Initiation à la cryptographie symétrique

Charles De Clercq

1 Introduction

L'objectif de cette activité est double. Il s'agit à la fois d'introduire les problèmes bien réels de la cryptographie, mais aussi l'utilisation d'outils mathématiques pour (tenter) de résoudre ces problèmes. Nous avons fait le choix de vous faire découvrir la cryptographie avant tout par l'*expérience*, l'idée étant que pour réussir à décrypter un code, il vaut mieux parfois être observateur et attentif, plutôt qu'avoir recours à un super-calculateur !

Je vous recommande vivement de consulter le site `http://www.bibmath.net/` ainsi que l'ouvrage *Cours de cryptographie* de Gilles Zémor si vous désirez en savoir plus sur le sujet. Ce cours est très fortement inspiré de ces références, qui proposent bien d'autres méthodes et applications cryptographiques.

2 Qu'est-ce que la cryptographie ?

La cryptographie est l'art de transmettre des données confidentielles. Son objectif est de mettre en place des outils permettant de transmettre un message sous forme cryptée, de telle sorte que seules certaines personnes puissent retrouver le message originel.

Le message de départ, avant qu'il ne soit crypté, est le *message en clair*. Le message obtenu après avoir crypté le message en clair est le *cryptogramme*. Avant de rentrer dans de plus amples détails, voilà un exercice qui devrait éveiller votre curiosité. Quelle sera votre stratégie ?

***Exercice* 1**

`ZS GWUBS HFOQS JCIG OJOWH Z'OWF RS QSG QVCGSG EI'SQFWJSBH GIF ZSG AIFG ZSG JOUOPCBRG, ZSG JCZSIFG, DCIF GS RCBBSF SBHFS SIL RSG FSBGSWUBSASBHG GIF ZSG USBG RI JCWGWBOUS CI ZSG QCIDG O TOWFS, EI'WZG GCBH GSIZG O RSQCRSF.`

`ZCIWG OFOUCB`

Solution

Le signe tracé vous avait l'air de ces choses qu'écrivent sur les murs les vagabonds, les voleurs, pour se donner entre eux des renseignements sur les gens du voisinage ou les coups à faire, qu'ils sont seuls à décoder.

Louis Aragon

3 Problématiques de la cryptographie

3.1 Un peu d'histoire

Un des aspects essentiels de la cryptographie est donc de trouver un moyen de cryptage (on parle de *fonction cryptographique*) aussi difficile à déjouer que possible pour les éventuels "pirates". Comme vous

l'avez (peut-être) vu, le cryptage de l'exercice 1 n'est pas très sophistiqué. Il s'agit en fait du premier exemple d'usage de la cryptographie, le *Chiffrement de César*. Son principe est simple : on choisit un chiffre, grâce auquel on décale l'alphabet. On obtient par exemple pour le chiffre 4 le cryptage suivant.

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
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

Suétone, un écrivain Romain du I^{er} siècle évoque dans *La vie des 12 Césars* que Jules César employait déjà à cette époque le même type de chiffrement que celui de l'exercice 1. L'exercice suivant est l'occasion de réfléchir sur les stratégies mises en place lors de l'exercice 1.

***Exercice* 2**

Pouvez-vous identifier le défaut principal du chiffrement de César ?

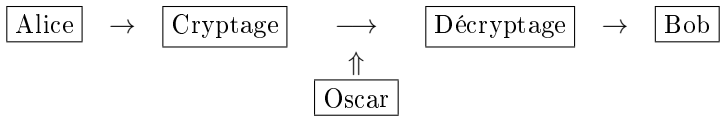
Solution

Il n'y a que 26 décalages possibles pour le chiffrement de César, autant que de lettres de l'alphabet (en comptant le décalage de 0 !). Un ordinateur ou un humain (suffisamment patient) peut très facilement tester ces 26 possibilités et est sûr de décrypter le cryptogramme.

3.2 Et les destinataires ?

Comme nous l'avons vu, le chiffrement de César est loin d'être inviolable. Mais un autre problème bien plus général se pose : comment le destinataire peut-il décrypter le message, puisqu'il ne connaît pas a priori le chiffre de décalage ? Bien entendu, il n'est pas question de transformer le destinataire en "pirate" !

Le destinataire doit (ne serait-ce que pour des questions de temps) être capable de décrypter le message sans encombre. Cette situation (dite de *communication confidentielle*) est présentée le plus souvent de la façon suivante :



Deux personnes que l'on appelle, comme il est d'usage, Alice et Bob, veulent communiquer de manière confidentielle. Le *cryptanalyste* (le "pirate") Oscar réussit a obtenir le message crypté et essaie de le décrypter. Comme nous l'avons vu plutôt avec le chiffrement de César, pour que Bob puisse décrypter le message, il faut qu'il connaisse la "clé", c'est à dire le décalage choisi par Alice pour crypter le message en clair.

La parade à ce problème trouvée par César durant l'antiquité est originale. César rasait la tête d'un esclave et inscrivait la clé sur son crâne, puis attendait que ses cheveux repoussent avant de l'envoyer au destinataire. Cette méthode est aussi discutable humainement qu'inefficace bien entendu, et nous verrons par la suite comment contourner ce problème.

Notons que le chiffrement de César a été encore utilisé bien après l'antiquité, et même jusqu'au 20eme siècle. Il est encore d'ailleurs utilisé dans certains forums de discussions sur internet pour éviter les spoilers !

3.3 Cryptographie par permutation

Un exemple légèrement plus élaboré que le cryptage de César est le *cryptage par permutation*. Le fonctionnement est très simple et similaire au cryptage de César. Chaque lettre est remplacée par une autre, choisie au hasard. Il n'est donc plus question de retenir que le "décalage" comme pour la méthode de César.

Bien entendu, il ne faut pas choisir la même lettre pour crypter deux lettres différentes.
Voilà un exemple de cryptage par permutation.

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

***Exercice* 3**

Combien y a-t-il de cryptages par permutation différents ?

Solution

Pour remplacer le A, on dispose des 26 lettres de l'alphabet. Pour le B il n'y a plus que 25 possibilités, et ainsi de suite. Il y a donc $26 \times 25 \times 24 \times \cdots \times 2 \times 1$ possibilités de cryptage par permutation.

Ce nouveau type de cryptage évite un écueil : il n'est plus possible de décrypter le cryptogramme en essayant brutalement toutes les possibilités (il y en a trop !). Nous allons voir dans la prochaine partie qu'il existe cependant d'autres possibilités pour décrypter de tels messages.

4 Les limites du cryptage par permutation

Comme nous l'avons vu précédemment, le cryptage par permutation n'est pas raisonnablement attaquable en testant toutes les clés possibles (on parle dans ce cas d'une attaque *brute force*). Comment allez-vous donc réussir à décrypter les messages suivants ?

***Exercice* 4**

```
                                                                F RFDCO,

   BEQDO QSQMQO,

   V'QORQDQ RFD SF RDQOQUGQ MLAO DFRRQSQD S'CHRLDGFUBQ PA BLUGQYGQ FNCU PQ PQBDJRGQD AU
HQOOFXQ. SF NLDBQ IDAGQ U'QOG DCQU OFUO AU RQA PQ HFSCBQ.

   ICQU BLDPCFSQHQUG,
BEFDSQO PQ BSQDBT
```

Solution

A Paris,

Chers élèves,

J'espère par la présente vous rappeler l'importance du contexte afin de décrypter un message. La force brute n'est rien sans un peu de malice.

Bien cordialement,
Charles De Clercq

***Exercice* 5**

`MV OUKDO YFUQ KLIKOQ VOQ FCKMLUQ SIHFMUOQ NVIQ YO SFQFDY TIO YO YOCMQMLU.`

`FUYDO XMYO`

Solution

`Il entre dans toutes les actions humaines plus de hasard que de décision.`

`André Gide`

***Exercice* 6**

`UT RULD ETPPCBUT DTIPTE ST IT YFQST DTPKCE NL'CU Q'O KCE KLILQ DTIPTE.`

`JTKQ-MPKQIFCD STQCKL`

Solution

Le plus terrible secret de ce monde serait qu'il n'y ait aucun secret.

Jean-François Deniau

Comme le montrent les exercices précédents, il existe malgré l'énorme nombre de possibilités plusieurs façons de résoudre (avec un peu de chance et beaucoup d'essais) un cryptogramme crypté par permutation. En effet il faut savoir tenir compte, comme à l'exercice 4, des indices extérieurs au code mais pourtant bien présents dans le message. Ce détail, bien qu'il paraisse anodin à première vue, a déjà été décisif dans l'histoire de la cryptographie, comme nous le verrons lorsque nous aborderons le XX^{eme} siècle et la machine *Enigma*.

Un autre indice déterminant est la répartition et la proportion des lettres dans le cryptogramme. En effet les lettres ont une fréquence d'apparition bien spécifique dans chaque langue. Par exemple en Français, la lettre apparaissant le plus fréquemment est le "E". En observant le code crypté, il est fort probable de pouvoir identifier le cryptage de cette lettre en observant la lettre qui est la plus présente. Une étude des mots courts permet aussi de proche en proche de pointer des absurdités et (avec un peu de chance) de s'approcher d'un décryptage complet.

Bien entendu, notre chère Alice pourrait bien nous réserver une fourberie, en fournissant par exemple à Bob un message ne contenant aucun "E". Cette méthode n'est donc pas infaillible mais s'avère parfois très performante.

5 Autres méthodes cryptographiques

5.1 Des lettres aux chiffres

Un autre moyen de cryptage est le *carré de Polybe*. Polybe (historien grec du II^{eme} siècle avant J.C.) dispose les lettres de l'alphabet dans un tableau de taille 5×5. Pour crypter un message, il suffit de remplacer une lettre par ses coordonnées.

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

Le carré de Polybe

La lettre "A" est donc remplacée par 11, tandis que la lettre "S" correspondra a 43 après cryptage. Remarquons que cette méthode a deux intérêts. D'une part le message crypté est plus difficile à lire car il n'est plus évident de reconnaître directement les lettres. En outre seuls les neuf symboles $1, ..., 9$ sont utilisés. Notons enfin que l'on peut compliquer encore un peu plus la situation en remplissant le tableau de Polybe dans un autre ordre que l'ordre alphabétique.

Le carré de Polybe était encore utilisé au début du XX^{eme} siècle. Les nihilistes Russes (une organisation clandestine visant a renverser le Tsar) utilisaient cette méthode pour communiquer quand ils étaient emprisonnés, comme l'atteste la photographie ci-dessous des geôles de Saint Petersbourg, où les détenus communiquaient en frappant en rythme, à la manière du Morse.

FIGURE 1 – Panneau à l'entrée d'une cellule de St. Petersbourg

Exercice 7

Cryptez le titre de votre livre (ou film, ou musique, ou jeu...) préféré à l'aide du carré du carré de Polybe. Faites-le décrypter par votre voisin.

5.2 La méthode de Vigenère

Nous présentons désormais la méthode considérée comme l'aboutissement des méthodes classiques de cryptographie. Les méthodes précédentes (méthode de César, méthode par permutation, tableau de Polybe) sont bien faibles face aux attaques car il est facile d'y identifier la fréquence d'apparition des lettres. C'est au XVI^{eme} siècle qu'est introduite une nouvelle méthode, la méthode de Vigenère.

FIGURE 2 – Blaise de Vigenère

Vigenère, diplomate, écrivain et historien Français publie en 1586 le *Traicté des chiffres ou Secrètes manières d'écrire*, proposant une nouvelle méthode de cryptage. L'idée est d'améliorer la méthode de César, en modifiant le décalage à chaque nouvelle lettre. L'intérêt de cette méthode est donc qu'au fur et à mesure du texte, une même lettre est cryptée de manières différentes, puisque le décalage change à chaque lettre. Plutôt que de longues explications, examinons cette méthode par un exemple.

Choisissons le message en clair "CRYPTOGRAPHIE" ainsi que la clé "TEST". On dispose le message en clair et la clé de la manière suivante pour obtenir le cryptogramme :

C	R	Y	P	T	O	G	R	A	P	H	I	E
T	E	S	T	T	E	S	T	T	E	S	T	T

Une fois cela fait, il devient très simple de crypter notre mot, en se reportant au tableau de correspondance de Vigenère, présenté à la figure 3.

A la première lettre "C" est associée la clé "T". La première lettre du cryptogramme est la lettre se trouvant à l'intersection de la ligne "C" et de la colonne "T", c'est à dire "V". On recommence l'opération pour chacune des lettres afin d'obtenir le cryptogramme

VVQIMSYKTTZBX

Comme vous le remarquez, il est complètement vain d'essayer de décrypter ce message en fonction de la répartition des lettres, puisque par exemple la lettre "V" correspond dans le cryptogramme aux deux lettres "C" et "R". Le cryptage est donc très simple avec cette méthode, mais qu'en est-il du décryptage ?

Le décryptage est lui aussi très aisé, à condition de connaître la clé qui a été utilisée pour crypter. On introduit à nouveau le cryptogramme ainsi que la clé dans un tableau comme suit :

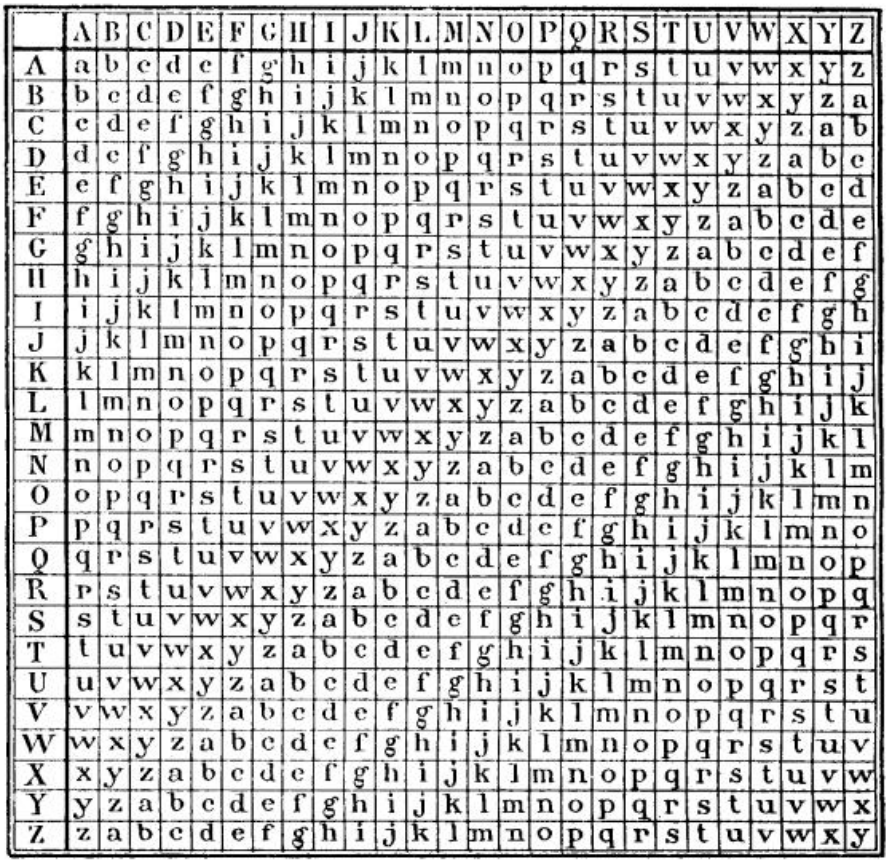
V	V	Q	I	M	S	Y	K	T	T	Z	B	X
T	E	S	T	T	E	S	T	T	E	S	T	T

Pour retrouver la première lettre du message en clair, on regarde la colonne associée à la première lettre de la clé : "T". Dans cette colonne on retrouve la première lettre du cryptogramme : "V". La première lettre du message en clair n'est autre que la lettre correspondant à la ligne du "V", c'est à dire "C".

***Exercice* 8**

Vérifier que l'on retrouve bien le message en clair par cette méthode. Choisissez une clé et cryptez votre livre (votre groupe de musique, votre matière...) préféré en utilisant cette clé et la méthode de Vigenère. Donnez la clé a votre voisin ainsi que le cryptogramme pour qu'il puisse retrouver le message en clair.

FIGURE 3 – Tableau de correspondance de Vigenère



	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

La méthode de Vigenère introduit donc la notion de clé, qui est essentielle. Il peut cependant paraître inutile de crypter un message si la personne devant le décrypter ne connaît pas la clé (ce qui est inexact, comme nous le verrons par la suite). Un des avantages de la méthode de Vigenère est que la clé est la même, pour crypter le message en clair et pour décrypter le cryptogramme. On parle alors de *cryptographie symétrique*.

***Exercice* 9**

Décrypter le code suivant.

```
QEXHSDI DI VMGINIRI.
```

Solution

Indice : la clé est constituée de 2 voyelles. La clé s'avère être EA et on décrypte en trouvant : Méthode de Vigenère.

6 Aperçu de certaines méthodes du XXème siècle

Toutes ces méthodes semblent bien archaïques, à l'heure de l'informatique et d'Internet. Nous allons cependant voir dans cette partie que les problématiques (et les moyens de décryptages) évoqués précédemment ont eu une grande importance, en particulier au XX^{eme} siècle.

6.1 Quand la cryptographie intervient dans l'histoire

C'est au XX^{eme} siècle que la cryptographie s'impose comme une science à part entière, en grande partie (comme souvent malheureusement) pour son utilité lors de la première et la seconde guerre mondiale.

Évoquons dans un premier temps exemple frappant de l'importance prise par la cryptographie datant de 1917. La première guerre mondiale fait alors rage en Europe, et les États-Unis n'ont pas pour le moment décidé de prendre part aux hostilités. En Janvier 1917, l'Allemagne cherche à couper à tout prix les ravitaillements américains pour l'Angleterre, mais ne souhaite pas couler trop de navires Américains pour éviter leur entrée en guerre.

Afin de limiter les approvisionnements Américains, les Allemands décident d'inciter le Mexique à déclarer la guerre aux États-Unis en échange d'une aide financière et militaire. Arthur Zimmermann, ministre Allemand des affaires étrangères, envoie donc au président Mexicain un message crypté contenant les informations nécessaires ainsi que les intentions allemandes.

Le message est finalement intercepté par les services secrets britanniques, qui réussissent à décrypter le message en quelques semaines, le 22 Février 1917. Une fois transmis au président Américain, la réponse ne se fait pas attendre et le 6 Avril 1917, le président Woodstone déclare officiellement la guerre à l'Allemagne.

6.2 La seconde guerre mondiale

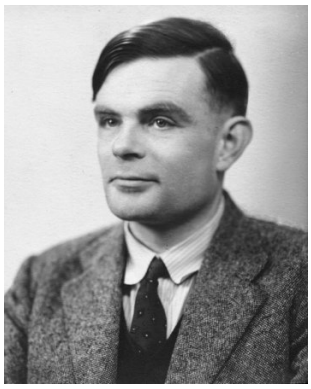
La cryptographie semble définitivement un enjeu majeur dès la seconde guerre mondiale. En 1940, l'Europe est ravagée par la guerre. La France et la Pologne ont capitulé et les sous-marins Allemands sèment la terreur le long des côtes Anglaises. Afin d'être toujours plus imprévisibles, ils communiquent à l'aide d'une machine mise en place par l'état-major Allemand nommée "Enigma".

FIGURE 4 – La machine Enigma

Cette machine permet de crypter n'importe quel message de manière très efficace et permet aux sous-marin de communiquer en toute impunité. L'Angleterre recrute alors de nombreux mathématiciens en vue

d'essayer de décrypter les messages cryptés à l'aide d'Enigma. Parmi eux se trouve Alan Türing, mathématicien qui conçoit à ces fins le premier ordinateur, baptisé Colossus.

FIGURE 5 – Le mathématicien Alan Türing



A l'aide d'informations glanées dans certains sous-marins (et grâce à certaines faiblesses dans le protocole Allemand), mais aussi grâce au soutien conjugué de la Pologne et des États-Unis, les Anglais parviennent finalement à décrypter ces messages et sauver nombre de navires. Cet avantage est d'autant plus décisif que les Allemands ne sauront jamais que cette prouesse a été réalisée, tandis que les alliés préparaient leurs débarquements en toute discrétion.

6.3 Une application actuelle de la cryptographie

Le système de cryptage le plus utilisé actuellement est le système RSA, que vous avez étudié lors d'un cours précédent. Rappelons que le système RSA repose sur la difficulté à factoriser les entier de grande taille en un produit de facteurs premiers. Nos cartes bancaires, par exemple, utilisent ce système de cryptage.

Toute carte bancaire est équipée d'une puce qui renferme une signature unique et ne pouvant être modifiée. Cette signature repose sur une clé (très) secrète à laquelle très peu de personnes ont accès. En insérant une carte dans un terminal, celui-ci vérifie que la signature a bien été générée par la clé secrète pour autoriser une transaction.

En 1998, Serge Humpich, un ingénieur Français, réussit a découvrir la clé secrète en factorisant l'entier sur lequel repose le système RSA. Il arrive ainsi a montrer qu'il est possible de fabriquer une carte bancaire fonctionnant chez les commerçants. Il est condamné en 2000 pour cette falsification et pour avoir montré qu'il était possible de contourner ce système. Une nouveau nombre (plus grand et donc plus difficile à factoriser) remplace depuis cette affaire l'ancien, et la nouvelle clé secrète est pour le moment inviolée.

7 Cryptographie symétrique et informatique

Comme nous l'avons vu précédemment, le cryptage de Vigenère s'avère être un système assez performant. Nous nous proposons maintenant de voir comment mettre en place le cryptage de Vigenère sur ordinateur.

7.1 Représentation binaire des nombres entiers

Nous représentons les nombres avec un système décimal (en base 10) dont les éléments sont les symboles $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. D'autres systèmes existent et sont utilisés quotidiennement. Par exemple pour la mesure du temps il est d'usage de travailler en base 60, puisque 145 secondes correspondent à 2 minutes et 25 secondes.

L'informatique repose sur un composant electronique : le *transistor*. Le transistor a été inventé en 1948 par les Américains Bardeen, Shockley et Brattain. La particularité de ce composant est qu'il possède deux positions : 1 qui correspond à "ouvert" et 0 qui correspond à "fermé". De plus une impulsion électrique permet de faire passer le transistor de la position 0 a 1 et inversement.

Comme nous allons le voir, il est possible (en travaillant en base 2) de représenter tous les nombres, uniquement avec des 0 et des 1. C'est pourquoi l'ordinateur peut se révéler utile pour calculer. En représentant de la même manière les lettres de l'alphabet par des 0 et des 1, l'ordinateur devient aussi une aide puissante pour crypter et décrypter des messages.

7.2 Comment trouver l'écriture d'un entier en base 2

L'écriture d'un nombre entier en base 2 est simple et repose sur la division euclidienne. Considérons un nombre entier n, et effectuons la division euclidienne de n par 2 :

$$n = 2 \times q_1 + r_1, \text{ où } r_1 = 0 \text{ ou } r_1 = 1$$

En prenant soin de noter le reste r_1, on effectue cette fois la division euclidienne du premier quotient q_1 par 2 :

$$q_1 = 2 \times q_2 + r_2, \text{ où } r_2 = 0 \text{ ou } r_2 = 1$$

On note à nouveau le 2^{eme} reste r_2 et on effectue la division euclidienne de q_2, le deuxième quotient, par 2 :

$$q_2 = 2 \times q_3 + r_3, \text{ où } r_3 = 0 \text{ ou } r_3 = 1$$

On continue ainsi à diviser les quotients successifs par 2 jusqu'à ce qu'un certain quotient q_s soit nul. On dispose enfin les restes successifs gardés précieusement dans un tableau de la manière suivante :

2^{s-1}	$\cdots$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
r_s	$\cdots$	r_6	r_5	r_4	r_3	r_2	r_1

Comme d'habitude, cette méthode est aisée à comprendre par l'exemple. Écrivons donc en base 2 le nombre 54. On effectue tout d'abord la division euclidienne de 54 par 2 :

$$55 = 2 \times 27 + 1.$$

On note donc $r_1 = 1$, et on effectue la division euclidienne de 27 (le premier quotient) par 2 :

$$27 = 2 \times 13 + 1.$$

Ce qui nous donne $r_2 = 1$ et on effectue la division euclidienne de 13 par 2 :

$$13 = 2 \times 6 + 1.$$

D'où $r_3 = 1$, et on continue le processus :

$$6 = 2 \times 3 + 0.$$

Donc $r_4 = 0$ et $q_4 = 3$, et finalement

$$3 = 2 \times 1 + 1$$

ce qui implique que $r_5 = 1$ et $q_5 = 1$. Enfin on a

$$1 = 2 \times 0 + 1$$

d'où $r_6 = 1$ et $q_6 = 0$, on arrête donc le processus et on place les précédents restes comme suit dans un tableau :

$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
r_6	r_5	r_4	r_3	r_2	r_1
1	1	0	1	1	1

Remarquez que l'on a

$$\begin{aligned} 2^0 \times r_1 + 2^1 \times r_2 + ... + 2^5 \times r_6 &= 2^0 + 2^1 + 2^2 + 2^4 + 2^5 \\ &= 1 + 2 + 4 + 16 + 32 \\ &= 55 \end{aligned}$$

C'est la raison pour laquelle on présente la décomposition binaire d'un nombre sous la forme de ce tableau.

***Exercice* 10**

Trouver l'écriture binaire des nombres 18, 73, 1024, 884.

Solution

En base 2, on trouve 18 = (10010), 73 = (1001001), 1024 = (10000000000) et 884 = (1101110100).

***Exercice* 11**

Additionner les nombres (1101110100) et (1101110100) en base 2. A quel chiffre le résultat correspond-t-il en base 10 ?

Solution

L'addition en base 2 donne (11011101000) qui vaut précisément 1768.

Le cryptage de Vigenère est donc désormais très simple a implémenter informatiquement. L'alphabet possède 26 lettres, et tous les nombres inférieurs à 26 s'écrivent (en base 2) avec au plus 5 "0" ou "1" (on parle de *bits*). Le message en clair "AIR" peut donc s'écrire en convertissant en binaire la place de chacune de ses lettres dans l'alphabet :

`(00001-01001-10010).`

Crypter avec la méthode de Vigenère ne s'en avère que plus simple. Choisissons donc la clé "ART". L'écriture de ce mot en base 2 est `(00001-10010-10100)`. Pour crypter le message, il suffit d'ajouter ces longues séries (en oubliant les retenues !) de 0 et de 1. Le message crypté sera donc donné par

`(00000-11011-00110)`

Pour décrypter ce message rien de plus simple, il suffit d'ajouter à nouveau la clé `(00001-10010-10100)` au cryptogramme (toujours sans compter les retenues !) pour retrouver le message initial. Cette méthode de cryptage bien connue est appelée la méthode XOR.

***Exercice* 12**

Faite complètement l'exemple précédent, ou si vous préférez choisissez une autre message en clair et/ou une autre clé.

7.3 Une dernière stratégie cryptographique

Pour finir ce cours, nous allons faire une activité qui devrait vous mettre face à un problème cryptographique dramatiquement réel. Choisissons de séparer la classe en deux groupes, qui vont tous deux devoir faire office d'Alice et de Bob à la fois.

Chaque groupe choisit et garde jalousement sa clé secrète, ainsi qu'un message en clair. Une fois que le message crypté à l'aide de la méthode de Vigenère est transmis à l'autre groupe, l'autre groupe doit réussir à décoder ce message, sans même connaître la clé. Qu'allez vous donc faire ?