Première S

Travaux Personnels Encadrés

Le codage et le cryptage

“ En quoi le codage et le cryptage ont été des facteurs importants d’évolution de la société ? “

Mathématiques et Histoire

Lycée Henri Meck

Année 2018-2019

TPE par Diwisch Mathilda, Durand Yasmina, Krauth Elise et Pichon Sébastien

Sommaire :

Introduction :

75% de la population française utilisent quotidiennement internet en 2018 selon le figaro.fr. 54% de la population mondiale fait de même. Internet est donc devenu essentiel à nos vies. L'informatique et les sciences techniques connaissent un développement exponentiel depuis les années 1980.

Les notions de cryptage ou de codage peuvent paraître compliquées, et pourtant elles sont au cœur de notre société actuelle. Ces notions sont utilisées depuis des siècles pour les échanges d'informations, à des fins militaires ou politiques. Mais aujourd'hui le cryptage est utilisé partout, dans les systèmes informatiques, les puces électroniques ou encore à travers les codes-barres présents sur les produits simples de la vie que nous achetons tous les jours. Mais c'est en période de guerre que le codage de message a été le plus important, notamment durant la Seconde Guerre mondiale où la science se développait avec une rapidité incroyable. Les gouvernements ont alors beaucoup misé pour inventer des systèmes de cryptage de messages confidentiels, et inversement, inventer des systèmes de décryptage de ces messages.

Nous nous demanderons donc en quoi le codage et le cryptage ont été des facteurs importants pour l'évolution de la société. Avant toute chose, nous devons définir le terme de codage et celui de cryptage.

Dans le sens courant, nous pouvons dire que le codage permet de passer d'une représentation des données à une autre. Par exemple, les codes-barres sont l'une des catégories de codage possible. Il est également important de définir la cryptologie. Étymologiquement, ce terme signifie la « science du secret » ce qui représente bien la définition de ce terme. Autrement dit, la cryptologie est l'écriture secrète, soit la cryptographie, ainsi que son analyse appelée la cryptanalyse. La cryptologie est une science et une discipline ancienne puisque l'on trouve ses premières apparitions dans les hiéroglyphes des prêtres égyptiens ou encore dans la Bible. On peut alors dire que la cryptologie est un art ancien, mais une science nouvelle. On explique que c'est une science nouvelle car c'est un thème de recherche scientifique et académique, donc universitaire depuis les années 1970. La cryptographie, qu'est l'écriture secrète, a pour ambition de protéger des messages. Cela en s'assurant de leur confidentialité. L'écriture secrète se fait à base de clés.

Nous verrons dans une première partie les différents types de cryptage qui ont existé au fil du temps, depuis les premières grandes civilisations jusqu'à nos jours, et leurs utilisations. Puis dans une deuxième partie nous étudierons l'un des exemples les plus connus

de l’histoire du cryptage, la machine Enigma, durant la Seconde Guerre mondiale, son fonctionnement et ce qu’elle a engendré dans cette guerre.

I) Le cryptage selon les époques

A) Le cryptage, utilisé depuis l'Antiquité

1) La scytale : un moyen de cryptage ancien

La scytale spartiate, également connue sous le nom de bâton de Plutarque, est un des plus anciens dispositifs de cryptographie militaire connu, remontant au Ve siècle avant JC.

Il est composé d'un bâton de bois où repose une bande de cuir ou de parchemin enroulé. La bande que l'on utilise pour enrouler le bâton de bois est fine, il fallait alors tourner plusieurs fois autour du bâton afin qu'il soit recouvert. Il s'agissait ensuite de noter un message tout en longueur. Chacune des lettres étaient alignées, mais sur une partie différente de la bande en cuir (se référer à la photo pour une compréhension complète). Il fallait ensuite dérouler la bande pour trouver une liste de lettres sans signification. Le message était donc crypté.

Il est assez facile de casser le code de la scytale, car il ne s'agit pas d'une substitution. Une substitution est le processus permettant de remplacer une lettre par une autre. Le cryptage de la scytale est une transposition. Cela signifie que l'on change seulement la position des différentes lettres.

Pour décrypter le message, il faut d'abord compter le nombre de lettres, puis créer des grilles où l'on place toutes les lettres du message crypté dans l'ordre ligne par ligne ou colonne par colonne suivant comment le message se place.

Il existe une autre solution. Si on dispose d'un bâton de même diamètre que celui de la personne qui a crypté le message, il nous suffit d'enrouler à nouveau la bande de lettre pour découvrir le message.

Voici un exemple de la première méthode de décryptage :
Le message crypté est MHENMAI_IACNEG_

M	H	E	N	M
A	I	_	I	A
C	N	E	G	_

Pour crypter un message, on choisit une clé, ici 3, donc la grille aura 3 lignes et le nombre de colonne sera caractérisé par le nombre de caractères. Ici le mot a 15 caractères, il faudra donc un tableau de 3x5 soit 5 colonnes. On voit le message crypté de gauche à droite. Et si l'on veut le décrypter, il faut lire la grille de haut en bas.

Le message crypté est MACHINE ENIGMA.

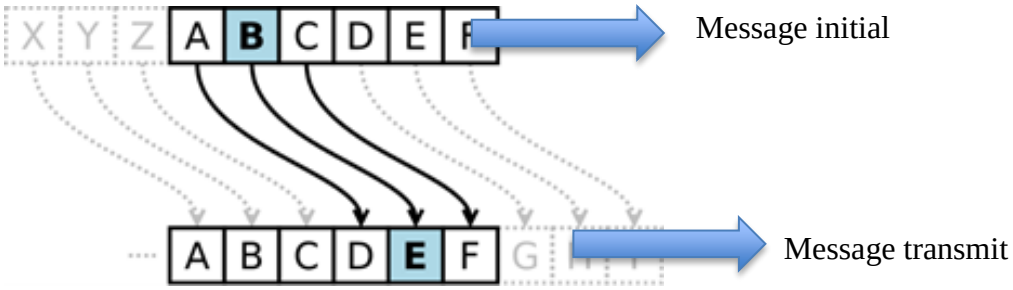
2) Le chiffre de César, un chiffrement par décalage

Un peu plus tard, les avancées scientifiques s'améliorent, on découvre alors le chiffre de César.

Le chiffre César permet de crypter un message de manière simple et rapide. Il tient son nom de Jules César, les historiens lui attribuent l'un des premiers protocoles cryptographiques.

Jules César qui était chef des armées, ne tenait pas à ce que ses ordres soient dévoilés et interceptés et qu'ils soient utilisés par ses ennemis avant même d'arriver sur les lieux de bataille. Dans ses lettres se trouvaient des mots incohérents, qui avaient été cryptés, le lecteur devait donc décrypter le message.

Le chiffre de césar est une méthode de cryptage utilisée depuis de nombreux siècles, il est employé depuis les romains. On parle aujourd'hui d'un protocole de chiffrement. Celui-ci est un simple décalage des lettres de l'alphabet, Il consiste à remplacer une lettre par une autre et de décaler l'alphabet par un nombre ''k''.



Sur le schéma ci-dessus on décale l'alphabet de trois rangs pour crypter le message. Le A devient D, le B devient E, le C devient F, etc. Le nombre k, correspond à la clé pour décrypter un message, pour cet exemple la clé est 3. César aurait envoyé un message contenant cette phrase :

DOHD MDFWD HVW

Si on utilise cette méthode avec comme clé le nombre k égale 3 alors on retrouve la phrase en latin

ALEA JACTA EST

Qui se traduit par « les dés sont jetés ».

Nous ne cessons de parler de chiffrement et de déchiffrement mais nous pouvons aussi décrire mathématiquement ces procédés. Ici nous utilisons le codage des 26 lettres de l'alphabet, en les faisant correspondre avec les entiers de 0 à 25 : le A devient 0, le B devient 1, et ainsi de suite jusqu'au Z qui devient 25.

Démonstration :

ALEA devient alors 0 11 4 0

Pour chiffrer un message on peut donc prendre la fonction :

$$C_k : x \rightarrow x+k$$

Ici pour k=3 $C_3(4) = 4+3 = 7$ $C_3(5) = 5+3 = 8$

Pour déchiffrer un message on prend la fonction :

$$D_k : x \rightarrow x-k$$

Ici pour k=3 $D_3(7) = 7-3 = 4$ $D_3(8) = 8-3 = 5$

On retrouve donc les numéros attribués à chaque lettre initialement et il nous suffit de traduire les numéros par leur lettre attribuée.

Ainsi 4 devient D et 5 devient E

Cette méthode est très peu sûre mais surtout facile à décoder. Si le texte est plutôt long plusieurs mots peuvent revenir dans les phrases comme « le, la, les, et » par exemple. De même la fréquence des lettres est souvent la même dans chaque texte, sachant que le « e » est la lettre la plus utilisée celle-ci revient le plus souvent et est simple à repérer. Nous pouvons par exemple voir avec la phrase :

« LE MESSAGE EST SIMPLE À DÉCRYPTER ».
« OH PHVVDJH HVW VLPSOH D GHFUBSWHU »

Dans cette phrase de six mots la lettre « E » est répétée sept fois. Si le texte est trop court cela est souvent impossible de le décoder à l'aide de cette méthode mais plus le texte est long plus celui-ci est simple à décoder grâce à la fréquence des lettres.

lettre	E	S	A	N	T	I	R	U	L	O	D	C	P
fréquence	17,76	8,23	7,68	7,61	7,30	7,23	6,81	6,05	5,89	5,34	3,60	3,32	3,24
lettre	M	Q	V	G	F	B	H	X	Y	J	Z	K	W
fréquence	2,72	1,34	1,27	1,10	1,6	0,80	0,64	0,54	0,21	0,19	0,07	≈ 0	≈ 0

Voici une table de fréquences d'apparition des lettres dans la langue française. En comparant, avec la fréquence d'apparition des lettres dans un message chiffré suffisamment long, on arrive généralement à le déchiffrer. On peut avoir une analyse plus précise en relevant les lettres doublées, les lettres côte à côte, les lettres en fin de mot… On peut donc se baser sur la structure des mots pour déchiffrer un message.

Aujourd'hui le chiffre de César n'est plus autant utilisé car cette méthode est trop simple à décrypter. Celle-ci est tout de même enseignée aux écoliers. Or les chercheurs ont développé certaines méthodes de cryptage mais aussi de codage en augmentant la fiabilité et la sécurité comme les codes-barres.

B) Le codage, une méthode utilisée quotidiennement

1) Le codage à travers les codes-barres

Les codes-barres ont été inventés par deux étudiants américains, Norman Joseph Woodland et Bernard Silver dans les années 1950.

Le brevet initial a été déposé le 7 octobre 1952. Avant eux les magasins devaient fermer au moins une fois par mois pour faire l'inventaire, les prix étaient saisis à la main et ont comptaient les boîtes. Les codes-barres sont exploités pour la première fois au « Marsh Supermarket de Troy » dans l'Ohio aux Etats-Unis sur un paquet de chewing-gums le 26 juin 1974.

Ils permettent aux entreprises de connaître leurs chiffres de ventes en direct. Les codes-barres aussi appelés les codes à barres sont utilisés dans de nombreux domaines. Cela représente une donnée numérique qui est symbolisée par des barres noires et des espaces. Leur largeur diffère en fonction de la disposition des barres utilisées et des données codées. Comme nous pouvons le voir ci-dessous.

Le code-barres est constitué de plusieurs groupement de chiffres qui définissent chacun une autre donnée. Le ‘’préfixe’’ code le pays d'origine dans lequel le produit a été industrialisé.

<u>Quelques codes de pays :</u>

De 300 à 379 pour la France

De 400 à 440 pour l'Allemagne

De 450 à 459 et de 490 à 499 pour le Japon

De 460 à 469 pour la Russie

De 500 à 509 pour le Royaume-Uni

De 690 à 695 pour la Chine

De 754 à 755 pour le Canada

De 800 à 839 pour l'Italie

Les 4 ou 5 chiffres après le préfixe correspondent au numéro de membre de l'entreprise participant au système EAN, celui-ci est attribué par GS1 France à une entreprise adhérente, en France on compte plus de 32 000 adhérents en 2013. Les 4 ou 5 chiffres suivant eux se réfèrent au numéro d'article du produit et sont attribués par le propriétaire de la marque commerciale. Et enfin le chiffre tout à droite est défini comme une clé de contrôle. Elle permet de confirmer la validité du code-barres par un contrôle, celui-ci est calculé grâce aux douze premiers chiffres.

La formule mathématique pour trouver le dernier chiffre est :

$$M - (X + 3 \times Y)$$

Prenons comme exemple le code-barres présenté page 10.

On lit ce code-barres de droite à gauche

On prend : - pour X la somme des chiffres placés en position paire

-pour Y la somme des chiffres placés en position impaire

- pour M le nombre supérieur à (X +3*Y) divisible par dix

Application :

$X = 6+5+0+6+5+3 = 25$

$y = 0+9+4+2+7+1 = 23$

$X + 3 \times Y = 25 + 3 \times 23 = 94$

Donc $M = 100$

On fait alors $M - (X+3*Y) = 100 - 94 = 6$

La clé de contrôle est cohérente car elle correspond à 6, elle peut également être calculée sur le site: https://www.gs1.fr/Nos-services/Les-Services-Essentiels/Calcul-de-cle-de-controle

Les codes-barres sont omniprésents dans notre société, chaque jour on compte plus de 8 milliards de codes-barres scannés sur la planète entière.

2) Le codage à travers les codes QR (ou codes carrés)

Le flash code aussi appelé le QR (Quick Response) code est un code qui signifie que le contenu du code peut être décodé facilement, c'est un type de police de caractère qui permet de traduire une écriture faite de carrés noirs et blancs. C'est un code-barres à deux dimensions qui a été inventé en 1994 et a été disponible au public à partir de 1999.

A l'origine celui-ci était utilisé pour tracer les pièces automobiles Toyota par l'entreprise Denso-Wave au Japon et se retrouve maintenant sur presque tous nos produits. Une étude américaine récente dit que chaque jour, 2 750 000 américains flashent un code. Les Français eux, sont 89% à le connaître et plus de la moitié à les utiliser.

Effectivement, cette méthode est beaucoup plus efficace que l'URL (une adresse d'un site internet) car pour le flash code, il suffit de scanner le code avec son téléphone mobile grâce à une application alors qu'avec l'URL, nous devons taper précisément chaque lettre avec souvent des caractères spécifiques.

le QR	l'URL
	http://codageenigma.canalblog.com

Nous avons créé notre propre QR code, si vous le flashez à l'aide d'une application, celui-ci vous ramènera à notre blog où se trouve notre TPE en PDF.

Les flash codes ont différents usages : ils peuvent emmener sur un site web, sur un réseau social, sur une vidéo et permet de remplacer l'URL.

Comment le téléphone par exemple, scanne le flash code ?
Un QR Code a la capacité de stocker ses informations horizontalement et verticalement. En effet, la lecture se fera sur 2 axes, un QR Code peut être représenté par une matrice(x,y).

Le QR code à de nombreux avantages :

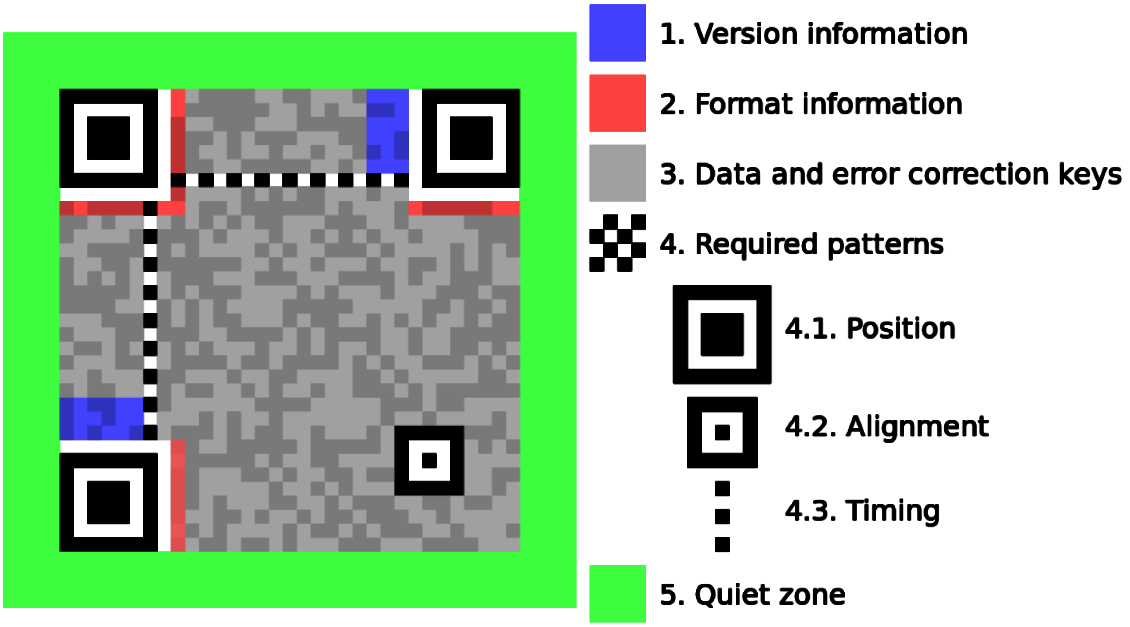
Le 2D (deux dimensions) du flash code permet d'augmenter la capacité de stockage : on peut stocker plus de 7 089 caractères numériques (de 0 à 9), et 4 296 caractères alphanumériques (de A à Z).Il est donc possible de décoder une information de plus de dix caractères en un QR code de 2 cm de côté. Il peut aussi être lu dans tous les sens (360°) et de manière très rapide. Il peut être lu avec seulement 30% de visibilité par le capteur (un téléphone par exemple).

Explication du QR code :

On retrouve sur chaque code des similitudes qui ont chacun des propriétés définies. On les appelle des marqueurs on retrouve en effet :

- trois carrés aux extrémités du code qui sont les marqueurs de position permettant de repérer le QR code dans l'espace ainsi que son orientation notamment grâce au côté droit en bas du code où il n'y a pas de carré ce qui permet de l'identifier (sur l'image ci-dessous = 4.1)
- des carrés qui ont un cadre noir avec un fond blanc et un point noir au centre donnent une approximation générale du code (sur l'image ci-dessous = 4.2)

- et deux lignes qui joignent les carrés des bords où sont alignés et où des pixels noirs et blancs se succèdent permet de simplifier la lecture en donnant une référence (sur l'image ci-dessous = 4.3)



Les flash codes font actuellement partie de nos vies. Il suffit de prêter attention à notre environnement quotidien pour voir des dizaines de flash code différents. Nous pouvons prendre différentes exemples : les affiches de pub, les musées ou sites historiques, les billets de trains, les billets de concerts, les cartes de cantines, les cartes de fidélités, etc.

Grâce à l'application "QR code lecteur", on peut accéder très vite à un grand nombre d'informations. Cette application compte plus de 50 millions de téléchargement.

Les publicitaires utilisent les flash codes afin de rediriger les clients potentiels vers leur page internet pour qu'ils puissent bénéficier d'informations supplémentaires. On peut également relever la présence de QR code sur des affiches visant à donner des informations. Par exemple, dans le village d'Altorf on trouve un panneau avec le nom de l'église et un QR code proposé pour en savoir plus sur ce monument.

Dans certaines villes, les QR codes sont présents sur des tombes et propose une biographie du défunt, on parle alors de QR code funéraire.

Les compagnies de transports utilisent également cette méthode. Nous pouvons citer la SNCF et son application mobile sur laquelle il est possible et très simple d'acheter des billets de train. Une fois l'achat effectué, si vous êtes contrôlés, il vous faudra montrer votre QR code disponible en ligne. Le même dispositif est employé pour les billets de concert par exemple. Notons que les smartphones sont adaptés à la présence de QR code dans leurs applications mobiles car lorsque l'on veut montrer un QR code pour son billet de train par exemple le téléphone augmente automatiquement la luminosité de l'écran pour une meilleur lecture. Il également est possible de payer, de passer un appel, envoyer un mail directement à une personne, participer à un concours (scanner le code pour participer et tenter de gagner un lot), lancer une vidéo YouTube, partager un article sur Facebook, être redirigé vers différentes pages web grâce à un scanne de flash code.

Les réseaux sociaux ont également compris que l'emploi de QR code peut être un gain de temps pour les utilisateurs. Des flash codes sont proposés pour chacun des profils créés sur Instagram, Twitter, Facebook ou encore Snapchat. Notons que snapchat a développé cette stratégie en nommant un QR code simplifié le "snapcode". Si vous prenez une photo du snapcode de votre ami sur Snapchat, on vous propose directement de l'ajouter à vos amis sur l'application. Et cela fonctionne aussi pour tous les autres réseaux sociaux cités au-dessus.

Les QR codes sont donc présents partout autour de nous et nous permettent un gain de temps considérable. Notons qu'il reste une contrainte, celle de posséder une application permettant la lecture des codes sauf pour les réseaux sociaux ou cela se passe en interne.

QR code vers la page Facebook de Coca Cola :

QR code commercial :

QR code pour appeler :

3. Le codage à travers les étiquettes RFID

L'histoire des étiquettes RFID

Les étiquettes à identification par fréquence radio aussi appelé RFID sont nées en 1983. Le créateur de ces étiquettes est Charles Walton. La notion de l'identification par fréquence radio est présente depuis la Première Guerre mondiale. En effet en 1935 Robert Watson-Watt créé une application, utilisée par l'armée britannique, qui va permettre aux Anglais de différencier les avions des alliés avec ceux des ennemis. Ce système est appelé IIF ce qui correspond à « Identify friend or foe ». Celui-ci est encore utilisé de la sorte aujourd'hui pour le trafic aérien.

Avant la naissance des puces et des étiquettes RFID, plusieurs articles ont été écrits. Des années 1940 aux années 1970 l'utilisation de ces systèmes est principalement tournée vers l'usage militaire notamment dans le secteur nucléaire. A la fin des années 1970, ces systèmes se répandent, cette technologie est adoptée dans le secteur privé comme par exemple pour l'identification des locomotives ou encore pour la reconnaissance du bétail en Europe.

Au début des années 1980 les tags passifs font leur apparition, ils permettent de recevoir l'énergie par le signal du lecteur, quelques centimètres suffisent pour la lecture de l'information. Le tag est alors moins cher et supprime la source d'énergie embarquée.

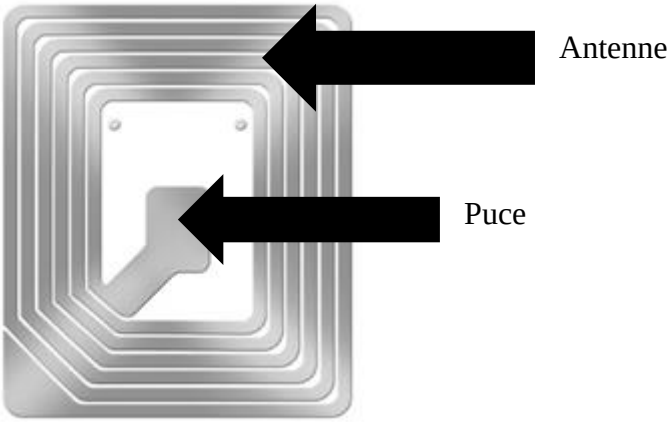
Dans les années 1990 c'est le début de la normalisation pour une interopérabilité des équipements RFID. Le système est aussi miniaturisé ce qui donne lieu à son placement dans une puce électronique par IBM.

En 1999, des industriels créent le centre d'identification automatique au MIT avec l'objectif de standardiser la technologie RFID. Ce centre a été fermé en 2003 lorsque les travaux sur le code produit industriel (EPC) ont été achevés, et les résultats ont été transférés au EPC global Inc. nouvellement fondée par le Uniform Code Council et EAN International (dénommés maintenant GS1 US et GS1).

Depuis 2005, les technologies RFID sont largement répandues dans la majorité des secteurs industriels comme l'aéronautique, l'automobile, la logistique, les transports, la santé et dans la vie quotidienne.

Qu’est-ce qu’une étiquettes RFID ?

Les radios-étiquettes sont des petits autocollants que l’on applique sur un objet ou un produit, il existe aussi de même des puces utilisant le même principe qui sont implantés dans le corps de certains organismes-vivants comme des animaux ou encore sur les humains. Ces petits objets comportent une antenne qui est reliée à une puce électronique qui admet la réception et la réponse aux informations radio émises de l’émetteur au récepteur et inversement.



Elles permettent d’immatriculer un objet ou autre et dans certains cas de stocker des données supplémentaires. Elles peuvent être adoptées pour identifier les objets, elles se nomment alors étiquettes électroniques. Les humains les utilisent en les incorporant dans les passeports, les cartes de crédits et les cartes de transport elles sont alors appelées cartes sans contact, et enfin on peut aussi injecter une puce dans le corps des animaux domestiques comme le chat, on parle alors de puce sous-cutanée.

Comment ça marche ?

Un système de radio-identification combine deux pôles. Pour le fonctionnement de ce système il est essentiel qu’il y ait un marqueur, ce qui correspond à une étiquette, une puce RFID ou encore un tag. Il est aussi indispensable qu’un lecteur RFID soit présent.

Le Lecteur RFID est un émetteur de radiofréquence qui va permettre de détecter la puce qui passe à proximité de celui-ci. Il envoie à une courte distance l'énergie dont les puces RFID ont besoin pour être lues. Les marqueurs peuvent être détectés à une certaine distance, tout dépend du type de puce et de signal radio utilisé.

En effet il existe différentes fréquences, les basses fréquences qui vont jusqu'à 100 à 500 kHz avec une lecture à quelques centimètres, les moyennes fréquences jusqu'à 10 à 15 MHz avec une lecture de 50 à 80 centimètres et enfin les hautes fréquences qui vont de 850/950 MHz à 2,4/5,8 GHz avec une lecture à plusieurs mètres.

L'étiquette est activée à l'aide d'un signal radiofréquence, celui-ci est émis par le lecteur qui est lui-même muni d'une carte électronique et d'une antenne. (L'antenne de ce lecteur peut prendre différentes formes et le lecteur peut lui être fixe ou mobile.) Une fois que l'étiquette reçoit le signal du lecteur elle émet un signal en retour, le lecteur peut ainsi lire les données de la puce. Pour communiquer les étiquettes RFID à basse et à moyenne fréquence adoptent un champ électromagnétique envoyé par l'antenne du lecteur et de l'étiquette. La puce va donc être activée, les programmes qui ont été programmés sont alors activés.

Il existe différents types d'étiquettes, certaines sont passives. Les étiquettes passives fonctionnent en lecture seule (comme les codes à barres linéaires). Dans ce cas, l'antenne capte certaines fréquences qui lui fournissent suffisamment d'énergie pour lui permettre d'émettre à son tour son code d'identification unique. Ces étiquettes passives sont programmées avec des données non modifiables, pour une capacité de 32 à 128 bits.

Elles sont fournies vierges à l'utilisateur. Dans la majorité des cas, le fournisseur l'a déjà munie d'une identification. Lors de sa pose sur l'objet à tracer, l'utilisateur va écrire les données qui lui seront utiles par la suite. Lors de la vie ultérieure de l'étiquette, cette information pourra être lue mais ne pourra être ni modifiée ni complétée. Certains dispositifs plus sophistiqués disposent de capteurs leur permettant d'identifier les variations physiques comme la température (produits surgelés par exemple). Certains tests ont été faits avec une encre magnétique qui joue le rôle de l'antenne.

D’après ces nombreux exemples, on constate que le codage et le cryptage ont une place très importante dans la société. Aujourd’hui on les applique à de nombreux domaines tous très différents. Certains sont plus complexes et plus importants que d’autres. Ce fût le cas également de la machine Enigma qui a eu un rôle déterminant dans le déroulement de la Seconde Guerre mondiale et a eu un impact considérable dans le secteur de l'informatique tel qu’on le connaît aujourd’hui.

II) La machine Enigma, un moyen pour crypter

A. La naissance de la machine Enigma

1. Le contexte de l'invention

La machine Enigma a été développée en 1918 par Arthur Scherbius et Richard Ritter.

Arthur Scherbius:

Richard Ritter:

Les inventeurs sont deux ingénieurs allemands ayant créé une société dans laquelle Arthur Scherbius dirigeait la recherche et le développement en voulant sans cesse innover. Sachant que l'un de ces sujets favoris était celui de remplacer les systèmes dépassés de cryptographie, nous pouvons ajouter qu'Arthur Scherbius a fait ses études en ingénierie à Munich puis à Hanovre. Bien qu'Arthur Scherbius ne s'intéresse pas tout de suite aux codes et aux chiffres, néanmoins, il a créé un nouveau système de chiffrement dès les années 1910. Pour son innovation Arthur Scherbius utilise des rotors désynchronisés. Il conçoit plusieurs modèles et les propose à l'armée allemande. Après plusieurs refus, l'armée de terre allemande opte finalement, en 1926, pour le modèle Enigma-D. Son usage s'étend alors à toute l'organisation militaire allemande. Quelques années plus tard, en 1929, Arthur Scherbius meurt. Il ne verra donc pas la portée intégrale et l'impact de son invention, la machine Enigma.

Les services de renseignements polonais s'intéressent également en secret à la machine Enigma au début des années 30 face à la menace allemande grandissante. Lors de l'invasion de la Pologne par l'Allemagne en 1939, les polonais décident de partager leurs secrets et leur connaissance concernant la machine Enigma avec les Alliés. C'est au Deuxième Bureau qui n'est autre que les services de renseignements français, que les

Polonais partagent leur savoir. Les Français, eux, partagent ce qu'ils ont appris aux britanniques. L'*Intelligence Service* monte alors une équipe chargée de reproduire la machine afin de déchiffrer les messages codés allemand**.**

2. Les premières utilisations de la machine

La machine Enigma, qui rappelons-le, a vu le jour en 1918, a eu de nombreuses utilisations. En effet, la première utilisation de la machine fut commerciale et initialement destinée aux entreprises mais ce fut un échec puisqu'elle était trop chère au goût de celles-ci. Les deux ingénieurs, Arthur Scherbius et Richard Ritter, essayent de vendre cette machine à de nombreuses administrations comme la marine allemande qui s'y intéresse mais finit par refuser, ou encore au ministère des affaires étrangères de la République de Weimar qui aurait pu s'en servir pour chiffrer ses télégrammes diplomatiques, mais qui, lui aussi, va y renoncer. Ils vont alors changer de stratégie et vont essayer de vendre cette machine à des clients potentiels dans le secteur privé et à l'étranger. En 1923, Scherbius et Ritter participent au grand salon suisse de la poste et des communications, mais ils ne vendent que quelques machines sans trouver le client qui fera la différence.

La première version de la machine se nomme : Enigma-A. Elle est en vente dans les années 1920. Mais son prix est très élevé, correspondant à 30 000 euros aujourd'hui. En 1925 l'armée suédoise semble intéressée, Arthur Scherbius et Richard Ritter négocient donc avec les Suédois et finissent par trouver un accord mais celui-ci n'aboutira jamais. La marine de guerre allemande reprend pourtant contact avec eux et va commander cette fois un nombre important de machine. Pendant ce temps Scherbius améliore la machine Enigma.

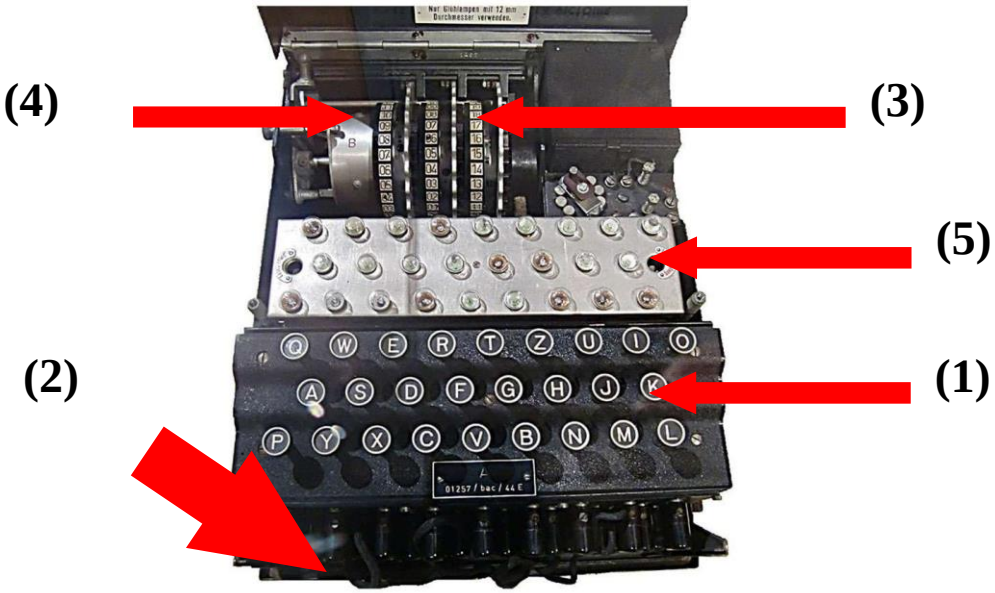
On note trois versions successives de la machine. L'Enigma-D devient le modèle le plus répandu. En effet, cela s'explique car c'est le modèle qui va être employé par les agents de la marine militaire allemande dès 1926. Trois ans plus tard, en 1929, l'armée de terre allemande s'équipe elle aussi de la machine Enigma. Très vite, l'utilisation de la machine s'étend à toute l'armée allemande. La machine Enigma sera alors surnommée « la Machine M » par les allemands. La Wehrmacht améliore la complexité de cette machine afin d'augmenter la sécurité. On constate alors que les premiers usages de la machine étaient commerciaux.

B. Le fonctionnement de la machine Enigma

1. Les composants

La machine Enigma reproduit un chiffrage par substitution poly-alphabétique rendu complexe pour éviter tout décryptement. Nous allons procéder à l'explication du système électromécanique d'une Enigma standard, celle utilisée dans la Wehrmacht (armée allemande). Dans ce modèle, elle est composée :

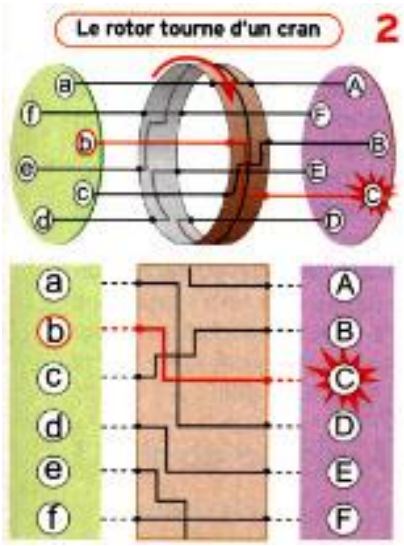
- (1) D'un clavier alphabétique pour taper le message
- (2) D'un tableau de connexion
- (3) De 3 rotors mobiles avec 26 positions chacun. En 1938 les Allemands décident de faire passer le nombre de rotors de 3 à 5, la Pologne ne peut donc plus déchiffrer les messages de son dangereux voisin.
- (4) D'un rotor réflecteur à 26 positions également
- (5) De 26 ampoules : Lorsqu'on appuie sur une touche du clavier, un courant électrique issu du clavier traverse le dispositif de cryptage et allume une diode du tableau lumineux qui correspond à une lettre chiffrée.



2. Coder un message

Le brouilleur : Le brouilleur est l'élément principal de cryptage que l'on retrouve dans la machine Enigma, il est constitué, dans les premières versions, des 3 rotors et du réflecteur.

Les rotors sont des disques de la taille d'un palet de hockey faits d'un matériau isolant. Ils tournent sur un axe et sont composés de 26 contacts électriques sur chaque face, ils sont reliés aléatoirement deux-par-deux par des liaisons électriques à l'intérieur du rotor. Donc chaque contact correspond à une lettre de l'alphabet. Lorsqu'une lettre est tapée, un courant électrique passe par ces 3 rotors et en ressort une lettre cryptée, par exemple si on tape la lettre A, elle ressortira des rotors en une lettre cryptée, par exemple F.
Les rotors constituent donc une substitution mono-alphabétique, il attribue à chaque lettre du clavier une lettre de sortie cryptée.



Voici un schéma simplifié d'un rotor. Après avoir tourné, les liaisons changent.

Mais pourquoi le rotor tourne-t-il ?

Comme l'indique son nom le rotor est fait pour tourner autour de son axe, et à chaque tour, les connexions changent. Si l'on prend le même exemple qu'avant, si la lettre A était relié à la lettre F via le rotor, une fois celui-ci ayant tourné d'un cran, les connexions sont

décalées d'un cran et donc A n'est plus reliée à la lettre F mais à une autre lettre, H par exemple.

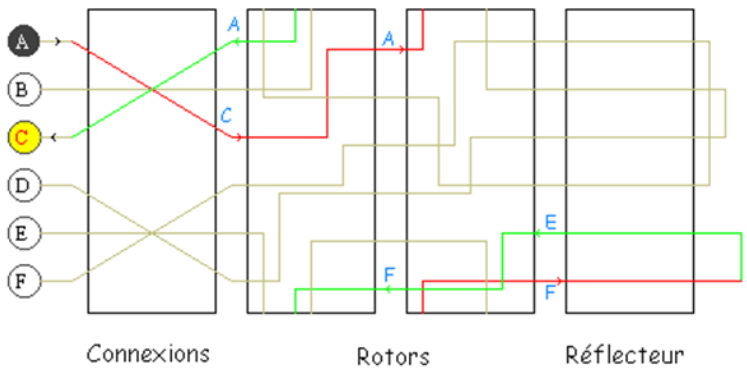
En tournant et changeant de position à chaque lettre, le rotor n'effectue donc plus une substitution mono-alphabétique mais poly-alphabétique.

Lors de l'invention de la machine, Scherbius a eu la bonne idée d'aligner les trois rotors l'un derrière l'autre, chacun ayant des connexions internes différentes et chacun engendrant donc des alphabets codés différents. Ainsi, lorsqu'une lettre est tapée, le premier rotor tourne. Après 26 lettres, le deuxième rotor tourne d'un cran puis le premier rotor fait de nouveau un tour de 26 positions pour que le deuxième retourne d'un cran… etc. cela donne 26^3 positions possible soit 17576 positions pour 3 rotors (26^5 = 11 881 376 positions pour 5 rotors).

Le réflecteur :

On sait maintenant comment crypter une lettre, mais il manque un élément important afin de retrouver la lettre originale à partir de la lettre cryptée : le réflecteur. Celui-ci permet de pouvoir crypter et décrypter « symétriquement ».

Sur le schéma ci-dessous, le système de brouillage a été simplifié à 2 rotors mais on peut quand même observer le fonctionnement du réflecteur. Si A est codé C alors pour la même position des rotors C est codé A. Lorsqu'une lettre est tapée, le courant électrique traverse les rotors et le réflecteur permet de renvoyer le courant dans le sens inverse. Le courant retraverse donc les rotors et affiche la diode correspondante à la lettre cryptée (ou décryptée).



La clef :

La clef d'un message se décompose en plusieurs données. Tout d'abord, il faut connaître les composantes de la clef du jour, qui changeait toutes les vingt-quatre heures et étaient les mêmes pour toute une armée, c'est-à-dire :

– L'ordre dans lequel les rotors étaient positionnés **:** Trois rotors sont choisis sur cinq disponibles, numérotés de I à V, et placés sur la machine dans un ordre bien déterminé.

– Le placement de la bague **:** Chaque rotor placé a un décalage de la bague déterminée, chaque bague d'un rotor pouvant être mise dans vingt-six positions différentes.
Etant donné que la bague ajoute peu à la force du cryptage, on ne la prendra pas en compte pour calculer le nombre de clefs. En effet, même si l'on ne connaît pas son réglage, on pourra retrouver des portions de texte clair, étant donné qu'elle n'introduit qu'un décalage au niveau de l'orientation des rotors et de leur rotation.

– Les couples de lettres interchangés **:** Le tableau de fiches était également fixé pour la journée. Dix fiches sont ainsi branchées lors de l'utilisation de la machine.
Enfin, il faut connaître la composante de la clef propre au message. Il s'agit de l'orientation des rotors : chaque rotor était tourné de telle sorte à ce que dans une fenêtre laissant apparaitre les lettres inscrites sur la bague, apparaisse une lettre constituante de la clef. Vingt-six alignements étaient donc possibles par rotor.
Le nombre de réglages possibles au niveau de l'ordre des rotors correspond au nombre de choix différents existant de trois éléments d'un ensemble en contenant cinq. On utilise une formule mathématique de dénombrement.
Il s'agit du nombre d'arrangements de *3* parmi *5* :
En mathématique, le principe d'arrangement fait partie de l'analyse du dénombrement et sert aux calculs de probabilité. Lorsque nous choisissons *k* objets parmi *n* objets, nous pouvons les représenter par un *k-uplet* d'éléments distincts et on en constitue une liste ordonnée sans répétition possible, c'est-à-dire dans laquelle l'ordre des éléments est pris en compte (si l'on permute deux éléments de la liste, on a une liste différente, et un élément ne peut être présent qu'une seule fois).

Le nombre d'arrangement est noté A_n^k et ce nombre est égal à :

$$A_n^k = n\,(n-1)\,(n-2)\,....\,(n-k+1)$$

Pour résumer globalement le premier élément est choisi parmi *n*, le second parmi (*n* – 1)… etc jusqu'au dernier élément. On peut également ajouter la notion factorielle (où n!= 1x2x...xn) à la formule, elle devient alors :

$$A_n^k = \frac{n!}{(n-k)!} \text{ pour } k \geq n$$

Dans notre exemple à 3 rotors sur 5, le nombre d'ordres des rotors est : A_5^3

$$= \frac{5!}{(5-3)!}$$

$$= 60$$

Nombre de clefs différentes possibles correspondant :

Nombre de clefs = *1 507 382 749 377 250*

Le calcul permettant d'atteindre ce résultat est très complexe. Le voici ci-dessous en tant que source :

$$= C_{26}^{20} \text{ x } \prod_{i=0}^{9} C_{2(10-i)}^{2} \text{ x } \frac{1}{10!}$$

$$= \frac{26!}{20! \times 6!} \text{ x } \left(\frac{20 \times 19}{2} \text{ x } \frac{18 \times 17}{2} \text{ x } \ldots \text{ x } \frac{2 \times 1}{2} \right) \text{ x } \frac{1}{10!}$$

$$= \frac{26!}{20! \times 6!} \text{ x } \frac{20!}{2^{10}} \text{ x } \frac{1}{10!}$$

$$= \frac{26!}{6! \times 2^{10} \times 10!}$$

$$= 1\,507\,382\,749\,377\,250$$

Le nombre total de possibilités se calcule en multipliant :

Nombre d'ordre des rotors x nombre de réglage de 10 fiches x nombre de positions des rotors

Soit = *60 x 1 507 382 749 377 250 x* $26^3 = 1{,}589...x10^{21}$ ou environ 16 milliards de milliards de possibilités.

Si l'on parvenait à tester toutes les clefs une à une à raison d'une par seconde, le message serait décrypté environ au bout de cinq mille milliards d'années (soit beaucoup plus

que le temps passé depuis la création de l'Univers) ! Ce chiffre impressionnant est principalement dû à l'ensemble du brouilleur car sans lui la machine ne pourrait faire qu'un cryptage mono-alphabétique, un système que l'on savait décrypter il y a déjà plusieurs siècles comme nous l'avons vu précédemment.

C. La machine Enigma, un élément fondamental pour la guerre et plus encore

1. Son utilité dans la guerre

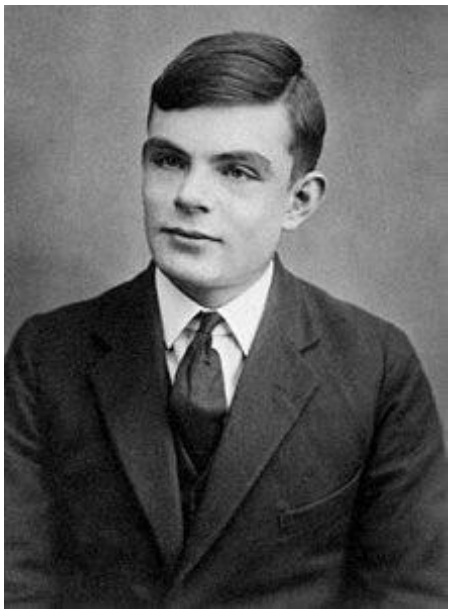
La deuxième Guerre mondiale est l'un des événements historiques les plus importants du 20ème siècle. En effet, elle a bouleversé l'organisation de la société en demandant l'emploi de nombreuses ressources et de différentes stratégies. Nous pouvons citer l'utilisation de la machine Enigma au cours de la deuxième Guerre mondiale notamment par les forces armées allemandes. Rappelons que la seconde Guerre mondiale a opposé les Alliés et l'Axe durant près six ans, de 1939 à 1945.

La machine a été utilisée par l'armée allemande jusqu'à leur défaite. Comme déjà indiqué, c'est la Kriegsmarine qui décide de s'en équiper initialement en 1926. La Heer (armée de terre) et la Luftwaffe (armée de l'air) lui emboîtent le pas trois ans après. Ainsi en 1929, toutes les branches de la Wehrmacht sont équipées d'Enigma. La machine offrira un avantage considérable aux Allemands lors de la Blitzkrieg permettant de coordonner efficacement infanterie, aviation et marine tout en s'assurant de la sécurité du transfert d'information. La machine restera efficace jusqu'aux environs de 1943 où les Alliés arriveront enfin à "casser" le code d'Enigma, mais les allemands étant sûrs de leur avance, continueront à l'utiliser sans savoir que les Alliés décryptent déjà tous leurs messages.

2. Alan Turing, le sauveur des Alliés

Alan Turing est né en février 1912 à Londres, c'était un mathématicien et cryptologue britannique. Turing est considéré comme le précurseur de l'ordinateur.

Alan Turing :



Dès son plus jeune âge Turing se démarque de ses camarades, il apprend à lire tout seul et en seulement 3 semaines, il montre également une grande facilité en mathématiques et en résolution d'énigmes. À 13 ans, Turing rejoint la Sherborne School, et dès son premier jour de classe il ne passe pas inaperçu. Le jour de la rentrée est celui de la grève générale de 1926. Mais entêté à faire sa rentrée, il parcourt à bicyclette les 90 km qui séparent son domicile de sa nouvelle l'école. En 1927, Turing se lie d'une grande amitié avec son camarade Christopher Morcom, passionné de sciences et de mathématiques comme lui, plusieurs personnes estiment qu'Alan Turing était secrètement amoureux de celui-ci. Quand Christopher meurt en février 1930 de la tuberculose, Turing n'admet pas la disparition de son ami. Persuadé que l'esprit de Morcom continue à exister, il décide de dédier ses travaux à son défunt ami.

Turing étudie ensuite au King's College de l'Université de Cambridge. Et en 1936 il publie un article, « *On Computable Numbers, with an Application to the Entscheidungsproblem* » où il y résout le problème de décisions énoncé en 1928 par l'Allemand David Hilbert, connu sous le nom allemand d'« *Entscheidungsproblem* ». Pour cela il présente le concept de la « machine universelle », une machine qui accomplit toutes les

tâches de n'importe quelle autre machine. Celle-ci est considérée comme l'ancêtre de l'ordinateur.

Au moment de la déclaration de guerre, Turing est appelé par l'armée britannique à rejoindre le service consacré au décryptage de la machine Enigma allemande. Il rejoint donc le centre secret de Bletchley Park, un centre créé par les services secret Anglais (MI6).
En 1952, ses travaux n'étant pas reconnus car classés Secret Défense, Turing est accusé d'homosexualité et « d'atteinte à la pudeur » et est condamné à la castration chimique.

Alan Turing se suicide avec du cyanure pendant la nuit de 7 juin 1954 et est retrouvé mort chez lui le 8 juin. C'est en 2013 que Turing est gracié à titre posthume par la reine Elizabeth II et devient réellement un "héros de guerre". Selon plusieurs historiens, le travail de Turing aurait permis de raccourcir la guerre de 2 ans et de sauver pas loin de 14 millions de vies.

Alan Turing à Bletchley Park :

Au commencement de la guerre, Alan Turing intègre l'équipe chargée de décrypter et de craquer le code de la machine Enigma dirigée par le commandant Alastair Denniston. Il y retrouve les brillants Hugh Alexander, John Cairncross, Peter Hilton, Keith Furman et Charles Richards, chacun d'eux est maître dans son domaine.

Mais pendant les premiers temps il ne s'entend pas bien avec ses coéquipiers car il est perçu comme associable. Il ne les aide pas et préfère faire ses travaux seul, travaillant sur une « bombe électromagnétique » destinée à casser Enigma. Mais pour la construction Turing a besoin de 100 000£ (ce qui est une somme considérable en période de guerre). Denniston refuse de lui attribuer ce financement. Bien décidé à construire sa machine, Alan Turing écrit une lettre avec son équipe directement à Winston Churchill, qui accepte de verser les 100 000£ et nomme par la même occasion Turing chef de l'équipe de décryptage. En 1940, la construction de la machine de Turing, qu'il surnomme « Victory », commence.

Malheureusement pour Turing, sa « bombe à casser Enigma » ne fonctionne pas assez rapidement au cours des premiers essais car les clés nazies pour Enigma changent chaque jour à minuit et le premier message est le bulletin météo de la journée. Donc l'équipe n'avait que 18 heures pour tester toutes les clés, ce qu'ils n'avaient jamais encore réussi. « Victory » ne fonctionnant pas, Denniston essaye de chasser Turing du programme mais il cède finalement et accepte de laisser Turing tranquille lui laissant 6 mois pour faire ses preuves.

Puis un jour, lors d'une fête, grâce à une information venant d'une réceptionniste de message, Turing apprend que l'un des officiers allemands met toujours les mêmes lettres au début de ses messages (les clés que les officiers allemands étaient censés changer à chaque fois). Grâce au bulletin météo journalier de l'armée allemande comprenant toujours les mots « Temps » et « heil Hitler », il détient suffisamment d'informations pour faire marcher la machine. Il rentre donc celle-ci dans sa machine. Et elle fonctionne, il trouve la combinaison du jour et intercepte pour la première fois un message allemand ! Cependant Alan Turing et son équipe décident de garder le secret car si l'armée anglaise empêche l'attaque de tous les objectifs des allemands, ceux-ci se rendront tout de suite compte que les Alliés ont cassé le cryptage d'Enigma.

Turing en informe tout de même le chef du MI6 présent à Bletchley, les services de renseignement anglais. Ils décident d'un commun accord que Turing et son équipe doivent maintenant calculer statistiquement le nombre d'interventions anglaises suffisantes pour gagner la guerre et le maximum à ne pas dépasser pour que les Allemands ne se rendent compte de rien. Quant aux services secrets leur travail est d'inventer de fausses sources sur l'obtention des informations.

3. Ce qu'Enigma a changé dans le développement informatique

Tout d'abord ce n'est pas Enigma même qui a permis directement le développement informatique mais plutôt ses conséquences indirectes. Ce ne sont pas les Allemands mais les Anglais qui ont passé un cap dans la programmation. La "bombe de Turing" est programmée avec un langage binaire composé uniquement de 0 et de 1, le même langage qu'utilisent les ordinateurs tels que nous les connaissons aujourd'hui.

En 1945, Turing prend connaissance du rapport "von Neumann" qui décrit la composition générale et liste les méthodes de programmation d'un ordinateur. Turing rédige alors le premier plan détaillé d'un ordinateur qu'il appellera l'ACE (Automatic Computing Engine). Malheureusement ce projet n'aboutira jamais pour des raisons administratives et budgétaires. Mais contre tout hasard, en 1948, Turing est appelé par Max Newman, un ancien de ses professeurs à l'université de Manchester où celui-ci dirige le développement de l'un des tout premiers véritables ordinateurs le *Manchester Mark I*. Turing accepte et travaille à la programmation de l'ordinateur.. Dans l'article "Computing Machinery and Intelligence", il

explore le problème de l'intelligence artificielle et propose une expérience maintenant connue sous le nom de test de Turing, où il tente de définir une épreuve permettant de qualifier une machine de « consciente ». Turing fait alors le pari que d'ici cinquante ans, il n'y aurait plus moyen de distinguer les réponses données par un homme ou un ordinateur, et ce sur n'importe quel sujet. Et il avait raison. En 2018 (soit environ 60 ans après), l'intelligence artificielle développée par Google a réussi à prendre un rendez-vous dans un salon de coiffure et de tenir une conversation avec la gérante qui ne s'est pas rendue compte qu'elle parlait à un robot (vidéo dans la bibliographie).

Conclusion :

Les sciences ont fourni des éléments essentiels à l'évolution de notre société. La cryptologie, science du secret, a permis d'inventer le codage et le cryptage. Les premières formes de cryptage ont aidé les premiers grands empires, tel que l'Empire romain, à mener des campagnes militaires bien coordonnées et donc à agrandir leurs territoires et leur influence dans le monde. Le cryptage a aussi permis à des pays de déclencher la guerre la plus meurtrière de l'histoire de l'Humanité mais aussi d'en réduire sa durée, provoquant par la même occasion les débuts de l'informatique. Aujourd'hui le codage sert à nous faciliter la vie avec des technologies informatiques extrêmement rapides. Nous pouvons donc dire que le codage et le cryptage ont été des facteurs de l'évolution de la société et des civilisations antérieures à celle que nous connaissons aujourd'hui.

Bibliographie :

Film : Imitation Game (2014)

https://www.etaletaculture.fr/geekeries/le-chiffre-de-cesar/

https://fr.wikipedia.org/wiki/Scytale

https://fr.wikipedia.org/wiki/Chiffrement_par_décalage

https://grandzebu.net/informatique/codbar/ean13.htm

https://www.lsa-conso.fr/le-code-barres-40-ans-d-histoire-de-la-grande-consommation,141022

https://www.youtube.com/watch?v=eUAN2FUkJbg

http://ww2.ac-poitiers.fr/techno/IMG/pdf/tutoriel_code_qr.pdf

https://www.unitag.io/fr/qrcode/what-is-a-qrcode

https://www.1min30.com/social-media-marketing/10-exemples-dutilisation-de-qr-codes-cross-canaux-16559

https://open-freax.fr/code-qr-explications/

http://cerig.pagora.grenoble-inp.fr/memoire/2004/rfid.htm

https://www.youtube.com/watch?v=SWofZ0M3uK0

https://fr.wikipedia.org/wiki/Radio-identification

http://igm.univ-mlv.fr/~dr/XPOSE2012/RFID_Modbus/RFID/histoire.html

https://en.wikipedia.org/wiki/Arthur_Scherbius

https://fr.wikipedia.org/wiki/Enigma_(machine)

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/enigmaguerre

https://www.apprendre-en-ligne.net/crypto/Enigma/

https://lejournal.cnrs.fr/articles/alan-turing-et-le-decryptage-des-codes-secrets-nazis

https://www.nouvelobs.com/societe/20151202.OBS0598/code-secret-enigma-la-dgse-remet-les-anglais-a-leur-place.html

https://lejournal.cnrs.fr/articles/alan-turing-et-le-decryptage-des-codes-secrets-nazis

https://www.frenchweb.fr/petite-histoire-de-la-cryptographie-de-la-machine-enigma-a-lordinateur/264879

Vidéo de l'intelligence artificielle : https://www.youtube.com/watch?v=YCWJ0z6_z34

Livre : Comprendre les codes secrets, cryptologie et codage, par Pierre Vigoureux