. Chacun est libre de l'utiliser, de s'en inspirer, ou d'en proposer un autre plus adapté à la présentation souhaitée et imaginée.

Plan

Introduction

I) Définitions (cryptologie, cryptographie, cryptanalyse)

II) Un événement historique dans lequel la cryptologie à jouer un rôle

III) Imitation Game (avec extrait si besoin, dilemme moral, Alan Turing)

IV) Proposer un code et un décodage (vu en cours ou personnel)

Conclusion : problèmes rencontrés, évolution de la cryptologie, ouverture vers un autre événement historique, ...