FICHE 1
Quelques messages cryptés à remettre au clair

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 151120210315141401091912011216080102052 0

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 1511202103151414010919120112160801020520

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 1511202103151414010919120112160801020520

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 1511202103151414010919120112160801020520

FICHE 2
Table de correspondance

Table de correspondance entre caractères utilisés dans les messages et nombres servant à les coder :

caractère	a	b	c	d	e	f	g	h
nombre	01	02	03	04	05	06	07	08

caractère	i	j	k	l	m	n	o	p
nombre	09	10	11	12	13	14	15	16

caractère	q	r	s	t	u	v	w	x
nombre	17	18	19	20	21	22	23	24

caractère	y	z
nombre	25	26

Table de correspondance entre caractères utilisés dans les messages et nombres servant à les coder :

caractère	a	b	c	d	e	f	g	h
nombre	01	02	03	04	05	06	07	08

caractère	i	j	k	l	m	n	o	p
nombre	09	10	11	12	13	14	15	16

caractère	q	r	s	t	u	v	w	x
nombre	17	18	19	20	21	22	23	24

caractère	y	z
nombre	25	26

Table de correspondance entre caractères utilisés dans les messages et nombres servant à les coder :

caractère	a	b	c	d	e	f	g	h
nombre	01	02	03	04	05	06	07	08

caractère	i	j	k	l	m	n	o	p
nombre	09	10	11	12	13	14	15	16

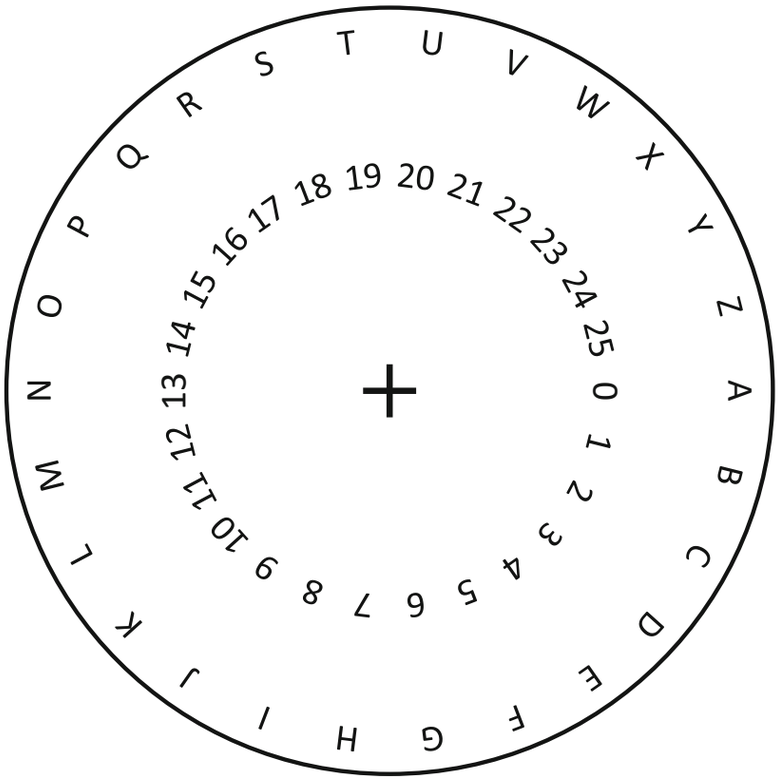
caractère	q	r	s	t	u	v	w	x
nombre	17	18	19	20	21	22	23	24

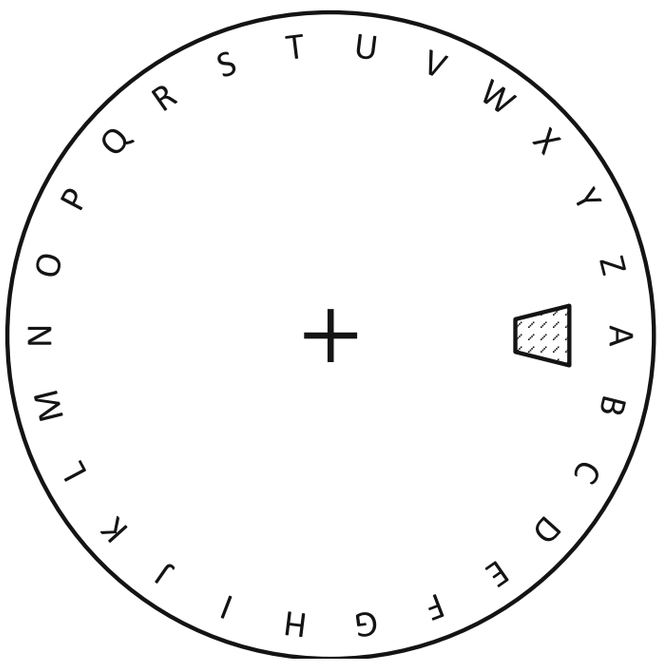
caractère	y	z
nombre	25	26

FICHE 3
Fabriquer un rouleau à chiffrer/déchiffrer

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

FICHE 4
Fabriquer un disque à chiffrer / déchiffrer





FICHE 5
Exercices de chiffrement mono-alphabétique

Exercice 1

À l'aide du tableau de correspondance ci-dessous, chiffre le message : « bonne chance pour casser ce code »

Alphabet clair	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
Alphabet chiffré	J	T	K	L	I	E	X	M	B	D	O	A	Z	U	C	H	S	W	V	P	Y	N	Q	F	G	R

Exercice 2

À l'aide du même tableau de correspondance, déchiffre le message « D JB EBUB »

Exercice 3a

Sachant qu'il existe $4x10^{26}$ (4 suivi de 26 zéros) clés possibles pour le chiffrement mono-alphabétique, combien de temps faudrait-il pour qu'un individu teste toutes les clés et déchiffre ainsi le message ? On suppose qu'une personne met seulement 5 secondes pour tester une clé (générer le message en clair et le lire pour voir s'il a une signification).

Exercice 3b

Et si tous les êtres humains travaillaient ensemble pour résoudre ce problème, combien de temps cela prendrait-il ?

Exercice 3c

Et si on utilisait le plus puissant des supercalculateurs (Tianhe-2, de l'armée chinoise), capable de tester 10^{15} clés par seconde, combien de temps cela prendrait-il ?

Exercice 4

Choisis un mot-clé ou une phrase-clé et remplit l'alphabet chiffré ci-dessous. Attention à ne pas utiliser la même lettre plusieurs fois !

Utilise cette nouvelle table de correspondance pour chiffrer un message court. Transmets ce message à ton voisin (ainsi que la clé) et vérifie qu'il déchiffre bien ton message.

Alphabet clair	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
Alphabet chiffré																										

FICHE 6
Analyse fréquentielle

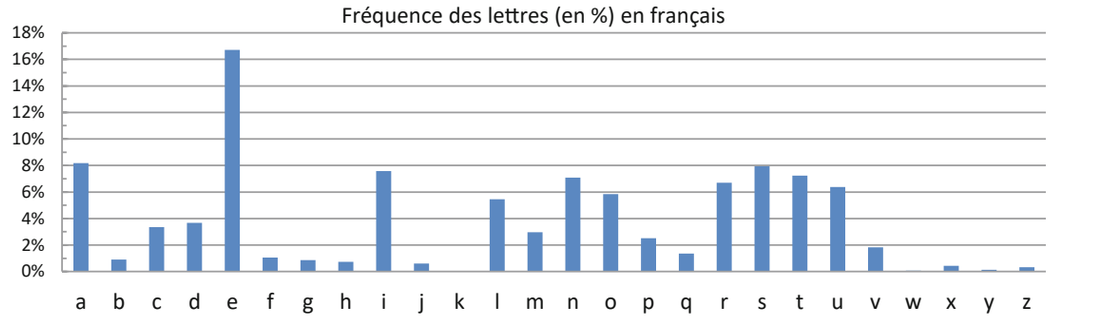
Exercice 1 : Relève la fréquence d'apparition de toutes les lettres de ce texte (il s'agit du préambule à la Déclaration universelle des droits de l'homme et du citoyen de 1789).
Les representants du peuple francais, constitues en assemblee Nationale, considerant que l'ignorance, l'oubli ou le mepris des droits de l'Homme sont les seules causes des malheurs publics et de la corruption des gouvernements, ont resolu d'exposer, dans une declaration solennelle, les droits naturels, inalienables et sacres de l'Homme, afin que cette declaration, constamment presente a tous les membres du corps social, leur rappelle sans cesse leurs droits et leurs devoirs; afin que les actes du pouvoir legislatif, et ceux du pouvoir executif, pouvant etre a chaque instant compares avec le but de toute institution politique, en soient plus respectes; afin que les reclamations des citoyens, fondees desormais sur des principes simples et incontestables, tournent toujours au maintien de la Constitution et au bonheur de tous.
(Note : pour simplifier le travail, nous avons supprimé les accents dans ce texte.)

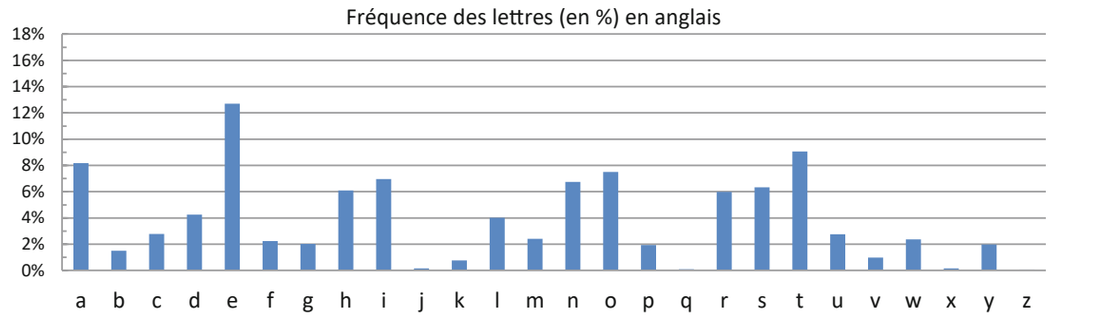
Exercice 2 : Voici un texte chiffré par substitution mono-alphabétique. La clé n'est pas connue. Défi : cryptanalysez ce texte.
ZRJ VDAARJ CLWJJRCK RK ERARMHRCK ZWIHRJ RK RULMP RC EHDWKJ. ZRJ EWJKWCBKWDCJ JDBWLZRJ CR FRMNRCK RKHR TDCERRJ GMR JMH Z'MKWZWKR BDAAMCR.

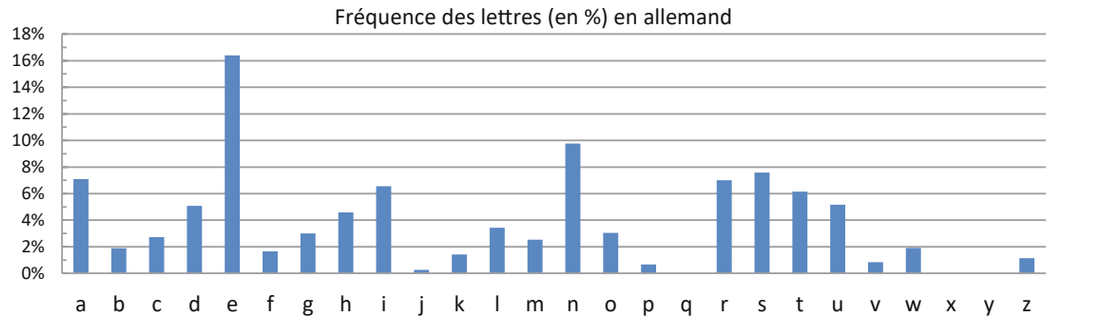
Exercice 1 : Relève la fréquence d'apparition de toutes les lettres de ce texte (il s'agit du préambule à la Déclaration universelle des droits de l'homme et du citoyen de 1789).
Les representants du peuple francais, constitues en assemblee Nationale, considerant que l'ignorance, l'oubli ou le mepris des droits de l'Homme sont les seules causes des malheurs publics et de la corruption des gouvernements, ont resolu d'exposer, dans une declaration solennelle, les droits naturels, inalienables et sacres de l'Homme, afin que cette declaration, constamment presente a tous les membres du corps social, leur rappelle sans cesse leurs droits et leurs devoirs; afin que les actes du pouvoir legislatif, et ceux du pouvoir executif, pouvant etre a chaque instant compares avec le but de toute institution politique, en soient plus respectes; afin que les reclamations des citoyens, fondees desormais sur des principes simples et incontestables, tournent toujours au maintien de la Constitution et au bonheur de tous.
(Note : pour simplifier le travail, nous avons supprimé les accents dans ce texte.)

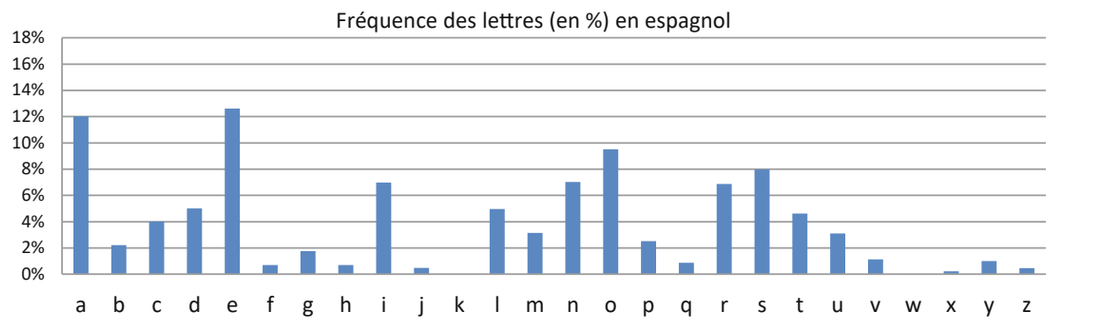
Exercice 2 : Voici un texte chiffré par substitution mono-alphabétique. La clé n'est pas connue. Défi : cryptanalysez ce texte.
ZRJ VDAARJ CLWJJRCK RK ERARMHRCK ZWIHRJ RK RULMP RC EHDWKJ. ZRJ EWJKWCBKWDCJ JDBWLZRJ CR FRMNRCK RKHR TDCERRJ GMR JMH Z'MKWZWKR BDAAMCR.

FICHE 7
Quelques histogrammes de référence









FICHE 8
César et Al-Kindi, les premiers acteurs de la cryptographie

Les hommes ont toujours voulu protéger leurs communications, qu'il s'agisse d'envoyer des ordres militaires, d'espionner les puissances ennemies, de faire du commerce ou même d'échanger des lettres amoureuses. À l'époque de Jules César, très peu de personnes savent lire, et sa méthode de chiffrement, pourtant très simple, suffit dans la plupart des cas.

Au sortir de l'antiquité, ce chiffrement s'est raffiné : plutôt que simplement décaler l'alphabet, on mélange les lettres apparemment au hasard (en réalité, on utilise un mot- ou une phrase-clé). Les possibilités sont immenses et il est impossible, si l'on ne connait pas la clé, d'essayer tous les alphabets possibles. Ce chiffrement par « substitution mono-alphabétique » (à une lettre « en clair » correspond une, et une seule, lettre chiffrée) restera inviolé pendant près de 1 000 ans, jusqu'à ce qu'Al-Kindi invente une méthode (appelée « analyse de fréquence ») qui permet de le briser en quelques minutes.

Al-Kindi, de son vrai nom Abū Yūsuf Ya'qūb ibn Isāq al-Kindī, est l'un des plus grands savants arabes, auteur de plus de 290 manuscrits sur l'astronomie, les mathématiques, la médecine, la philosophie… Au IXe siècle après J.-C., alors que l'Occident s'enferme dans l'obscurantisme, les sciences arabes connaissent leur âge d'or. Al-Kindi remarque que certaines lettres sont beaucoup plus fréquentes que d'autres et que le chiffrement mono-alphabétique ne modifie pas ces fréquences. Par exemple, si « e » est chiffré en « L », la lettre « L » aura la même fréquence, dans le message chiffré, que la lettre « e » dans le message clair. Connaissant la fréquence des lettres dans une langue, il devient facile de retrouver le texte clair, si celui-ci est assez long. Al-Kindi devient le premier cryptanalyste de l'histoire.

Il faudra attendre le XVe siècle pour que Léon Battista Alberti invente le chiffrement par substitution poly-alphabétique, puis que Blaise de Vigenère le perfectionne. Cette méthode utilise plusieurs alphabets chiffrés et résiste à l'analyse de fréquence. Elle fera autorité pendant 3 siècles jusqu'à ce que Charles Babbage découvre une méthode pour la briser.

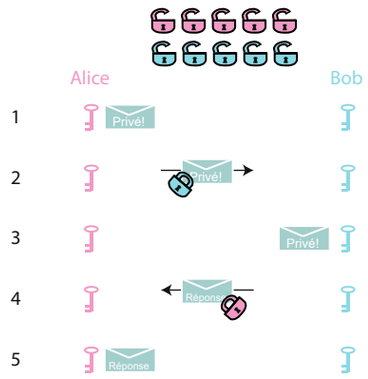
Depuis, la course continue entre les cryptographes (qui inventent des chiffrements) et les cryptanalystes (qui attaquent ces chiffrements). La cryptographie s'est mécanisée, puis informatisée. Les cryptographes actuels sont davantage mathématiciens que linguistes, mais les enjeux restent les mêmes. Cependant, comme nous le verrons, depuis l'essor d'Internet et la numérisation de nos communications, ces enjeux ont pris une dimension nouvelle :

- D'un côté, les États peuvent intercepter toutes les communications (e-mail, téléphone…) échangées entre deux individus, et souhaitent limiter l'usage de la cryptographie pour préserver la sécurité (espionner les terroristes, en particulier).
- D'un autre côté, les citoyens prennent conscience de l'importance qu'il y a de préserver leur intimité, qu'il s'agisse de leur vie de famille, leur santé, leurs opinions politiques, croyances religieuses, orientations sexuelles… Que peuvent devenir ces informations dans les mains d'un employeur, d'un assureur ou d'un gouvernement non démocratique ?

FICHE 9
Histoire de la cryptographie à clé publique

Dans les années 1960, l'informatique se développe et ouvre de nouvelles possibilités. La cryptographie, jusque-là réservée aux seules agences gouvernementales, devient accessible aux entreprises, voire aux particuliers. Mais, si deux personnes souhaitent communiquer secrètement, elles doivent se mettre d'accord sur une clé servant au chiffrement et au déchiffrement. L'échange des clés, qui a toujours été un casse-tête dans l'histoire de la cryptographie, devient un problème insurmontable à mesure que la cryptographie se démocratise.

Whitfield Diffie et Martin Hellman vont résoudre ce problème en 1976, dans un article intitulé New directions in cryptography resté fameux. Ces deux mathématiciens montrent qu'il est possible de communiquer secrètement en utilisant un chiffrement asymétrique. Le chiffrement asymétrique utilise 2 clés, l'une publique, l'autre privée. La clé publique permet de chiffrer le message, mais seule la clé privée permet de le déchiffrer.



Deux ans plus tard, Ron Rivest, Adi Shamir et Leonard Adleman améliorent cette idée pour créer l'algorithme RSA (nommé d'après leurs initiales). L'algorithme RSA utilise, pour simplifier, un très grand nombre, N, que l'on peut décomposer comme le produit de 2 nombres premiers *p* et *q*. N=*p*x*q*. N est la clé publique, tandis que *p* et *q* constituent la clé privée. N permet de chiffrer un message, mais l'opération de déchiffrement nécessite de connaître *p* et *q*. La sécurité de RSA repose sur le fait qu'il est très difficile de calculer les diviseurs d'un très grand nombre (on dit aussi « factoriser » un nombre). Même avec les meilleurs calculateurs, la factorisation peut prendre des années si le nombre est suffisamment grand. Pour cette raison, RSA est l'algorithme de chiffrement le plus utilisé dans le monde.

RSA est très sûr mais nécessite des moyens de calcul importants. Paul Zimmermann a résolu ce problème en 1991 en inventant un logiciel appelé PGP (*pretty good privacy*) qui est un compromis entre un chiffrement « classique » à clé privée et un chiffrement RSA. PGP a permis de démocratiser la cryptographie en la rendant accessible aux ordinateurs grand public. Cela lui a valu des poursuites judiciaires de la part du gouvernement américain. Certains gouvernements tentent en effet de limiter l'usage de la cryptographie de manière à pouvoir continuer d'intercepter les communications. Pour cela, ils exigent en général :

• Soit de limiter la taille des clés utilisées : une clé de taille « moyenne » est trop difficile à casser pour un ordinateur classique, mais pas pour un supercalculateur. Ainsi, la confidentialité est assurée vis-à-vis des particuliers, mais pas des agences gouvernementales ni des très grandes entreprises qui possèdent des supercalculateurs.

• Soit de déposer ses clés privées dans un « coffre » géré par un organisme « de confiance » (une agence gouvernementale par exemple). Ainsi, les communications sont secrètes pour tout le monde sauf pour ceux qui ont accès au coffre.

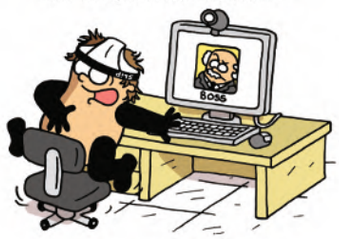
Longtemps réservée aux armées et aux diplomates, la cryptographie est aujourd'hui utilisée par de nombreux services : les banques (cartes bancaires, transactions sécurisées sur Internet), le commerce électronique, les messageries électroniques (carte SIM, e-mail…), les services médicaux (carte Vitale…), le vote électronique, etc.

FICHE 10
Dix conseils pour rester Net sur le Web

10 conseils de la CNIL pour rester Net sur le web

1 Réfléchis avant de publier !

Sur internet, tout le monde peut voir ce que tu mets en ligne : infos, photos, opinions.



2 Respecte les autres !

Tu es responsable de ce que tu publies en ligne alors modère tes propos sur les réseaux sociaux, forums... Ne fais pas aux autres ce que tu n'aimerais pas que l'on te fasse.

3 Ne dis pas tout !

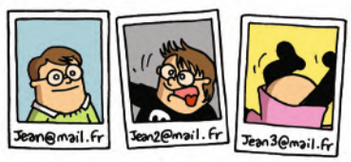
Donne le minimum d'informations personnelles sur internet. Ne communique ni tes opinions politiques, ni ta religion, ni ton numéro de téléphone...

4 Sécurise tes comptes !

Paramètre toujours tes profils sur les réseaux sociaux afin de rester maître des informations que tu souhaites partager.

5 Crée-toi plusieurs adresses e-mail !

Tu peux utiliser une boîte e-mail pour tes amis et une autre boîte e-mail pour les jeux et les réseaux sociaux.



6 Attention aux photos et aux vidéos !

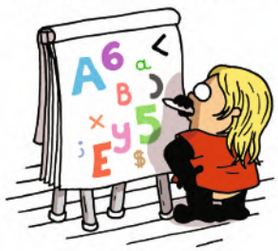
Ne publie pas de photos gênantes de tes amis ou de toi-même car leur diffusion est incontrôlable.

7 Utilise un pseudonyme !

Seuls tes amis et ta famille sauront qu'il s'agit de toi.

8 Attention aux mots de passe !

Ne les communique à personne et choisis-les un peu compliqués : ni ta date ni ton surnom !



9 Fais le ménage dans tes historiques !

Efface régulièrement tes historiques de navigation et pense à utiliser la navigation privée si tu utilises un ordinateur qui n'est pas le tien.

10 Vérifie tes traces !

Tape régulièrement ton nom dans un moteur de recherche pour découvrir quelles informations te concernant circulent sur internet.

CNIL
Commission Nationale de l'Informatique et des Libertés

Retrouvez d'autres conseils et astuces sur www.cnil.fr et sur www.educnum.fr ! #EducNum