ircam Centre Pompidou

UPMC SORBONNE UNIVERSITÉS

Bases de l'Arithmétique & Cryptologie Romantique

Ninon Devis: ninon.devis@ircam.fr

TD 1 & 2

Exercice 1 - Questions introductives de Cryptologie

1. Rappeler la définition de la cryptologie.

   ➔ Science du secret regroupant la *cryptographie* et la *cryptanalyse*.

2. Quelle est la différence entre cryptographie et cryptanalyse ?

   ➔ Cryptographie: *protéger* les données par le chiffrement, étude des algorithmes qui le permettent (les *cryptosystèmes*)

   ➔ Cryptanalyse: *retrouver* l'information claire à partir du chiffré, étude de la sécurité des cryptosystèmes.

Exercice 1 - Questions introductives de Cryptologie

3. Quelle est la différence entre la cryptographie et la stéganographie ?
   - ➔ Stéganographie: dissimuler l'information. Si on dispose de l'information, il est aisé d'en prendre connaissance.
     - ◆ Ex: Encre invisible, message sur le crâne dont on laisse repousser les cheveux, micropoint…
   - ➔ Cryptologie: rendre un message inintelligible à autre que qui de droit.

4. Quel mathématicien célèbre s'est illustré en participant à la cryptanalyse de la machine à chiffrer utilisée par l'armée allemande pendant la seconde guerre mondiale ?
   - ➔ Alan Turing.

Exercice 1 - Questions introductives de Cryptologie

5. Donner le nom de la machine de la question précédente.

➔ Enigma

- *The Imitation Game*

6. L'utilisation des moyens cryptographiques est-elle libre en France ? Qu'en est-il du transfert de moyens de cryptanalyse ?

➔ Loi pour la confiance dans l'économie numérique du 21 Juin 2004

- L'utilisation des moyens de cryptologies sont libres en France.
- Les moyens assurants les fonctions d'authentifications ou de contrôle d'intégrité sont libres depuis ou vers un pays membre UE
- Hors de ces domaines, une déclaration préalable est nécessaire pour l'import et une autorisation préalable est nécessaire pour l'export.

Exercice 2 - Rappels d'arithmétique de base

1. Que représente l'expression 31 mod 26 ? Quel est son représentant canonique?
   - ➔ C'est le reste (positif) de la division euclidienne de 31 par 26. Représente l'ensemble des entiers ayant pour reste lors de la division par 26 le même que celui de 31.
     - ◆ Sa valeur est 5.
     - ◆ On parle de classe modulo 26.

2. Que vaut -3 mod 26 ?
   - ➔ En maths: -3 mod 26 = 23.

Exercice 2 - Rappels d'arithmétique de base

3. Rappeler la définition d'un nombre premier et du PGCD entre deux entiers.
   - ➔ Nombre premier: Un entier naturel divisible par exactement deux entier: 1 et lui même.
   - ➔ Le PGCD de deux entiers est le plus grand diviseur commun à ces deux entiers.

4. Donner la table d'addition et de multiplication modulo 12.

5. Donnez l'ensemble des couples $(a, b) \in \{0, \ldots, 11\}^2$ tels que b soit l'inverse de a pour l'addition modulo 12.

5. Donnez l'ensemble des couples $(a, b) \in \{0, \ldots, 11\}^2$ tels que b soit l'inverse de a pour la multiplication modulo 12.

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

*	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

5. + 6. Pour trouver les inverses: si a parcourt les lignes, on cherche la colonne qui contient le neutre de l'opération correspondante. Cette colonne correspond à b.

- Neutre d'une opération: nombre qui ne modifie pas le résultat d'une opération.

➔ Quel sont les neutres de l'addition et de la multiplication ?

- Inverses pour l'addition: (0, 0), (1, 11), (2, 10), (3, 9), (4, 8), (5, 7), (6, 6), (7, 5), (8, 4), (9, 3), (10, 2), (11, 1).
- Inverses pour la multiplication: (1, 1), (5, 5), (7, 7) et (11, 11).

*	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

7. Exhiber un élément a dans {0, …, 11} différent de 0 tel qu'il existe un b != 0 et vérifiant a × b = 0 mod 12 .

➔ Chercher les 0 dans la table en dehors de la ligne et colonne 0:
2, 3, 4, 6, 8, 9, 10, c'est-à-dire tous les nombres non premiers avec 12.

8. Résoudre l'équation 7x + 5 = 4 mod 12.

➔ 7x + 5 = 4 mod 12 ⇔ 7x = 4 − 5 = 11 mod 12.
On cherche 11 dans la ligne des multiples de 7 et on lit sur la colonne de 11 la valeur de x .

➔ x = 5

Quid de 3x + 5 = 7 mod 12 ?

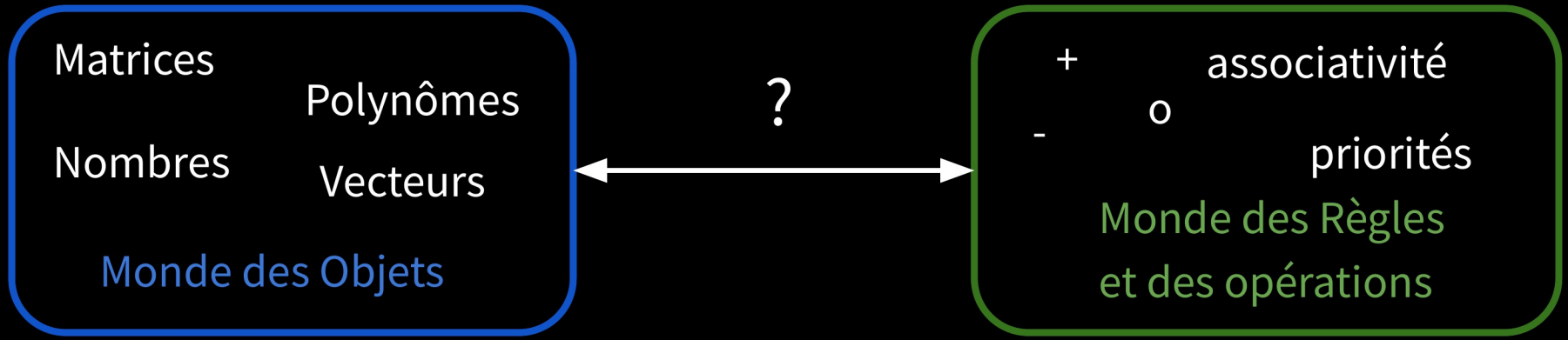
➔ 3x = 7 − 5 = 2 mod 12 Or il n'y a pas de 2 dans la ligne des multiples de 3 => pas de solution pour cette équation.

Exercice 3 - Structures Algébriques - Notions

« *The teaching of abstract algebra is a disaster, and this remains true almost independently of the quality of the lectures* » - Leron & Dubinsky, 1995 ✌️

➔ Utilités des structures algébriques:

- Comprendre les principes qui permettent d'effectuer les calculs classiques.
- Étendre ces principes à différents types d'objets
- Généraliser sur des objets abstraits et des types d'opérations variées.



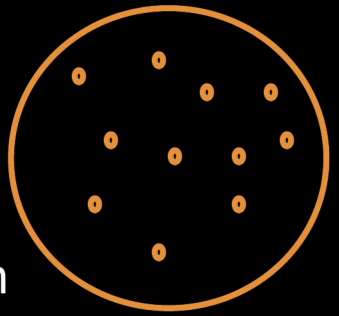
Structures Algébriques - Qu'est-ce ?

➔ Un ensemble d'objets mathématiques

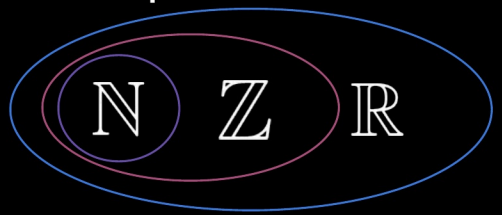
Pas de lien ou de relation entre les objets.

Objectif d'une structure...structurer !

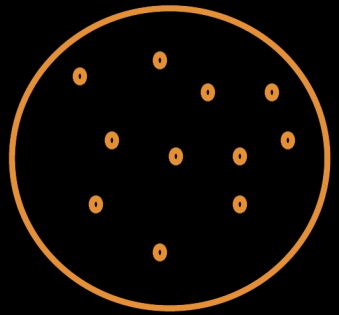
➔ Ajouter quelque chose pour créer du lien



Exemples:



.....



\+ Opération

➔ L'opération sera notée "♡" (dans ce cours)

➔ Les opérations vérifient une ou plusieurs propriétés.

➔ Un des objectifs de la structure algébrique: généraliser les opérations "classiques"

Structures Algébriques - Magma

➔ N'importe quel ensemble et n'importe quelle opération, noté: (E, ♡)

Exemple: définissons notre propre ensemble E et notre propre opération ♡

E = { ❀ , ☮ , ♬} Comment définir maintenant une opération ? => Avec une table !

♡	❀	☮	♬
❀	♬	☮	♬
☮	❀	♬	☮
♬	☮	❀	♬

➔ Notre magma est entièrement défini !

➔ On peut même résoudre des équations:

☮ ♡ x = ♬ , x = ?

➔ x = ☮

Problème: ce magma est peu intéressant

Structures Algébriques - Magma - Propriétés

➔ On ajoute des propriétés au magma pour le rendre intéressant à étudier.

N.B : “opération” ⇔ “loi de composition interne”

Les propriétés sur les magmas:

➔ Commutativité: on obtient le même résultat en composant dans un sens ou dans l’autre: $\forall x, y \in E, \quad x \heartsuit y = y \heartsuit x$

➔ Associativité: $\forall x, y, z \in E, \quad (x \heartsuit y) \heartsuit z = x \heartsuit (y \heartsuit z)$

➔ Neutre: $\forall x \in E, \quad \exists e \in E, \quad x \heartsuit e = e \heartsuit x = x$

➔ Symétrique: Tout élément de E possède un symétrique:

$\forall x \in E, \quad \exists \bar{x} \in E, \quad x \heartsuit \bar{x} = \bar{x} \heartsuit x = e$

Structures Algébriques - Groupes

Groupe: Structure algébrique composée d'un ensemble (G, ♡) telle que:

- ➔ La loi de composition ♡ est interne: si $x \heartsuit y = z$, alors $z \in G$
- ➔ ♡ est associative.
- ➔ Il existe un élément neutre dans G.
- ➔ Loi de Symétrie.
- ★ Règle "ANIS": associatif, neutre, interne et symétrique.

.....

Groupe cyclique (ou monogène) : C'est un groupe qui peut être engendré par un élément: $\exists\ g \in G$ tel que $\forall\ a \in G$, $a = g \heartsuit g \heartsuit g \heartsuit \ldots \heartsuit g$

.....

Groupe abélien : Groupe commutatif

Exercice 3 - Structures Algébriques

1. Rappeler la définition d'un groupe.

➔ Ensemble G muni d'une loi de composition interne,
- d'une opération • associative (pour tout x, y et z $\in$ G, x • (y • z) = (x • y) • z)
- d'un élément neutre (il existe e tel que pour tout x $\in$ G, x • e = e • x = x)
- d'un inverse pour tous les éléments (pour tout x $\in$ G, il existe y $\in$ G tel que x • y = y • x = e.

➔ Il est dit commutatif lorsque l'opération • est commutative.

2. Vérifier que l'ensemble des classes modulo un entier n muni de l'addition forme bien un groupe (on le note généralement Z/nZ) (Z/nZ, +)

➔ L'associativité vient de celle de Z, l'élément neutre 0 et l'inverse de n est $-n$.

Le groupe Z/nZ est cyclique, il peut être représenté sur un cercle.

Exercice 3 - Structures Algébriques

3. Rappeler la définition d'un groupe cyclique. Montrer que le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique.

➔ Groupe cyclique: qui peut être engendré par un élément. $\exists\ g \in G$ tel que $\forall\ a \in G,\ \exists\ k \in G$ tel que $a = g + g + g + \ldots + g,\ k$ fois

➔ Ici $\mathbb{Z}/n\mathbb{Z}$ est engendré par 1!

4. Montrer que tout groupe fini cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Ce dernier est donc le groupe cyclique de cardinal n canonique. *TODO*

5. Rappeler la définition d'un groupe commutatif (dit aussi abélien). Donner un groupe de permutation qui n'est pas commutatif. *TODO*

Exercice 3 - Structures Algébriques

4. Montrer que tout groupe fini cyclique de cardinal n est isomorphe à Z/nZ. Ce dernier est donc le groupe cyclique de cardinal n canonique.

- *Morphisme de groupe*: application entre deux groupes qui respecte la structure de groupe. Pour deux groupes (G, ♡) et (G', ♬),
  C'est une application f: G⟶G', telle que $\forall\ x, y \in G, \quad f(x \heartsuit y) = f(x) \beamednote f(y)$

➔ Soit (G, x) cyclique de cardinal n, engendré par 1_G
Par définition, tout élément de G est de la forme g^k
Si on considère le morphisme $\varphi : \mathbb{Z} \mapsto k$
définit par : $\varphi(k) = g^k k$

➔ C'est un isomorphisme de groupe de G dans Z/nZ.

Exercice 3 - Structures Algébriques

5. Rappeler la définition d'un groupe commutatif (dit aussi abélien). Donner un groupe de permutation qui n'est pas commutatif.

- Groupe abélien: $\forall\, x, y \in G, \quad x \heartsuit y = y \heartsuit x$

→ Groupe de permutation non commutatif :

$\sigma_1 : 1 \mapsto 2 \quad 2 \mapsto 1 \quad 3 \mapsto 3$

$\sigma_2 : 1 \mapsto 1 \quad 2 \mapsto 3 \quad 3 \mapsto 2$

D'où : $\sigma_1 \circ \sigma_2 : 1 \mapsto 2 \quad 2 \mapsto 3 \quad 3 \mapsto 1$

$\sigma_2 \circ \sigma_1 : 1 \mapsto 3 \quad 2 \mapsto 1 \quad 3 \mapsto 2$ } $\neq$!

Exercice 4 - Python, les listes et les statistiques

2. Étant donnée une variable aléatoire discrète X représentée à l'aide de deux listes de même longueur donner une fonction Python permettant de calculer l'espérance de X.

➔ Espérance: moyenne des valeurs (liste V) pondérée par les probabilités (liste P). La somme des probabilité = 1.

$$esperance(\mathcal{X}) = \sum_i P_i V_i$$

3. Avec les mêmes notations que la question précédente, donner une fonction Python permettant de calculer la variance et l'écart type de X.

➔ La variance et l'écart type permettent de juger de la dispersion des valeurs.

$$variance(\mathcal{X}) = esperance(\mathcal{X}^2) - esperance(\mathcal{X})^2 = (\sum_{i=1}^{n} P_i V_i^2) - (\sum_{i=1}^{n} P_i V_i)^2$$

$$ecarttype(\mathcal{X}) = \sqrt{variance(\mathcal{X})}$$

Exercice 4 - Python, les listes et les statistiques

$$esperance(\mathcal{X}) = \sum_i P_i V_i$$

Cf le corrigé pour les codes !

$$variance(\mathcal{X}) = esperance(\mathcal{X}^2) - esperance(\mathcal{X})^2 = (\sum_{i=1}^{n} P_i V_i^2) - (\sum_{i=1}^{n} P_i V_i)^2$$

$$ecarttype(\mathcal{X}) = \sqrt{variance(\mathcal{X})}$$

Exercice 5 - Mono-alphabétique

1. Rappeler le principe de base de la cryptographie mono-alphabétique. Avec quelle opération mathématique cela peut-il se définir ? Quelle est la clé secrète?

➔ Chaque caractère est remplacé par un symbole unique.

➔ Classiquement, il s'agit d'une permutation de l'alphabet dans lui-même ou une bijection entre deux alphabets finis différents (mais de même cardinal).

Rappel:

- Soit E un ensemble, on appelle et on note Card(E), le nombre d'éléments de E.
- Bijection: tout élément de l'ensemble de l'arrivée ne possède qu'un antécédent.

➔ La clé secrète est alors la chaîne de caractères en laquelle l'alphabet initial est transformé par chiffrement.

Exercice 5 - Mono-alphabétique

2. **(Chiffrement de César)** Quelle est la particularité du chiffrement de César dans l'ensemble des chiffrements mono-alphabétiques ? En déduire que la clé secrète peut être définie par le symbole dans l'alphabet d'arrivée correspondant à une lettre fixée dans l'alphabet de départ (le A par exemple). Rappeler avec quelle opération mathématique le chiffrement et le déchiffrement de César peut se définir.

➔ C'est un chiffrement par décalage.

➔ Pour un décalage correspondant à :
la clef secrète peut se résumer à "C"

A	B	C	D	...
C	D	E	F	...

➔ Classiquement, opération modulo le nombre de caractères dans l'alphabet.
$(x + d) \bmod n$ où d est la longueur du décalage et n la longueur de l'alphabet.

Exercice 5 - Mono-alphabétique

3. **(Chiffrer, déchiffrer des messages pour César)** L'alphabet de départ et d'arrivée est le même : les caractères majuscules non accentués.

Chiffrer le message ATTAQUESURLUTECEDEMAIN avec la clé "R".

➔ Substitution explicite:

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- RSTUVWXYZABCDEFGHIJKLMNOPQ

    - Devient: RKKRHLVJLICLKVTVUVDRZE

➔ Via le terminal, on peut utiliser "tr" (translate):

```
$ echo "ATTAQUESURLUTECEDEMAIN" | tr 'A-Z' 'R-ZA-Q'
```

Exercice 5 - Mono-alphabétique

Déchiffrer le message IVIRYNPELCGBYBTVR avec la clé N.

➔ Substitution explicite:

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- NOPQRSTUVWXYZABCDEFGHIJKLM

    - Devient: VIVELACRYPTOLOGIE

➔ Via le terminal, on peut utiliser “tr”:

```
$ echo "IVIRYNPELCGBYBTVR" | tr 'N-ZA-M' 'A-Z'
```

Remarque: cette substitution est sa propre inverse s(s(c)) = c, on l’appelle rot13. Il existe une commande Unix qui l’implémente:

```
$ echo IVIRYNPELCGBYBTVR | rot13
```

Exercice 5 - Mono-alphabétique

4. En supposant que les alphabets d'entrée et de sortie soient celui des 26 lettres majuscules, estimer la difficulté de retrouver un texte clair à partir d'un chiffré sans connaître la clé pour un chiffrement par décalage ou plus généralement un chiffrement mono-alphabétique.

➔ 26 par décalage, $26! = |S_{26}|$ par chiffrement mono-alphabétique.

5. Sur quel principe mathématique se base la cryptanalyse d'un chiffrement mono-alphabétique ?

➔ L'analyse des fréquences (ici fréquence des lettres)

Exercice 6 - Poly-alphabétique

1. Le chiffrement de Vigenère peut être vu comme une généralisation du chiffrement de César : au lieu de décaler chacune des lettres du message clair selon une lettre (la clé secrète), on va décaler des blocs de lettres selon un mot. Donner un schéma expliquant le chiffrement de Vigenère.

➔ $C = (c_1, \ldots, c_l)$ la clef secrète, on découpe le texte en tranches de l lettres et pour le caractère t_p en position p on associe $(t_p + c_{p \bmod l}) \bmod |A|$.

2. À l'aide de la clé "CESAR", déchiffrer le message XSMSRXIRDVLEIUVNUMEJRSANKU obtenu en utilisant le chiffrement de Vigenère.

➔ On découpe en blocs de 5 lettres XSMSR | XIRDV | LEIUV | NUMEJ | RSANK | U

➔ Puis on décale: VOUSA VEZDE JAQUE LQUES POINT S

Exercice 6 - Poly-alphabétique

Avec la clef “CIPHER”, chiffrer le message LATTAQUEESTPREVUEPOURDEMAIN.

➔ On découpe en blocs de 5 lettres LATTAQ | UEESTP | REVUEP | OURDEM | AIN
➔ Puis on décale: NIIAEH WMTZXG TMKBIG QCGKID CQC

3. Expliquer quel principe mathématiques permet de modéliser le chiffrement de Vigenère.

➔ La substitution poly-alphabétique.

Exercice 7 - Indice de Coïncidence

1. Rappelez la définition de l'indice de coïncidence d'un texte.

➔ Probabilité d'obtenir deux caractères identiques en choisissant un couple au hasard dans ce texte.

$$IC = \sum_{i \in \mathcal{A}} \frac{n_i(n_i - 1)}{n(n-1)}$$

où n_i est le nombre de lettres i dans le texte et n est la longueur totale de ce dernier.

Exercice 7 - Indice de Coïncidence

2. D'après le tableau suivant, calculer l'indice de coïncidence d'un texte écrit en anglais.

Langue	A	B	C	D	E	F	G	H	I	J	K	L	M
Français	9,42	1,02	2,64	3,39	15,87	0,95	1,04	0,77	8,41	0,89	0,00	5,34	3,24
Anglais	8.08	1.67	3.18	3.99	12.56	2.17	1.80	5.27	7.24	0.14	0.63	4.04	2.60

Langue	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Français	7,15	5,14	2,86	1,06	6,46	7,90	7,26	6,24	2,15	0,00	0,30	0,24	0,32
Anglais	7.38	7.47	1.91	0.09	6.42	6.59	9.15	2.79	1.00	1.89	0.21	1,65	0.07

- En français: $n_A = 942$, $n_B = 102$ … et $n = 10006$, soit IC = 0.075...
- En anglais: $n_A = 808$, $n_B = 167$… et $n = 9999$, soit IC = 0.066…
- Pour un texte aléatoire équidistribué de 1040 caractères: 40 fois chaque lettre.

$$IC = \frac{26 * 40 * 39}{1040 * 1039} = \frac{39}{1039} = 0.0375$$

Exercice 7 - Indice de Coïncidence

2. Montrez que l'indice de coïncidence est invariant par chiffrement par substitution. Qu'en déduisez-vous sur le principe de distinction ?

$$IC_{\mathcal{P}} = \sum_{i \in \mathcal{A}} \frac{n_{\sigma(i)}(n_{\sigma(i)} - 1)}{n(n-1)}$$

$$\{\sigma(i), i \in \mathcal{A}\} = \{i \in \mathcal{A}\}$$

➔ D'où $IC_P = IC$

➔ un texte chiffré se distingue de la même façon qu'un texte clair d'un texte aléatoire.

C'est un distingueur pour les textes issus d'un langage vis-à-vis de l'aléatoire.

Exercice 8 – Test de Kasiski vs Indice de Coïncidence

1. Rappelez le principe du test de Kasiski.

- *Objectif*: trouver la taille de la clef d'un texte chiffré par Vigenère.

➔ On cherche les chaînes de caractères répétées dans le chiffré.

- Fonctionnement par l'exemple:
  - `'crypto is short for cryptography'`
    - 'crypto' est répété 2 fois espacé de 20 caractères
    - Si on aligne ce texte clair avec une clef de longueur 6 (ne divise pas 20):
  - `'abcdefabcdefabcdefabcdefabcdefab'`
  - `'crypto is short for cryptography'`
    - les deux instances ne seront pas chiffrées de la même manière: le test de Kasiski échoue.
    - Si on aligne ce texte clair avec une clef de longueur 5 (divise 20):
  - `'abcdeabcdeabcdeabcdeabcdeabcdeab'`
  - `'crypto is short for cryptography'`

Exercice 8 – Test de Kasiski vs Indice de Coïncidence

1. Rappelez le principe du test de Kasiski.

- *Résumé:* Trouver des suites de quelques lettres qui apparaissent plusieurs fois dans le texte chiffré, prendre alors le pgcd des distances entre les répétitions pour les différentes suites et si tout va bien c'est la longueur de la clef.

2. Le texte suivant est issu d'un chiffrement par Vigenère d'un texte en anglais. Utilisez le test de Kasiski pour retrouver la longueur de la clé. Peut-on conclure directement à l'aide des indications données dans le texte ? Si non, pour quelle raison ? Si oui expliquer comment.

GSRLCVXYEJ TBZKEIPAGP BEAVTBEAVH

- Décalages: BEA:[20;25] SST:[36,456] YEA:[74,102,497] JOO:[231,345] SSTBPK:[36;456]

Factorisation des décalages:

$5 \;//\; 2^2 \times 3 \times 5 \times 7 \;//\; 2^2 \times 7 \;//\; \underbrace{5 \times 79}_{=497-102} \;//\; 3 \times 37 \;//\; 2^2 \times 3 \times 5 \times 7$

La longueur de la clef est *probablement* 7

Exercice 8 – Test de Kasiski vs Indice de Coïncidence

3. Expliquer comment l'indice de coïncidence permet de retrouver la longueur de la clé lors d'une cryptanalyse de Vigenère.

- On essaie différentes longueurs de clefs k: pour chaque k, on découpe le texte en blocs de longueurs k.
- Chaque bloc est sensé être chiffré avec la même clef.
- On calcule ensuite l'indice de coïncidence moyen de ces suites.
- Soit il est proche de l'IC de la langue du texte clair, soit proche d'un texte aléatoire!
- La longueur de la clef est probablement le plus petit k pour lequel cet IC moyen est nettement plus élevé que les autres.

Exercice 8 – Test de Kasiski vs Indice de Coïncidence

4. Le tableau suivant est le résultat pour k = 3, . . . , 20, du calcul de l'indice de coïncidence moyen des sous-chaînes $S_i = s_i s_{i+k} s_{i+2k} \cdots$ pour $i \in [0, k-1]$. En déduire la longueur de la clé du chiffrement de Vigenère utilisé pour chiffrer ce texte en anglais.

- Rappel: ex 7 nous avions $IC_{anglais} = 0.066$

  Et pour un texte aléatoire: $IC_{alé} = 0.0375$

k	IC moyen	k	IC moyen
3	0.0431208310349463	12	0.0423336353568912
4	0.0429338103756708	13	0.0396449704142012
5	0.0412621359223301	14	0.0701810833389781
6	0.0428238229266580	15	0.0410287751464222
7	0.0683182595511363	16	0.0429611131476051
8	0.0426682692307692	17	0.0427533861152915
9	0.0450287596385600	18	0.0436051815362160
10	0.0414027149321267	19	0.0445558340295182
11	0.0405418663975556	20	0.0412307692307692

La longueur de clef 7

(plus petit k pour lequel IC est élevé et $\approx IC_{anglais}$)