UN APERÇU DE *l'histoire de la cryptologie*

INTRODUCTION

Les communications ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Le besoin d'être en mesure d'envoyer un message de façon sécuritaire est probablement aussi ancien que les communications elles-mêmes. D'un point de vue historique, c'est lors des conflits entre nations que ce besoin a été le plus vif. Dans notre monde moderne, où diverses méthodes de communication sont utilisées régulièrement, le besoin de confidentialité est plus présent que jamais à une multitude de niveaux. Par exemple, il est normal qu'une firme désire protéger ses nouveaux logiciels contre la piraterie, que les institutions bancaires veuillent s'assurer que les transactions sont sécuritaires et que tous les individus souhaitent que l'on protège leurs données personnelles. Le besoin de communications sécuritaires a donné naissance à la science que nous appelons cryptologie.

Cette brochure offre un bref aperçu de la cryptologie, tout particulièrement du point de vue historique. On y décrit des méthodes de chiffrement classiques qui étaient utilisées il y a 2000 ans ainsi que d'autres méthodes datant du 20e siècle. À la fin de la brochure, vous trouverez des exercices ainsi qu'une liste de références.

Pour les lecteurs intéressés, il existe une multitude de sources d'information sur l'histoire de la cryptologie. Certaines machines à chiffrer sont exposées au Musée canadien de la guerre à Ottawa. On trouve des musées qui traitent (de façon partielle ou exhaustive) des aspects historiques de la cryptographie aux États-Unis (au National Cryptologic Museum près de Fort Meade au Maryland), en Grande-Bretagne (à Bletchley Park près de Londres) ainsi qu'au Canada (au Musée des communications et de l'électronique de Kingston, en Ontario). Il est assez facile de trouver des livres traitant de l'histoire de la cryptographie pendant la Deuxième Guerre mondiale, notamment de la fameuse machine Enigma allemande, un appareil à roues codeuses. Le «Web» (W3 sur l'Internet) est aussi une riche source d'informations, bien que la qualité de celles-ci puisse varier d'un site à l'autre. Une liste de sites (en particulier ceux correspondant aux trois musées mentionnés ci-haut) est fournie à la fin de la brochure.

UN APERÇU DE *l'histoire de la cryptologie*

LA CRYPTOLOGIE

L'opération de *chiffrement* transforme un *texte en clair* en un *texte chiffré*, appelé *cryptogramme*, au moyen d'une clé (qu'on dénomme la *clé de chiffrement*). Le *déchiffrement* est le traitement des données qui retransforme le texte chiffré en texte en clair. La *cryptographie* est la science qui consiste à créer de tels systèmes de chiffrement. La *cryptanalyse* est la science complémentaire qui consiste à déterminer certaines propriétés de ces systèmes dans le but de reconstituer le texte en clair, souvent en l'absence des paramètres qui sont nécessaires pour le déchiffrement. La *cryptologie* englobe la *cryptographie* et la *cryptanalyse*. Le chiffrement est généralement accompli avec un algorithme bien défini et une *clé*. Ceci s'applique aussi au déchiffrement bien que les algorithmes ne soient pas nécessairement les mêmes pour ces deux étapes.

Prenons un exemple : supposons que l'on désire transmettre le nombre 521 de façon sécuritaire. Supposons aussi que le destinataire et l'expéditeur partagent une clé secrète, disons 122, et un système de chiffrement qui consiste en l'addition du texte en clair (521) et de la clé (122). Dans ce cas-ci, le chiffrement donne 643. Puisque le destinataire connait la clé (122) et la méthode de chiffrement (addition), il ou elle peut déchiffrer le message reçu en appliquant l'opération inverse, c'est-à-dire en soustrayant 122 de 643 pour aboutir au texte en clair : 521. Une personne qui intercepterait le texte chiffré éprouverait beaucoup de difficultés à effectuer le déchiffrement sans la clé, même en connaissant la méthode de chiffrement.

UN APERÇU DE *l'histoire de la cryptologie*

SYSTÈMES MANUELS

Par *système manuel*, on entend habituellement les méthodes cryptographiques qui requièrent simplement du papier et un crayon. Il n'est pas surprenant que ces systèmes soient les plus anciens.

Système de chiffrement de César

L'un des premiers systèmes de chiffrement fut probablement celui utilisé par Jules César il y a environ 2000 ans. Le principe appliqué consistait à remplacer chaque lettre de l'alphabet par celle située trois places plus loin dans l'ordre alphabétique. S'il fallait dépasser la lettre Z, on revenait à la lettre A. Ce système est un exemple de substitution car chaque lettre est toujours remplacée par une même lettre. L'alphabet de susbstitution utilisé par le système de chiffrement de César est indiqué ci-dessous.

```
Alphabet :       ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution :   DEFGHIJKLMNOPQRSTUVWXYZABC
```

Si l'on applique ce système, le texte **MA PETITE VACHE A MAL AUX PATTES** devient **PD SHWLWH YDFKH D PDO DXA SDWWHV**, ce qui peut être représenté sous forme continue comme **PDSHWLWHYDFKHDPDODXASDWWHV** pour plus de confidentialité. Dans certains cas, les lettres chiffrées peuvent être regroupées en blocs de 5 caractères. Si l'on procédait de la sorte, on obtiendrait : **PDSHW LWHYD FKHDP DODXA SDWWH V**.

Substitutions, permutations et transpositions

Le système de chiffrement de César offre un exemple de substitution mono-alphabétique où les lettres sont remplacées de façon précise. Évidemment, il n'est pas nécessaire de remplacer toutes les lettres comme l'a fait César. Par exemple, on peut utiliser la table de substitution suivante :

```
Alphabet :       ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution :   QWERTYUIOPASDFGHJKLZXCVBNM
```

Si on chiffrait le message **SOYEZ AUX AGUETS** avec cet alphabet, on obtiendrait le résultat suivant : **LGNTM QXB QUXTZL**.

Il est préférable que le texte chiffré soit transmis sans espaces entre les mots, car ceci peut donner un indice à l'intercepteur. Quand la langue utilisée est connue, une substitution peut souvent être résolue en employant l'analyse des fréquences et en cherchant des mots-clés. Par exemple, si l'on considère la langue française, la lettre la plus commune est **E**. D'autres lettres très communes sont **A, S, N, T, I, R, U, L, O** et **D**, ces lettres étant indiquées plus ou moins en ordre de fréquence décroissante. Les fréquences varient selon le contenu du texte de base, et donc l'ordre des lettres les plus fréquentes peut changer. Si les espaces entre les mots sont conservés dans la représentation chiffrée, cela

favorise l'analyse des mots comportant peu de lettres. Ainsi, il n'existe qu'un seul mot d'une lettre, soit **A,** et peu de mots de 2 lettres. Si la ponctuation est conservée, il s'agit encore d'un avantage pour la cryptanalyse. On peut déduire plusieurs observations utiles de ce genre du texte chiffré suivant :

RZ QYONJTCYZNDES SMJ RZ MQESGQS HUE QTGMEMJS Z
QYSSY XSM MOMJSBSM XS QDEWWYSBSGJ.

En premier lieu, on remarque que la lettre la plus fréquente dans le texte chiffré est le **S**, que l'on suppose représenter **E**. **M** est aussi très fréquente, et le mot **SMJ** suggère le mot **EST**. Les mots **RZ** et **Z** correspondent probablement à **LA** et **A**. Cette analyse donne le résultat suivant :

LA ****T*A***E EST LA S**E**E ***
***S*STE A **EE* *ES S*STE*ES *E ******E*E*T**.

On complète alors le mot **SYSTEMES**, puis le groupe de lettres **EMENT**, et finalement le mot **SCIENCE**, ce qui donne :

LA C*Y*T*A**IE EST LA SCIENCE **I C*NSISTE**
A C*EE* *ES SYSTEMES *E C*I*EMENT.**

Puis, on compl te les mots **CONSISTE** et **CREER**, ce qui fait appara tre **CRY*TO*RA**IE**, soit **CRYPTOGRAPHIE**. On peut alors compl ter le d chiffrement :

LA CRYPTOGRAPHIE EST LA SCIENCE QUI CONSISTE A CREER
DES SYSTEMES DE CHIFFREMENT.

Voici donc le résultat obtenu :

```
Alphabet :        ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution :    Z QXSWCDE  RBGTNHYMJU   O
```

Est-il possible de compléter la substitution? Si vous utilisez une machine à écrire ou un ordinateur, la réponse vous viendra après quelques secondes de réflexion.

Une substitution basée sur l'alphabet du texte conserve la position de chaque lettre. Par contre, une *permutation* des lettres qui forment le texte en clair change l'ordre (mais pas l'*identité*) des lettres et constitue une autre méthode de chiffrement. Ces permutations s'appliquent à des blocs de texte en clair. Si nécessaire, des lettres sont ajoutées afin de compléter le bloc. Par exemple, prenons la permutation suivante sur blocs de cinq lettres :

```
Position originale dans le bloc de texte en clair :  12345
Nouvelle position dans le bloc de texte chiffré :    42135
```

Voici un exemple de chiffrement utilisant la permutation ci-dessus pour des blocs de cinq lettres et la lettre **X** pour compléter le dernier bloc :

```
Texte en clair :                              NAPOLEON ET JOSEPHINE
Texte en clair en blocs de 5 lettres :        NAPOL EONET JOSEP HINEX
Texte chiffré(permuté) en blocs de
5 lettres :                                   OANPL EOENT EOJSP EIHNX
Texte chiffré final :                         OANPLEOENTEOJSPEIHNX
```

Une autre forme de changement d'ordre est une *transposition*. En utilisant le même texte en clair que ci-haut, on construit une table où les espaces sont supprimés et où chaque ligne est de longueur n. Le texte chiffré est lu colonne par colonne. Voici un exemple élaboré avec n=6 à partir du texte en clair de l'exemple ci-haut :

N A P O L E
O N E T J O
S E P H I N
E X X X X X

Le texte chiffré est obtenu à partir des colonnes, et donne **NOSEANEXPEPXOTHXLJIX-EONX**. Il existe plusieurs variations, parfois très complexes, des méthodes décrites ci-haut. Il est aussi possible de combiner plusieurs méthodes de chiffrement pour améliorer la sécurité du système et le rendre beaucoup moins vulnérable à la cryptanalyse.

Méthode de Porta

Ce système fut mis au point en 1563 par l'Italien Giovanni Battista da Porta. Sa méthode est décrite au moyen de la table 1 ci-dessous. Elle nécessite un *mot-clé* dont les lettres forment les *lettres-clés*. La première colonne (contenant des paires de lettres en caractère gras) contient la composante du mot-clé. La rangée du haut, aussi indiquée en caractère gras, contient la composante primaire du texte en clair. Leur association permet une substitution réciproque pour une lettre-clé particulière. Supposons une lettre-clé. Si la lettre du texte en clair figure dans la rangée du haut, on lui substitue la lettre qui apparaît à l'intersection de la colonne où se trouve la lettre en clair et de la rangée où se trouve la lettre-clé. Si la lettre du texte en clair n'est pas affichée dans la rangée du haut, on la cherche dans la rangée où se trouve la lettre-clé et on lui substitue la lettre correspondante.

	a	b	c	d	e	f	g	h	i	j	k	l	m
AB	n	o	p	q	r	s	t	u	v	w	x	y	z
CD	z	n	o	p	q	r	s	t	u	v	w	x	y
EF	y	z	n	o	p	q	r	s	t	u	v	w	x
GH	x	y	z	n	o	p	q	r	s	t	u	v	w
IJ	w	x	y	z	n	o	p	q	r	s	t	u	v
KL	v	w	x	y	z	n	o	p	q	r	s	t	u
MN	u	v	w	x	y	z	n	o	p	q	r	s	t
OP	t	u	v	w	x	y	z	n	o	p	q	r	s
QR	s	t	u	v	w	x	y	z	n	o	p	q	r
ST	r	s	t	u	v	w	x	y	z	n	o	p	q
UV	q	r	s	t	u	v	w	x	y	z	n	o	p
WX	p	q	r	s	t	u	v	w	x	y	z	n	o
YZ	o	p	q	r	s	t	u	v	w	x	y	z	n

Table 1. La table de Porta

Chiffrons **BATAILLEDEMAINMATIN** en utilisant comme mot-clé le mot **SECRET**. La première lettre-clé est **S** et donc la rangée qui nous concerne est :

	a	b	c	d	e	f	g	h	i	j	k	l	m
ST	r	s	t	u	v	w	x	y	z	n	o	p	q

La première lettre du texte en clair est **B** et donc la lettre chiffrée est **S**. La deuxième lettre-clé est **E** et on regarde donc les deux rangées suivantes :

	a	b	c	d	e	f	g	h	i	j	k	l	m
EF	y	z	n	o	p	q	r	s	t	u	v	w	x

La deuxième lettre du texte en clair est **A** et donc la lettre chiffrée est **Y**. La troisième lettre-clé est **C** et on isole les deux rangées suivantes :

	a	b	c	d	e	f	g	h	i	j	k	l	m
CD	z	n	o	p	q	r	s	t	u	v	w	x	y

La troisième lettre du texte en clair est **T** et il s'en suit que la lettre chiffrée est **H**. Le chiffrement complet donne lieu au texte chiffré suivant (en notant que les lettres du mot-clé sont répétées autant de fois que nécessaire) :

```
Mot clé :          SECRETSECRETSECRETS
Texte en clair :   BATAILLEDEMAINMATIN
Texte chiffré :    SYHSTPPPPWXRZCYSIZJ
```

Méthode de Vigenère

Cette méthode de chiffrement est le fruit du travail de Blaise de Vigenère, un Français ayant vécu de 1523 à 1596. Il semble qu'elle fut mise au point par Vigenère lors de ses visites au Vatican. Le principe à la base de cette méthode consiste à utiliser une différente substitution alphabétique à chaque position, ce qui rend l'analyse des fréquences un peu moins attrayante. Un mot- clé est utilisé et écrit à maintes reprises au haut du texte en clair tout comme dans la méthode de Porta. Dans l'exemple qui suit, le mot-clé est **MONTREAL**. Pour chiffrer, on choisit la rangée de la table 2 ci-dessous qui correspond à la lettre appropriée du mot-clé et on opère une substitution alphabétique avec la lettre située à l'intersection de la colonne correspondant à celle-ci et de la rangée correspondant à la lettre du texte en clair. Le chiffrement du texte en clair s'effectue donc par autant de substitutions différentes qu'il y a de lettres dans le mot-clé.

```
Mot clé :          MONTREALMONTREALMO
Texte en clair :   CHARDASSAUTADROITE
Texte chiffré :    OVNKUESDMIGTUVOTFS
```

Pour cette méthode, le destinataire doit connaître le mot-clé et la table de chiffrement. Cette table peut être aussi simple que celle présentée ci-dessous. Le déchiffrement est accompli en procédant à l'inverse, tout simplement.

	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

Table 2 : Table de type Vigen re

Méthode de Playfair

Ce système fut inventé par Charles Wheatstone, un professeur de philosophie au King's College de Londres, en Angleterre. Ce système reçut son nom en 1854 lorsque Lyon Playfair, baron de St. Andrews, présenta la méthode lors d'un banquet. Le chiffrement de Playfair fut utilisé par les Britanniques pendant la guerre des Boers et la Première Guerre mondiale.

Voici une version simplifiée de cette méthode de chiffrement :

- Remplir une table de dimension 5 par 5 avec des lettres de l'alphabet en groupant deux des 26 lettres. Ceci peut être accompli avec un mot-clé en inscrivant consécutivement dans la table la première apparition de chaque lettre du mot-clé suivie des autres lettres

de l'alphabet. La table 3 est construite à partir du mot-clé **VANCOUVER** et en groupant **I** et **J**.

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

Table 3 : Une table de type Playfair

- Écrire le texte en clair par groupes de deux lettres. Si une paire contient la même lettre deux fois, on ajoute une *lettre complémentaire* (comme le **X**) entre les deux. Par exemple, **MISSION EN VIGUEUR** s'écrit comme suit **MI SX SI ON EN VI GU EU RX**. La lettre complémentaire est **X** et est utilisée à deux occasions, la deuxième fois pour compléter la dernière paire du message.
- Pour chaque paire de lettres, la table 3 est utilisée comme suit :
  - si les lettres sont dans la même colonne, chacune des deux est remplacée par la lettre située immédiatement en dessous; si une lettre est au bas de la colonne, elle est remplacée par celle se trouvant au haut de la colonne;
  - si les lettres sont dans la même rangée, chacune est remplacée par la lettre située immédiatement à sa droite; si l'une des lettres est la dernière de la rangée, elle est remplacée par la première de la même rangée;
  - si les deux lettres ne se trouvent ni dans la même rangée, ni dans la même colonne, elles sont remplacées comme suit : la première lettre chiffrée est obtenue en prenant la lettre située à l'intersection de la rangée contenant la première lettre du texte en clair et de la colonne comprenant la seconde lettre du texte en clair; la deuxième lettre chiffrée est obtenue en prenant l'intersection de la colonne contenant la première lettre du texte en clair et de la rangée contenant la deuxième lettre du texte en clair.

Les étapes du chiffrement du texte en clair de l'exemple ci-haut sont présentées dans le tableau ci-dessous. Le texte chiffré est ensuite écrit en une séquence continue de lettres : **QGPZQKVCRACFFEREHN**.

Texte en clair	Cas	Texte chiffré
MI	Diff rentes rang e et colonne	QG
SX	Diff rentes rang e et colonne	PZ
SI	Diff rentes rang e et colonne	QK
ON	M me rang e	VC
EN	Diff rentes rang e et colonne	RA
VI	Diff rentes rang e et colonne	CF
GU	Diff rentes rang e et colonne	FE
EU	M me rang e	RE
RX	M me colonne	HN

Autres méthodes

Les méthodes de chiffrement décrites jusqu'à maintenant sont telles que le texte en clair est combiné avec une clé secrète selon un algorithme spécifique pour produire le texte chiffré. Il existe toutefois plusieurs autres façons de transmettre secrètement un message : à vrai dire, celles-ci ne font pas nécessairement partie du domaine de la cryptologie. Par exemple, on peut utiliser de l'encre invisible sur certains types de papier. Le papier peut alors être chauffé ou traité avec des produits chimiques afin d'exposer le message secret. Une autre méthode est la miniaturisation de la représentation physique de l'information : on pense aux micro-points et aux microfilms, par exemple. Le chiffrement n'est donc pas la seule façon sécuritaire de transmettre un message secret, mais il est pratique et facile à utiliser, ce qui explique sa popularité.

SYSTÈMES MÉCANIQUES

Les systèmes manuels sont souvent lents et laborieux pour l'usager puisque fondés sur l'emploi de papier et crayons. De plus, ils ne permettent pas l'utilisation d'algorithmes compliqués. Des méthodes de chiffrement plus rigoureuses et complexes utilisant des appareils mécaniques ont donc été mises au point. La section qui suit offre un bref aperçu des plus célèbres de ces machines à chiffrer mécaniques.

Appareils à disques codeurs

Le premier appareil à disque codeur fut inventé par Léon Battista Alberti au 15e siècle. Il était formé de deux disques concentriques en cuivre, l'un de ces disques étant grand et fixe, et l'autre plus petit et mobile. Ces disques étaient divisés en 24 parties radiales égales. Le disque extérieur contenait les lettres du texte en clair dans l'ordre suivant :

{ A,B,C,D,E,F,G,I,L,M,N,O,P,Q,R,S,T,V,X,Z,1,2,3,4 },

c'est-à-dire un nombre suffisant de lettres de l'alphabet pour former la majorité des mots latins. De plus, le disque intérieur contenait la permutation suivante de l'alphabet latin :

{ m, r, d, l, g, a, z, e, n, b, o, s, f, c, h, t, y, q, i, x, k, v, p, et }.

Ce mécanisme, quoique assez simple en lui-même, illustre l'ingéniosité d'Alberti, qui combine pour la première fois une substitution dite polyaphabétique et l'usage d'un code. Le lecteur intéressé peut consulter la référence [1] pour obtenir une description plus détaillée des travaux d'Alberti.

Un autre exemple classique d'appareil à disque codeur est fourni par le «Confederate Cipher Disk», fabriqué en laiton. Cet appareil contient aussi des disques intérieur et extérieur, portant tous les deux les lettres en ordre alphabétique. L'idée première était d'utiliser ce mécanisme pour la méthode de Vigenère. Un appareil à disques codeurs (à construire) est fourni au centre de la brochure.

Le cylindre à roues codeuses CSP-488

Le cylindre à roues codeuses M-94/CSP-488

En 1922, l'armée américaine fit fabriquer le M-94, un appareil cylindrique comportant 25 anneaux (de diamètre d'environ 4 cm) en aluminium sur un pivot d'environ 10,5 cm de long. Ce mécanisme demeura en service jusqu'au début de la Deuxième Guerre mondiale. Il fut aussi utilisé par la garde côtière et la «Federal Communications Commission» des États-Unis. La marine américaine avait une version semblable dans la CSP-488.

L'appareil KRYHA

L'appareil KRYHA

Cet appareil apparu pour la première fois durant les années 1920. Son inventeur fut l'Ukrainien Alexandre Von Kryha. Cet appareil avait un demi-cercle fixe de lettres contre lequel était juxtaposé un disque codeur pourvu d'engrenages contrôlant le nombre de décalages du disque. Une manivelle servait à remonter un puissant ressort d'horlogerie qui entraînait la plate-forme sur laquelle était installée le disque codeur intérieur. La clé consistait en une autre roue dont les segments (ouverts ou fermés) contrôlaient la rotation du disque codeur intérieur. Malgré sa belle apparence et sa petite taille, cet appareil accomplissait essentiellement l'équivalent d'une substitution avec un cycle de chiffrement, dont la période n'était que de quelques centaines de caractères. Des cryptanalystes américains ont démontré que cet appareil était exploitable en quelques heures.

Le convertisseur M-209 de Hagelin

Fabriqué par Boris Hagelin au début des années 1940 pour l'armée américaine, le M-209 était un appareil mécanique simple mesurant 18 cm de large par 14 cm de profond et 9 cm de haut. Il pouvait être rangé dans un sac de toile vert et pesait environ 4 kilogrammes. Ses composantes principales incluaient six roues codeuses à 26, 25, 23, 21, 19 et 17 positions respectivement, assurant une longueur de cycle (c'est-à-dire le nombre d'étapes avant qu'une clé donnée se répète) de 101 405 850 pas. Pour manipuler cet appareil, l'utilisateur devait tourner le bouton externe (situé à gauche) afin de choisir la lettre du texte en clair, puis tourner ensuite la manivelle située à droite afin d'activer les composantes internes. Vers la fin de la révolution de cette manivelle, l'appareil imprimait la lettre chiffrée sur une bande-papier. Pendant la Deuxième Guerre mondiale, plus de 140 000 unités de cet appareil furent fabriquées, principalement par la firme «Smith Corona Typewriter» aux États-Unis.

L'appareil M-209B Hagelin

UN APERÇU DE *l'histoire de la cryptologie*

SYSTÈMES ELECTRO-MÉCANIQUES

Des machines à chiffrement assez complexes et efficaces fonctionnant notamment avec des piles comme source d'énergie furent mises au point au 20e siècle. Plusieurs furent utilisées pendant la Deuxième Guerre mondiale, dont la plus connue fut l'Enigma.

Enigma à 3 roues codeuses

Enigma à 4 roues codeuses

La machine ENIGMA

Ayant pour origine des brevets de 1919 d'Alexandre Koch et des brevets d'Arthur Scherbius durant les années 1920, l'Enigma fut produite en version commerciale en 3 modèles : A, B et C. Le modèle C était un appareil qui n'avait pas d'imprimante, mais plutôt un mécanisme qui illuminait les lettres chiffrées. Tous les modèles possédaient un clavier. Pendant les années 1930, l'Allemagne se réarmait et fit l'acquisition de la compagnie Enigma. Une version à trois roues codeuses de l'Enigma fut jugée adéquate en termes de sécurité. Pendant la Deuxième Guerre mondiale, cette Enigma portative à lampes (de grandeur et de poids similaires à ceux d'une machine à écrire) alimentée par une pile et logée dans une boîte en chêne servit l'armée (*Armee)*, la marine (*Kriegsmarine*), et les forces aériennes (*Luftwaffe*) allemandes.

L'Enigma différait par deux aspects importants des machines à roues codeuses précédentes. La dernière roue codeuse entrait en contact avec un tambour final (qui pouvait être considéré comme une roue codeuse en soi) qui avait 26 boutons de contact sur une seule face, ces boutons étant reliés l'un à l'autre par 13 fils internes. Ceci rendait le chiffrement réciproque, c'est-à-dire que $E(E(x)) = x$ mais avec la condition importante que $E(x) \neq x$ pour tout caractère x de l'alphabet où E est la fonction de chiffrement. Ce chiffrement réciproque permettait le déchiffrement avec la même configuration initiale que le chiffrement, à cette exception près que dans ce cas, c'étaient les lettres chiffrées qui étaient insérées au clavier, et donc les lettres déchiffrées qui étaient illuminées par les lampes respectives. L'autre aspect important était la présence d'engrenages qui assuraient un mouvement irrégulier des roues codeuses.

Les premières versions de la machine Enigma fonctionnaient avec trois roues codeuses comportant chacune, des deux côtés, 26 boutons conducteurs liés par 26 fils intérieurs suivant une permutation secrète. Les trois roues étaient choisies parmi cinq roues possibles (généralement nommées I, II, III, IV et V) et étaient insérées dans la machine suivant un ordre donné et secret. Chaque roue codeuse possédait un anneau pourvu d'une coche qui devait être placée à l'une des 26 positions possibles. Cette coche servait à entraîner la roue codeuse située immédiatement à gauche. La première roue codeuse (soit celle située tout-à-fait à droite) se déplaçait d'une position à chaque lettre tapée, tandis que la deuxième se déplaçait en moyenne d'une position toutes les 26 lettres tapées, et la troisième (située à gauche) d'une position toutes les 676 lettres tapées. La machine était aussi pourvue, sur sa face verticale, d'un système de brouillage se présentant sous la forme

d'un tableau de connexions comportant 26 prises où l'on introduisait habituellement 10 fiches à double contact (le maximum étant 13 fiches). Ces 26 prises étaient identifiées par les 26 lettres de l'alphabet.

Pour chaque message, lorsque l'opérateur tapait une lettre sur le clavier, le courant électrique parcourait le trajet suivant : de la lettre tapée, il se rendait au système de brouillage, et suivait ensuite les roues codeuses de droite à gauche jusqu'au tambour, puis retraversait les roues codeuses en sens inverse (selon un trajet différent de celui l'ayant amené au tambour) avant de passer par le système de brouillage pour aller allumer une lettre sur le panneau destiné à cet effet.

Des valeurs secrètes, définies quotidiennement, servaient à établir les paramètres initiaux suivants : a) choix et ordre des roues codeuses à insérer de gauche à droite dans la machine; b) positions (ringstellung) des anneaux des trois roues codeuses; c) paires de fiches (au nombre de 10) à brancher dans le système de brouillage (p. ex. EB aurait signifié qu'il fallait accoupler les prises E et B). L'opérateur de l'appareil devait choisir aléatoirement trois lettres, qui deviendraient les positions de départ des roues. Ces trois lettres étaient ensuite chiffrées et transmises au destinataire, qui devait alors les déchiffrer pour définir les mêmes paramètres pour son appareil, de manière à ce que les machines soient synchronisées. Au cours de la Deuxième Guerre mondiale, diverses procédures furent employées pour chiffrer ces trois valeurs secrètes. Le lecteur intéressé à en savoir davantage peut consulter le chapitre 11 de la référence [2]. Un désavantage de l'Enigma était qu'elle n'imprimait pas les résultats, et donc que son utilisation nécessitait trois personnes : une pour lire le texte reçu et manipuler le clavier, une pour énoncer d'une voix forte chaque lettre illuminée et une autre pour rédiger le texte.

En février 1942, la marine allemande fit modifier ses machines Enigma en y ajoutant une quatrième roue codeuse (tout en réduisant la largeur du tambour) et en ajoutant une deuxième coche sur les anneaux de certaines roues codeuses. Ceci donna un nouvel essor à la cryptanalyse à Bletchley Park, près de Londres en Angleterre. Pendant les années menant à la Deuxième Guerre mondiale, trois mathématiciens polonais (Rejewski, Rozycki et Zygalski) avaient accompli du travail tout-à-fait remarquable, dans le domaine de la cryptanalyse, concernant l'Enigma et la façon dont elle pouvait être exploitée. Quand les hostilités ont été déclarées et que des modifications ont commencé à être apportées à l'Enigma, notamment par l'ajout d'un système de brouillage et l'introduction d'une modalité consistant à choisir 3 roues codeuses sur une réserve de 5, les Polonais ont cédé les résultats de leurs recherches aux Britanniques, qui ont grandement bénéficié de cette information. Pendant la Deuxième Guerre mondiale, les Britanniques avaient saisi des machines Enigma à trois et quatre roues codeuses ainsi que des listes de clés quotidiennes, ce qui leur avait permis de mettre au point les fameuses *Bombes*. Ces machines gigan-

Roues codeuses pour l'Enigma

tesques essayaient systématiquement les 60 combinaisons de trois roues codeuses (choisies parmi cinq roues possibles) ainsi que toutes les positions de départ possibles afin de décrypter un message. L'information amassée grâce aux succès de la cryptanalyse de l'Enigma tombait sous le nom de code **ULTRA.** Il y avait d'autres appareils cryptographiques allemands, tels que la famille *Geheimschreiber,* et notamment TUNNY dont les messages chiffrés pouvaient être exploités par *Colossus,* une autre machine monstre construite à Bletchley Park. Le lecteur intéressé à en apprendre davantage peut consulter les références [2], [3], [4], [5], [6], [7], [8] et [17]. Par ailleurs, d'autres détails sur Bletchley Park peuvent être obtenus sur l'internet, notamment sur les sites Web indiqués à la fin de cette brochure.

Les machines de Hebern

En 1910, Edward H. Hebern commença à mettre au point des machines de chiffrement aux États-Unis. Au début des années 1920, il inventa la machine à *code électrique* qui utilisait une seule roue codeuse. Il conçut aussi, en 1924, des appareils à trois et cinq roues codeuses comme prototypes pour la marine américaine. Très différentes de l'Enigma, les machines de Hebern utilisaient des roues codeuses dont le filage interne pouvait facilement être changé. De plus, ces roues codeuses pouvaient fonctionner dans le sens de rotation conventionnel ou dans le sens contraire. Par contre, ces machines possédaient toutes des faiblesses du point de vue cryptanalytique. Ces faiblesses sont décrites par William Friedman dans la référence [9].

Une machine SIGABA

Les machines TYPEX et SIGABA

À la suite d'une longue étude (1926-1935) portant sur les machines de chiffrement commerciales commes les machines Hebern, Kryha et Enigma, un comité interministériel britannique adopta une machine semblable à l'Enigma appelée Typex. Le modèle Mark III de Typex avait cinq roues codeuses interchangeables dotées d'un mouvement irrégulier. Cet appareil électrique était lourd et imprimait le texte chiffré sur bande-papier, l'imprimante étant située à l'arrière de la machine. Plusieurs versions de la Typex furent utilisées par l'armée britannique et la RAF. Le Canada en fit aussi l'emploi, surtout au sein du ministère de la Défense. La référence [3] offre davantage de précisions à ce sujet.

Juste avant 1940, l'armée et la marine américaines adoptèrent une machine similaire appelée ECM Mark II où ECM signifiait «*Electric Cipher Machine*». L'armée américaine lui donna le nom de Sigaba. Seuls les Américains utilisèrent cette machine, notamment pendant la Deuxième Guerre mondiale et par la suite.

Afin que l'on puisse échanger des messages chiffrés entre la Typex et l'ECM, on conçut pour cette dernière une cage spéciale à roues codeuses compatible avec la Typex. Equipée de cette façon, l'ECM était appelée la CCM, ce qui signifiait «*Combined Cipher Machine*». Que l'on sache, aucun appareil semblable n'a été fabriqué pour rendre la Typex compatible avec l'ECM.

La machine NEMA

La NEMA (*NEue MAchine*) fut mise en service en 1947 par la firme Zellwager A.G. en Suisse. Sa conception avait débuté en 1941 et deux prototypes avaient été fabriqués en 1944 pour le compte de l'Office du chiffre de l'armée suisse. La NEMA partageait plusieurs caractéristiques de l'ENIGMA telles qu'un réflecteur en plus de ses 10 roues codeuses. Par contre, elle permettait un mouvement beaucoup plus irrégulier des roues codeuses ainsi que du réflecteur. Cinq des roues codeuses, appelées *Fortschaltwalzen*, contrôlaient le mouvement des cinq autres. Celle située la plus à droite était rouge tandis que les neuf autres étaient noires. La NEMA avait une alimentation externe ajustable (soit 110v, 220v, etc.), un adapteur pour une prise d'ampoule et un panneau lumineux amovible pour en faciliter l'emploi. Les premiers utilisateurs de la NEMA furent l'armée et le service diplomatique suisses. Les deux modèles étaient identiques à part leurs roues codeuses.

Une machine NEMA

MÉTHODES MODERNES

Avec la prolifération des ordinateurs et l'essor de leur connectivité, plusieurs méthodes cryptographiques utilisent maintenant des logiciels plutôt que des machines électro-mécaniques. Bien plus, bon nombre de logiciels commerciaux intègrent maintenant des méthodes de chiffrement pour offrir plus de sécurité. La majorité de ces méthodes requièrent des connaissances mathématiques trop complexes pour être présentées dans cette brochure. Un certain nombre de concepts plus avancés sont exposés dans les références [10] et [12].

JEU-QUESTIONNAIRE

1. Révision :
   - Cet empereur romain inventa et utilisa l'un des premiers systèmes de chiffrement.
   - Ce système de chiffrement mécanique fut utilisé par la marine, l'aviation et l'armée allemandes durant la Seconde Guerre mondiale.
   - Il fut l'inventeur du système de chiffrement Playfair.
   - Cette machine à 10 roues codeuses, basée sur l'Enigma, fut utilisée par l'armée suisse après la Seconde Guerre mondiale.
   - Il fabriqua au début des années 1940 la M-209, une machine qui fut utilisée par l'armée américaine.
   - Cette méthode peut être utilisée pour tenter de percer des messages chiffrés par substitution.
   - Ce système fut utilisé par les Britanniques durant la guerre des Boers et la Première Guerre mondiale.
   - Ce terme est utilisé pour décrire des systèmes de chiffrement ne nécessitant que du papier et un crayon.
   - Nom donné à la machine britannique qui permit de déchiffrer de nombreux messages chiffrés au moyen de l'Enigma.
   - Ce Français inventa un système de chiffrement très célèbre pendant qu'il était au Vatican dans les années 1500.
   - Nom donné à l'activité visant à déchiffrer des messages codés sans en être le destinataire.
   - Mécanisme inventé par Leon Battista Alberti au 15e siècle.

2. Soit le chiffrement avec la méthode de César où n=5 au lieu de n=3. Déchiffrez le message suivant :

   RTSUWJRNJWRJXXFLJ!

3. Le texte en clair et le texte chiffré suivants ont été obtenus au moyen de la méthode de César avec un paramètre n. Le texte en clair est :

   RENCONTRE LUNDI

   et le texte chiffré :

   GTCRDCIGTAJCSX.

   Déterminez n.

4. Soit un alphabet ne contenant que 2 symboles {A,B}. Dans ce cas, il y a deux substitutions possibles. Le premier cas est celui où A représente A et B représente B… ce qui

n'est pas très utile! La deuxième substitution s'obtient en remplaçant A par B et vice-versa, ce qui n'est pas tellement plus utile.

- Combien y a-t-il de substitutions possibles en tout avec un alphabet de 3 symboles tel que {A,B,C}? de 4 symboles tel que {A,B,C,D}?
- Combien y a-t-il de substitutions possibles avec un alphabet de 26 symboles? de N symboles?

5. Donnez un exemple de système de chiffrement qui utilise une substitution suivie d'une permutation par blocs. Y a-t-il une différence si la permutation est effectuée en premier lieu? Pourquoi?

6. Déchiffrez la phrase suivante, qui a été chifrée au moyen d'une transposition par colonnes avec n < 11 colonnes :

INLNLSOTYENOAPNUBTETICSXEOEX.

7. Utilisez l'analyse des fréquences pour déchiffrer le message suivant,

OAI QORI PTQYZXEHXAI CRAIXPYHI UA OE DPA IYHX AH VZEHUA QEZXPA UAI QZYNOATAI UA QZYNENPOPXAI,

sachant que :
- les mots sont bien espacés
- le marquis de Laplace, probabiliste célèbre, en est l'auteur
- la voyelle la plus fréquente est le E, suivie du I
- la consonne la plus fréquente est le S, suivie du T
- les lettres C, F, H, J, K, W, X, Y et Z sont absentes.

8. Chiffrez le texte suivant au moyen de la méthode de Vigenère et du mot-code de votre choix :

SEULE UNE PERSONNE QUI RISQUE EST LIBRE.

9. Déchiffrez la phrase suivante, chiffrée avec la méthode de Vigenère et le mot-code **CLEF** :

WEMQKDIENPQTVNSIGKCCY.

10. (PLUS DIFFICILE - PROGRAMMATION) Implémentez la méthode de Vigenère sur ordinateur en utilisant le langage de programmation de votre choix. Le programme doit demander un mot-code à l'utilisateur et assurer le chiffrement et le déchiffrement au moyen de la table de Vigenère à la page 8.

RÉFÉRENCES

Voici, en plus des références indiquées précédemment, une liste d'autres publications qui approfondissent plusieurs sujets abordés dans la brochure. «*The Friedman Legacy*», en particulier, offre un sommaire de plusieurs exposés présentés par William Friedman, qui a été décrit comme «*Le pionnier le plus important dans l'application des principes scientifiques au domaine de la cryptographie*».

La référence [1] constitue une excellente source d'information sur l'histoire de la cryptographie. Elle examine divers sujets dans une perspective historique et fournit de bonnes descriptions techniques.

[1] KAHN, David. *The Codebreakers: History of Secret Communication*, MacMillan Publishing Co., 1967.

[2] HINSLEY, F.H. et Alan STRIPP. *Codebreakers: The Inside Story of Bletchley Park*, Oxford University Press, 1993.

[3] HODGES, Andrew. *Alan Turing: The Enigma*, Touchstone, 1993.

[4] WINTERBOTHAM, Frederick W. *The Ultra Secret*, Dell Publishing, 1974.

[5] CALVOCORESSI, Peter. *Top Secret Ultra*, Pantheon, 1980.

[6] MONTAGU, Ewen. *Beyond Top Secret U*, Readers Union, 1978.

[7] GARLINSKI, Jòzef. *The Enigma War*, Scribners, 1979.

[8] KAHN, David. *Seizing the Enigma*, Houghton Mifflin Co., 1991.

[9] *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*, NSA Publication: Sources in Cryptologic History, nº 3, 1992.

[10] SCHNEIER, Bruce. *Applied Cryptography*, Wiley, 2e édition, 1996.

[11] DEAVOURS, Cipher, David KAHN, Louis KRUH, Greg MELLEN et Brian WINKEL. *Cryptology: Machines, History & Methods*, Artech House, 1989.

[12] STINSON, Doug. *Cryptography, Theory and Practice*, CRC Press, 4e édition, ISBN 0-8493-8521-0, 1996.

[13] LERVILLE, Edmond. *Les cahiers secrets de la cryptographie*, Editions du Rocher, 1972.

[14] SACCO, Général L. *Manuel de cryptographie*, Payot (édition française), 1951

[15] LANGE, André, E.-A. SOUDART. *Traité de cryptographie*, Librairie Félix Alcan, 1935.

[16] GIVIERGE, Général M. *Cours de cryptographie*, Berger-Levrault, 3e édition, 1936.

[17] SINGH, Simon. *The Code Book*, Doubleday, 1999.

[18] BAUDOIN, Roger. *Eléments de cryptographie*, A. Pedone, 1939.

[19] KAHN, David. *La guerre des codes secrets*, InterEditions, 1980.

[20] DE VIGENÈRE, Blaise. *Traité des chiffres*, Guy Trédaniel, 1996 (réimpression de 1586).
[21] SMITH, Michael. *Station X*, Channel 4 Books, 1998.
[22] KIPPENHAM, Rudolf. *Code Breaking*, Overlook Press, 1999.

SITES WEB D'INTÉRÊT

1. Bletchley Park (Angleterre)
   http://www.cranfield.ac.uk/CCC/BPark/
2. National Cryptologic Museum (Fort Meade, Maryland, Etats-Unis)
   http://www.nsa.gov:8080/museum/
3. Musée de l'électronique et des communications militaires (Kingston (Ontario) Canada)
   http://www.c-and-e-museum.org/
4. Centre de la sécurité des télécommunications (Canada)
   http://www.cse-cst.gc.ca/

5 Machines cryptographiques du U.S.S. Pampanito (États-Unis)
http://www.maritime.org/ecm2.shtml

6. Applet Java simulant une Enigma à 3 roues codeuses
   http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/

REMERCIEMENTS

De nombreuses personnes ont participé à la préparation de la présente brochure. Les auteurs souhaitent tout particulièrement remercier :

- leurs collègues du CST qui ont revu le texte et formulé des suggestions;
- Le service des communications visuelles du CST, qui a assuré la conception graphique du document;
- Les Services linguistiques, qui ont révisé la version française du texte;
- le USS Pampanito, qui a fourni la photo du cyclindre à roues codeuses CSP-488;
- le National Cryptologic Museum, qui a fourni la photo de la machine ECM/SIGABA.