Thème d'étude 2: nombres premiers et cryptographie.

Introduction:

Définition : *cryptographie: code graphique déchiffrable par l'émetteur et le destinataire seulement.*

Définition : *crypter : rendre incompréhensible un message.*

De tout temps, trouver un moyen de coder un message secret a été une préoccupation importante, en particulier pour les militaires. Par exemple, Jules César a utilisé un code secret pour transmettre des informations à ses généraux sur les champs de bataille.

Actuellement, notamment avec le développement d'Internet et du commerce électronique, crypter un message est devenu indispensable pour tous les citoyens. En effet, lorsqu'un client paye avec sa carte bancaire, il n'a pas vraiment envie que son numéro de carte, qui transite par des réseaux électroniques, tombe au main de n'importe qui. Si un intrus parvient à obtenir ce numéro de carte bancaire qui ne lui appartient pas, il peut acheter avec ce simple numéro.

Il en va de même pour toute autre information que l'on juge confidentielle, d'où la nécessité de coder certains messages, en utilisant un code qui ne peut pas être « brisé », c'est à dire qu'un intrus ne peut pas décoder.

Les humains, et les mathématiciens en particulier, ont donc cherché à trouver des méthodes pour coder leur messages confidentiels, des méthodes sans cesse plus performantes. En parallèle, les mêmes individus ont cherché les techniques les plus efficaces pour décoder tous les types de message. Tout cela a bien sûr pris un essor fulgurant avec l'arrivée des ordinateurs et des moyens de calcul modernes.

Actuellement, les techniques de codages les plus efficaces sont basées sur les mathématiques. Elles utilisent ce que l'on appelle les *nombres premiers*, ces nombres bien particuliers qui ont pour propriété de n'avoir que deux diviseurs : 1 et eux–mêmes.

Ce deuxième thème va nous emmener à la découverte de la cryptographie.

Mais avant de nous intéresser à la cryptographie proprement dite, nous allons devoir développer un certain nombre d'outils plus ou moins théoriques. Allons-y.

1. Où utilise-t-on la cryptographie ?

Lis le document 1. Peux-tu dire à quel(s) moment(s) la cryptographie est utilisée dans cette histoire ? Tu peux souligner les moments de l'histoire qui te semblent pertinents.

2. Quelques messages

Décode les différents messages proposés dans les documents 2 et 3.

Quels sont les avantages et les inconvénients des différentes techniques de codage que tu as rencontrées ?

3. Les diviseurs d'un nombre

Définition : on dit qu'un nombre entier *n* est un *diviseur* d'un nombre entier *A* si le résultat de la division euclidienne de *A* par *n* est 0.
On dira alors que *A* est un multiple de *n*.

Remarque : dès que l'on parle de *diviseur* ou de *multiple*, il est convenu que l'on ne parle que de nombres entiers. Cette notion n'a pas de sens pour les décimaux.

1. 102 est-il divisible par 12 ?
2. 255 est-il divisible par 17 ?
3. 597 est-il divisible par 13 ?
4. 8 715 est-il divisible par 83 ?
5. Traduis les divisions euclidiennes précédentes par l'écriture de la forme $a = b \times q + r$ qui leur est associée. Peut-on lire sur cette écriture les réponses précédentes ?
6. Traduis par une égalité le fait que 11 est un diviseur de 143 ; que 85 est un multiple de 17.
7. De manière générale, en utilisant le calcul littéral, comment peut-on traduire le fait que *n* est un diviseur de *A*.
8. Exemples : comment écrit-on les multiples de 3 ; de 7 ; les nombres divisibles par 12 ; par 147 ?

4. Le plus grand diviseur commun :

1. Écris, en ordre croissant, la liste de *tous* les diviseurs de 210 et de tous les diviseurs de 90.
2. Quel est le plus grand diviseur commun à 210 et 90 ?
3. Que penses-tu de cette méthode pour le trouver ? Permet-elle de le découvrir ? Est-elle efficace.

Définition : Si *a* et *b* sont deux nombres entiers, alors le plus grand nombre entier *n* qui divise *à la fois a* et *b* est appelé le plus grand diviseur commun de *a* et de *b*.
On note alors : n = **PGCD (** a **;** b **)**

4. Application : Trouve le PGCD de 143 et 85 ; de 27 et 30.

5. L'algorithme d'Euclide :

Comme tu as pu le constater, la méthode vue au paragraphe précédent pour calculer le PGCD est très longue et peu efficace dès que les nombres sont un peu grands (*cela est dû au fait qu'il n'est pas facile de trouver les diviseurs d'un nombre, retiens cette petite remarque qui sera très importante lorsque nous étudierons les techniques de cryptographie*).

Il existe une autre méthode, fondamentale et qui se généralise à beaucoup de domaines des mathématiques : c'est l'algorithme d'Euclide.

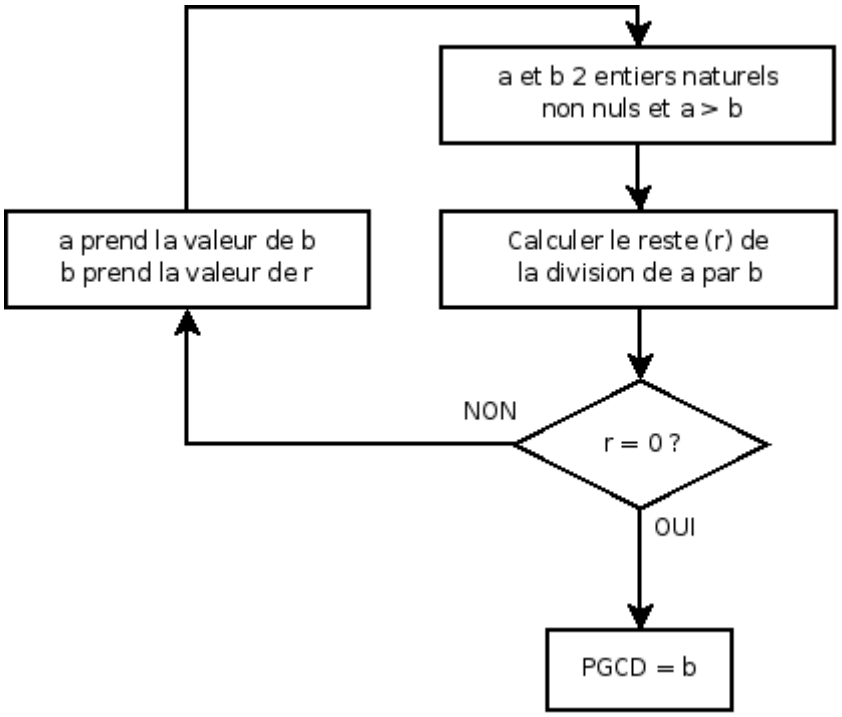
Nous allons donner la méthode, sans la justifier car cela sera fait l'an prochain (*oui, oui, nous somme obligés d'anticiper sur le programme de 3ème…*).

Cette méthode était déjà connue du temps d'Euclide (environ 300 avant J.C.), elle n'est donc pas toute récente et pourtant elle n'a rien perdu de son efficacité ni de sa pertinence.

Voici donc cette méthode, présentée sous forme d'un schéma :

Principe :

- on divise a par b (division euclidienne)
- on trouve le reste r ;
- si $r = 0$, l'algorithme se termine :
  PGCD(a ; b) = b
- si $r \neq 0$, on remplace a par b et b par r ;
  puis on recommence à partir de (1).



Exemple numérique : on veut calculer le PGCD de 1224 et 936 :

étapes	a	b	r
1	1224	936	288
2	936	288	72
3	288	72	0

$1224 = 1 \times 936 + 228$
$936 = 3 \times 288 + 72$
$288 = 4 \times 72 + 0$

L'algorithme s'arrête lorsque l'on trouve un reste nul.

Le **PGCD de a et b est le dernier reste non nul trouvé**.

PGCD(1224 ; 936) = PGCD(936 ; 288) = PGCD(288 ; 72) = 72.

1. Pourquoi est-on sûr que l'algorithme d'Euclide se termine toujours.
2. Quelle touche sur ta calculatrice te permet de trouver directement le quotient et le reste de la division euclidienne ?
3. Calcule le PGCD de 702 et 273.
4. Calcule le PGCD de 1 466 652 et 9 478.
5. Programme une feuille de calcul au tableur qui permet de calculer le PGCD de deux nombres, sachant que le premier est plus grand que le second.

   La fonction qui donne le reste de la division euclidienne est MOD :
   MOD(1 224; 936) = 288.

   Prévois un nombre de lignes suffisant.

6. Calcule le PGCD de 1 457 784 et 214 786.

6. Nombres premiers entre eux :

Définition : deux nombres sont dits *premiers entre eux* s'il n'ont qu'un seul diviseur commun, à savoir 1.

1. Si deux nombres sont premiers entre eux, quel est leur PGCD ?
2. Donne quelques exemples de nombres premiers entre eux.
3. 221 et 69 sont-ils premiers entre eux ? Applique l'algorithme d'Euclide en utilisant ta calculatrice et en remplissant le tableau ; puis vérifie avec ta feuille tableur.
4. 4 803 et 3 202 sont-ils premiers entre eux ?
5. En utilisant la feuille tableur, trouve deux nombres à 6 chiffres qui sont premiers entre eux.

7. Nombres premiers :

Définition : un nombre est dit *premier* s'il n'a que deux diviseurs : 1 et lui-même.

1. Vérifie que 2, 7, 13 sont des nombres premiers.
2. Vérifie que 24, 143, 221 ne sont pas premiers.
3. 29 et 53 sont-ils des nombres premiers ?
4. Trouve un nombre premier à 3 chiffres.

6. Décomposition en facteurs premiers :

Théorème : Tout nombre entier s'écrit de manière unique comme un produit de nombres premiers.

Exemple : $15 = 3 \times 5$ $126 = 2 \times 63 = 2 \times 7 \times 9$

1. Écris les nombres suivants sous forme de produit de nombres premiers :
   20 440 5040

7. Congruences :

1. La suite de symboles suivante est constituée de 7 symboles différents; cette suite se prolonge aussi loin que l'on veut. :

   a. A quelle position se trouve le troisième ■ ?
   b. A quelle position se trouve le cinquième ? Justifie ta réponse.
   c. Quel symbole occupe la 28ème position? Justifie ta réponse.
   d. Quel symbole occupe la 410ème position? Justifie ta réponse.
   e. Quel symbole occupe la 3 000ème position? Justifie ta réponse.

2. Il est 8 h. Quelle heure sera-t-il dans 5 h ? dans 12 h ? dans 28 h ? dans 32 h ? dans 1000 h ?

Définition : Soit n un nombre entier supérieur ou égal à 1 et a et b des nombres entiers.
On dit que a est congru à b modulo n s'il existe un nombre entier tel que :

$$a = b + k \times n.$$

On écrit alors : $a \equiv b\ [n]$ ou $a \equiv b \bmod n$.

3. Reprenons les réponses de la question **1. a.** À quel entier, modulo 7, le nombre entier 410 est-il congru ? et 3 000 ?
4. À combien 3 728 est-il congru modulo 9 ? modulo 12 ? modulo 234 ?
5. Si l'on prend un nombre n. À quels nombres peut-il être congru modulo 7 ? modulo 12 ?
6. À combien 7^6 est-il congru modulo 5 ? modulo 7 ?

8. Congruences et nombres premiers :

Considérons le nombre 7. Nous avons vu qu'un nombre n ne peut être égal qu'à 0 ; 1 ; 2 ; 3 ; 4 ; 5 ou 6 modulo 7.

1. Calcule a^7 modulo 7 pour $a = 0$; 1 ; 2 ; 3 ; 4 ; 5 ; 6.
2. Que remarques-tu ?
3. Prends maintenant le nombre 5 et effectue la même étude (attention, ici a varie entre 0 et 4 !). Que remarques-tu ?
4. Prends maintenant le nombre 8 et effectue la même étude. Que remarques-tu ?
5. Pourquoi as-tu observé un résultat remarquable en **1.** et **3.** et pas en **4.** ?

Ce que tu viens de remarquer est un résultat très important en cryptographie est appelé le *« petit théorème de Fermat »*.

« Petit théorème » de Fermat : Si p est un nombre premier, pour tout entier a, on a :

$$a^{p-1} \equiv 1 \ mod\ p$$

d'où : pour tout entier a, $a^p \equiv a \ mod\ p$

6. Essaie avec 11. Que se passe-t-il ?

9. Le système RSA :

Voir le document de synthèse sur le système RSA.

10. Recherche de grands nombres premiers : nombres de Fermat :

Pierre de Fermat a été un grand mathématicien dont nous avons déjà parlé et qui a laissé une conjecture célèbre qui n'a été démontrée que 350 ans plus tard par Andrew Wiles.

Par ailleurs, il a aussi affirmé que les nombres $F_k = 2^{2^k} + 1$ doivent être des nombres premiers ; mais il a avoué qu'il ne savait pas le démontrer pour tout nombre k.

1. Qui était Pierre de Fermat ?
2. Calcule les premiers nombres de Fermat (par exemple, pour $k = 1$, …, 5).
3. Sont-ils premiers ?

11. Recherche de grands nombres premiers : nombres de Mersenne :

Mersenne, contemporain de Fermat, a lui proposé de chercher des nombres premiers parmi les nombres :

$$M_r = 2^r - 1 \text{ où } r \text{ est lui-même un nombre premier}$$

1. Qui était Mersenne ?
2. Saurais-tu déterminer quelle est la nature (premier ou non) des nombres M_r pour r inférieur à 60 ?

Actuellement (novembre 2004), on ne sait pas démontrer s'il y a une infinité de nombres de Mersenne premiers. On vient de découvrir un facteur au nombre M_{971} premier nombre dont on ne savait rien.

On vient de découvrir un 41ème nombre premier M_r avec r = 24 036 583 et le nombre M_r a 7 235 733 chiffres…

3. Saurais-tu trouver la liste des 41 nombres de Mersenne qui sont premiers ?

Sais-tu qu'il y a un prix à gagner pour qui trouvera un 42ème nombre de Mersenne premier ?

Document 1

Alice aime son travail de paysagiste dans l'entreprise Thagem où elle doit aménager l'environnement de travail des mille cinq cents employés du site de Palombes-sur-Seine. L'essentiel de son activité est en plein air. C'est le printemps, les bouleaux lâchent leur pollen, et tout irait pour le mieux sans ce maudit rhume des foins qu'elle traîne depuis son adolescence. Ce soir en quittant le travail, il faudra qu'elle passe voir son médecin pour se faire prescrire un traitement anti-allergique.

En descendant les escaliers de son appartement parisien, elle allume son téléphone mobile :

– Allô, docteur Maison ? Puis-je passer cette après-midi vers 17 h 30 ?

Le rendez-vous est rapidement pris. La journée commence bien. Elle croise sans le remarquer le facteur venu déposer le courrier dans le hall de son immeuble et s'engouffre dans le métro, passe machinalement son sac à main le long du tourniquet et pense déjà aux aventures du commissaire Evenberg, héros du roman qu'elle a commencé avant-hier et qui lui fera passer plus vite son trajet.

Après avoir présenté son badge aux tourniquets d'accès de Thagem, son esprit commute déjà sur les tâches de la journée. Elle démarre la fourgonnette de service pour aller prendre livraison des nouveaux rosiers destinés à agrémenter les abords du lac artificiel, fierté du directeur, et qui a obtenu le prix du meilleur environnement d'entreprise de la région.

À midi, elle vérifie le solde de la carte Moneix qui lui permet de payer le repas sans avoir à se préoccuper de faire l'appoint aux caisses. 1 € 23. Elle doit la recharger.

La journée passe vite. Elle repasse le tourniquet vers la sortie. C'est l'heure de son rendez-vous chez le médecin. Il fait beau. Elle décide de prendre un vélo en libre service avec son passe Circulo.

Elle avait oublié le changement d'adresse du docteur Maison ! Sans se démonter, elle télécharge l'application de navigation vers son téléphone qui lui indiquera la nouvelle adresse et l'itinéraire pour arriver à l'heure.

– Puis-je avoir votre carte Vitalix ?

Alice se laisse ausculter, et se réjouit d'avance à l'idée de soulager son nez bouché, ses démangeaisons et l'irritation insupportable de ses yeux.

– Vous n'avez qu'une sévère allergie au pollen, je n'ai rien remarqué d'autre, vous prendrez du Rhumacyine en cas de production nasale importante.

Alice sourit intérieurement en pensant au vocabulaire médical.

– Cela fera vingt-trois euros.

– Acceptez-vous la carte bancaire ?

– Oui, je préfère même ! Avoir moins d'espèces dans mon cabinet me rassure. Je me suis déjà fait braquer.

De retour dans son appartement, elle branche son ordinateur en se souvenant soudain qu'aujourd'hui est la date limite pour valider la déclaration de revenus du foyer.

« Une mise à jour est disponible pour votre ordinateur, télécharger ? »

– Encore !

Elle accepte la mise à jour, l'ordinateur redémarre. Enfin elle valide sa déclaration des revenus.

Elle en profite pour commander sur Mississipi.fr la suite des aventures du commissaire Evenberg qui viennent de paraître.

C'est fini pour les préoccupations de la journée. Il est temps de se détendre avec Bob en allumant le téléviseur. Il y a au programme un bon film italien des années soixante-dix sur la chaîne thématique à laquelle ils sont abonnés.

La cryptologie, l'art des codes secrets, Philippe Guillot, edP, 2013

Document 2: Quelques messages codés

Message 1 : Décode le message suivant : 3 15 4 5 6 1 3 9 12 5 1 3 1 19 19 5 18

Message 2 : Décode le message suivant : F R G H G H M X O H V F H V D U

Message 3 : Décode le message suivant : C D G D M R E T A T O A E E A I S U R

Message 4 : un message a été codé. La personne qui a crypté son message a obtenu le code suivant :

32 15 13 11 43 43 15 14 15 41 35 32 54 12 15

En utilisant le document 3, décode ce message.

Message 5 : un message a été codé. La personne qui a crypté son message a obtenu le code suivant :

Zd bcmocx bfggocxk mcz&dokf

En utilisant le document 3, décode ce message.

Message 6 : un message a été codé. La personne qui a crypté son message a obtenu le code suivant :

HCNM BU GDSHBEAVMJZQU

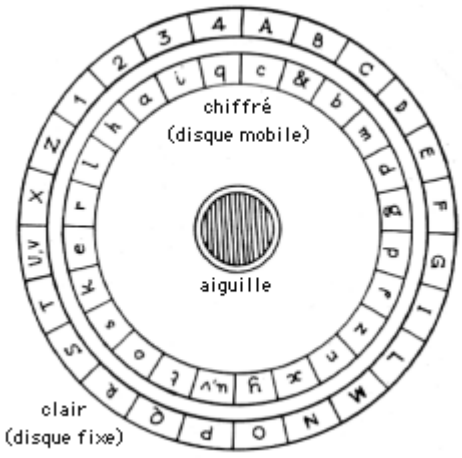
En utilisant le document 3, décode ce message.

Document 3

	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

Clé : MUSIQUE

	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



Document 1: corrigé

Alice aime son travail de paysagiste dans l'entreprise Thagem où elle doit aménager l'environnement de travail des mille cinq cents employés du site de Palombes-sur-Seine. L'essentiel de son activité est en plein air. C'est le printemps, les bouleaux lâchent leur pollen, et tout irait pour le mieux sans ce maudit rhume des foins qu'elle traîne depuis son adolescence. Ce soir en quittant le travail, il faudra qu'elle passe voir son médecin pour se faire prescrire un traitement anti-allergique.

En descendant les escaliers de son appartement parisien, elle allume son téléphone mobile :

– Allô, docteur Maison ? Puis-je passer cette après-midi vers 17 h 30 ?

Le rendez-vous est rapidement pris. La journée commence bien. Elle croise sans le remarquer le facteur venu déposer le courrier dans le hall de son immeuble et s'engouffre dans le métro, passe machinalement son sac à main le long du tourniquet et pense déjà aux aventures du commissaire Evenberg, héros du roman qu'elle a commencé avant-hier et qui lui fera passer plus vite son trajet.

Après avoir présenté son badge aux tourniquets d'accès de Thagem, son esprit commute déjà sur les tâches de la journée. Elle démarre la fourgonnette de service pour aller prendre livraison des nouveaux rosiers destinés à agrémenter les abords du lac artificiel, fierté du directeur, et qui a obtenu le prix du meilleur environnement d'entreprise de la région.

À midi, elle vérifie le solde de la carte Moneix qui lui permet de payer le repas sans avoir à se préoccuper de faire l'appoint aux caisses. 1 € 23. Elle doit la recharger.

La journée passe vite. Elle repasse le tourniquet vers la sortie. C'est l'heure de son rendez-vous chez le médecin. Il fait beau. Elle décide de prendre un vélo en libre service avec son passe Circulo.

Elle avait oublié le changement d'adresse du docteur Maison ! Sans se démonter, elle télécharge l'application de navigation vers son téléphone qui lui indiquera la nouvelle adresse et l'itinéraire pour arriver à l'heure.

– Puis-je avoir votre carte Vitalix ?

Alice se laisse ausculter, et se réjouit d'avance à l'idée de soulager son nez bouché, ses démangeaisons et l'irritation insupportable de ses yeux.

– Vous n'avez qu'une sévère allergie au pollen, je n'ai rien remarqué d'autre, vous prendrez du Rhumacyine en cas de production nasale importante.

Alice sourit intérieurement en pensant au vocabulaire médical.

– Cela fera vingt-trois euros.

– Acceptez-vous la carte bancaire ?

– Oui, je préfère même ! Avoir moins d'espèces dans mon cabinet me rassure. Je me suis déjà fait braquer.

De retour dans son appartement, elle branche son ordinateur en se souvenant soudain qu'aujourd'hui est la date limite pour valider la déclaration de revenus du foyer.

« Une mise à jour est disponible pour votre ordinateur, télécharger ? »

– Encore !

Elle accepte la mise à jour, l'ordinateur redémarre. Enfin elle valide sa déclaration des revenus.

Elle en profite pour commander sur Mississipi.fr la suite des aventures du commissaire Evenberg qui viennent de paraître.

C'est fini pour les préoccupations de la journée. Il est temps de se détendre avec Bob en allumant le téléviseur. Il y a au programme un bon film italien des années soixante-dix sur la chaîne thématique à laquelle ils sont abonnés.

La cryptologie, l'art des codes secrets, Philippe Guillot, edP, 2013

Les situations qui font intervenir un calcul cryptographique :

1. Authentification de l'abonné et chiffrement de la parole en téléphonie mobile.
2. Accès des facteurs parisiens aux immeubles à l'aide d'un badge qui les authentifie et autorise l'accès pendant l'horaire prévu de leur tournée.
3. Passage des tourniquets du métro avec le passe Navigo.
4. Accès aux locaux protégés à l'aide d'un badge d'accès.
5. Démarrage des véhicules après authentification de la puce incluse dans la clé de contact.
6. Chargement et dépense effectués avec la carte Moneo.
7. Sortie d'un local protégé à l'aide d'un badge.
8. Location d'un Vélib avec la carte Navigo.
9. Signature numérique des applications téléchargées sur les téléphones mobiles.
10. Chiffrement des données médicales confidentielles avec la carte Vitale.
11. Protection des transactions effectuées avec une carte bancaire.
12. Signature numérique des mises à jour des systèmes d'exploitation des ordinateurs.
13. Signature des déclarations de revenus effectuées sur Internet.
14. Sécurisation du commerce en ligne sur Internet.
15. Accès conditionnel aux programmes audiovisuels payants.

Solutions pour les messages codés:

Message 1 : codage alphabétique : CODE FACILE A CASSER

Message 2 : codage de Jules César : décalage de 3 rangs. CODE DE JULES CESAR

Message 3 : code de Marie Stuart : couper la liste en 2 et les aligner : CODAGE DE MARIE STUART

C D G D M R E T A T
O A E E A I S U R

Message 4 : c'est le carré de polybe. Chaque lettre est associée à un double chiffre, qui correspond à ses coordonnées dans le tableau.

CARRE DE POLYBE

Message 5 : c'est le cadran chiffrant d'alberti. Il contient deux disques que l'on peut faire tourner pour coder différemment à chaque fois. Chaque lettre correspond à une lettre aléatoire. Il manque les lettres J, U et W.

LE CADRAN CHIFFRANT D'ALBERTI

Message 6 : c'est la table de Vigenère. Elle utilise un mot clé.

Pour coder, on repère une lettre en haut, puis la lettre du mot clé qui correspond. A l'intersection de la colonne de la lettre en clair et de la ligne de la lettre du mot clé se trouve la lettre codée.

Pour décoder, on réécrit les lettres du mot clé sous le message codé. Ensuite, pour chaque lettre du message codé, on regarde la ligne de la lettre qui correspond dans le mot clé ; on parcourt cette ligne jusqu'à obtenir la lettre codée et on regarde à quelle colonne cela correspond : c'est la lettre en clair.

message	V	I	V	E	L	A	C	R	Y	P	T	O	G	R	A	P	H	I	E
clé	M	U	S	I	Q	U	E	M	U	S	I	Q	U	E	M	U	S	I	Q
chiffré	H	C	N	M	B	U	G	D	S	H	B	E	A	V	M	J	Z	Q	U

HCNMB UGDSH BEAVM JZQU