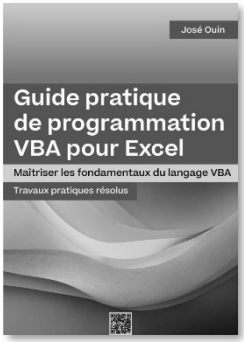
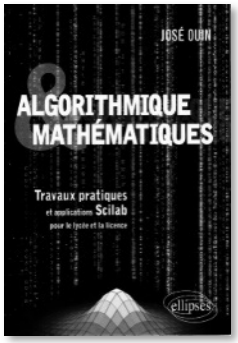
José Ouin
Ingénieur INSA Toulouse
Ancien élève de l'ENS Cachan
Professeur Agrégé de Génie civil
Professeur Agrégé de Mathématiques

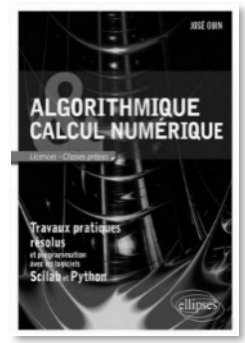
ENIGMA

Histoire, fonctionnement et programmation en Python et en VBA pour Excel

Du même auteur aux Editions Ellipses et sur Amazon







ISBN : 978-2-9593648-5-3

Avant-propos

Je dédie ce livre à tous les passionnés de programmation et de cryptanalyse, ceux qui, comme moi, trouvent dans ces disciplines un mélange fascinant de logique, de créativité et de mystère. C'est avec une immense passion que j'ai entrepris l'écriture de ce projet, qui m'a replongé dans l'atmosphère captivante du film « *The Imitation Game* », retraçant l'histoire d'Alan Turing et des efforts déployés à Bletchley Park pour casser les codes de la machine Enigma. Ce film, comme beaucoup d'entre vous l'ont sans doute ressenti, m'a rappelé à quel point la cryptanalyse est une aventure intellectuelle hors du commun.

Ce livre est né de mon désir de partager cette fascination pour l'Enigma, une machine à la fois ingénieuse et complexe, dont le fonctionnement électromécanique a défié les plus grands esprits de l'époque. Mon souhait est qu'à travers ces pages, vous puissiez, vous aussi, plonger dans les mécanismes internes de cette machine légendaire, et apprendre à chiffrer et déchiffrer des messages à l'aide du script Python et du classeur Excel utilisant VBA que j'ai créés pour simuler son fonctionnement.

Que vous soyez débutant ou expert en cryptanalyse et en programmation, j'espère que ce livre vous offrira une exploration enrichissante et stimulante de l'Enigma et de ses secrets. C'est une invitation à voyager dans le temps, tout en plongeant dans l'univers passionnant du code et du déchiffrement.

Bonne lecture et bonne exploration !

José Ouin

- Un avis positif ?

Merci de prendre le temps de laisser votre évaluation (☆☆☆☆☆) sur la page Amazon de ce livre. Vos avis aident les autres lecteurs à mieux comprendre l'ouvrage.

- Un avis négatif, une question, une suggestion ou une remarque ?

N'hésitez pas à m'envoyer un message via le formulaire de contact de mon site Internet. Lien : `https://joseouin.fr/bandeaucontact`

Table des matières

1- Introduction générale

1-1. Présentation de l'intérêt du chiffrement et de la sécurité des communications.

La cryptographie, ou l'art de rendre un message illisible à quiconque ne possède pas la clé pour le déchiffrer, est aussi ancienne que la communication elle-même. Des anciens codes de César aux systèmes numériques complexes d'aujourd'hui, le besoin de protéger les informations est une constante. Dans le contexte actuel, où les données personnelles, financières et même les communications gouvernementales sont transmises électroniquement, l'importance du chiffrement est plus critique que jamais.

1-1.1 Un besoin qui traverse les âges

Dans les sociétés anciennes, le chiffrement servait à protéger les informations militaires et diplomatiques. L'histoire regorge d'exemples où des messages cryptés ont changé le cours des événements : des émissaires de l'Empire romain aux réseaux d'espionnage de la Renaissance. À chaque époque, la confidentialité des informations pouvait déterminer l'issue d'une guerre, la chute d'un empire ou la survie d'une civilisation.

À l'ère moderne, ce besoin s'est intensifié avec l'essor des télécommunications, des ordinateurs et d'Internet. Les communications ne sont plus simplement locales, elles sont globales et instantanées. Le volume de données échangées quotidiennement est colossal, et ces informations sont de nature très variée : des transactions bancaires, des informations médicales, des dossiers militaires, des communications privées ou encore des documents commerciaux confidentiels. Toute fuite ou interception peut avoir des conséquences désastreuses.

1-1.2 La cryptographie comme rempart face aux menaces

Le chiffrement est ainsi devenu un outil essentiel pour assurer la sécurité des informations. Il permet non seulement de garantir la confidentialité, mais aussi l'intégrité des données (assurant qu'elles n'ont pas été altérées) et l'authentification (confirmant l'identité des parties impliquées dans la communication). De plus, dans un contexte où les cyberattaques se multiplient, la cryptographie est l'une des dernières lignes de défense contre les tentatives d'espionnage, de sabotage et de vol de données.

La protection des communications n'est plus seulement l'apanage des États ou des grandes entreprises. Aujourd'hui, chaque individu et chaque organisation est concerné par la sécurité des informations. Que ce soit pour envoyer un email, effectuer un achat en ligne ou échanger des messages confidentiels, la cryptographie joue un rôle central dans notre quotidien numérique.

3-2. Le rôle d'Arthur Scherbius et l'invention de la machine Enigma

L'histoire de la cryptographie a été marquée par des inventeurs et des visionnaires qui ont su repousser les limites de la technologie de leur époque pour garantir la sécurité des communications. Arthur Scherbius est l'un de ces pionniers, et son invention, la machine Enigma, est devenue un symbole d'ingéniosité technique et de complexité cryptographique. La machine Enigma, bien qu'elle ait été rendue célèbre par son utilisation durant la Seconde Guerre mondiale, est à l'origine une invention conçue pour des usages civils et commerciaux.

3-2.1 Qui était Arthur Scherbius ?

Arthur Scherbius

Arthur Scherbius est né en octobre 1878 à Francfort-sur-le-Main, en Allemagne. Ingénieur en électricité de formation, il a étudié à l'Institut polytechnique de Hanovre et à l'Université technique de Munich, obtenant un doctorat en ingénierie. Après avoir travaillé dans divers secteurs, dont l'électrotechnique, il est devenu inventeur et entrepreneur.

Scherbius était fasciné par l'idée de protéger les communications à une époque où les télécommunications prenaient une importance stratégique croissante, tant dans les milieux commerciaux que militaires. À cette époque, les systèmes de chiffrement étaient souvent manuels et relativement faciles à casser avec les méthodes traditionnelles de cryptanalyse. Scherbius a vu l'opportunité de combiner des technologies émergentes comme l'électromécanique avec la cryptographie pour créer une machine capable de rendre les communications presque inviolables.

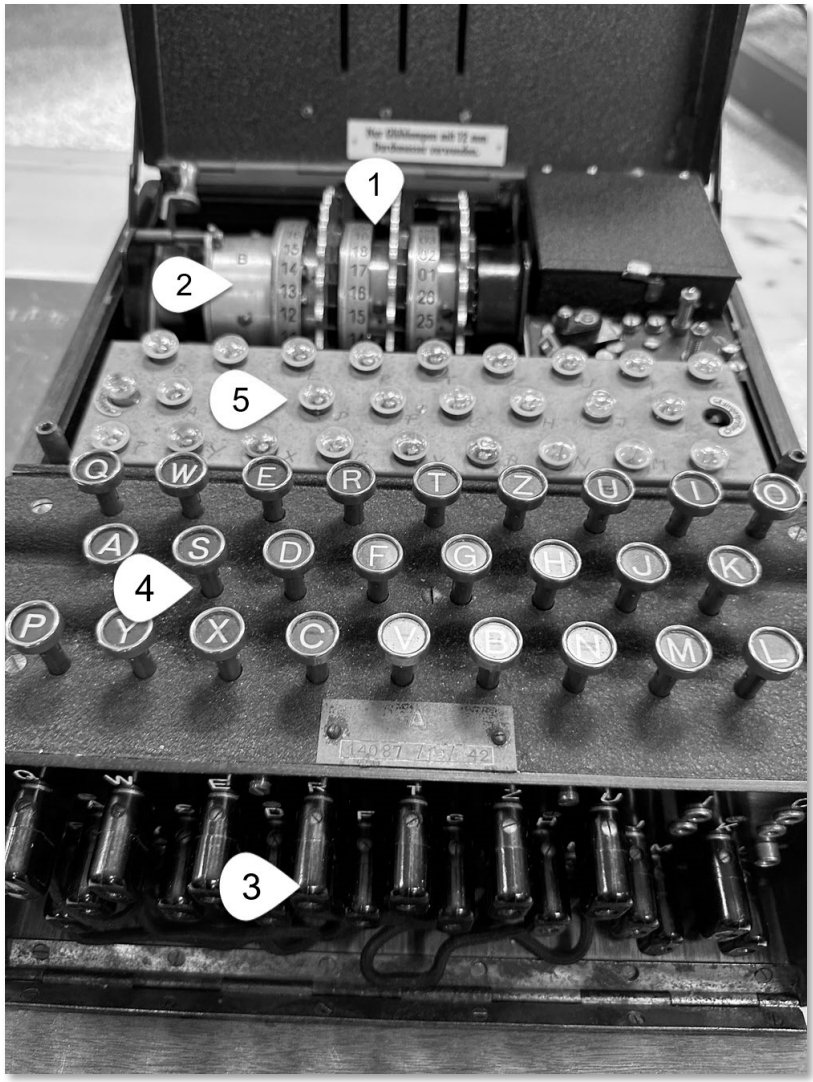
3-2.2 L'invention de la machine Enigma

En 1918, alors que la Première Guerre mondiale venait de se terminer, Scherbius déposa un brevet pour une machine de chiffrement qu'il appela "Enigma". Le brevet fut accepté en 1918 et la machine fut commercialisée dès 1923. Initialement, l'objectif de Scherbius était de vendre sa machine aux entreprises et aux gouvernements pour protéger leurs communications confidentielles.

L'invention d'Arthur Scherbius repose sur un principe fondamental de permutation des lettres, rendu complexe par l'ajout de composants mécaniques rotatifs. L'idée clé de la machine Enigma était de passer de systèmes de chiffrement statiques à un système dynamique où les lettres étaient substituées de manière différente à chaque frappe, augmentant ainsi de façon exponentielle le nombre de combinaisons possibles.

3-2.3 Les composants de la machine Enigma

La machine Enigma, capot ouvert : on peut voir clairement les rotors et le réflecteur, éléments clés du mécanisme de chiffrement. Les lampes du tableau lumineux, qui s'allument pour indiquer les lettres chiffrées, sont également visibles. Ces composants essentiels permettent à la machine de transformer chaque frappe sur le clavier en une lettre chiffrée, grâce au système complexe des rotors et du réflecteur.



Machine Enigma – Modèle 1942

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

Cette photographie illustre l'importance de la machine Enigma dans les communications cryptées de l'armée allemande pendant la Seconde Guerre mondiale. Elle montre comment les opérateurs travaillaient en équipe pour envoyer et recevoir des messages sécurisés sur le terrain. L'attention portée à l'utilisation correcte de la machine reflète l'importance cruciale de ces opérations pour garantir la sécurité des informations militaires.

Source

https://www.nationalmuseum.af.mil/

Photographie : Le général allemand Heinz Guderian dans un véhicule de poste de commandement. On aperçoit une machine Enigma en cours d'utilisation. Cette image illustre l'importance de la cryptographie pour les communications militaires sur le front, avec la machine Enigma servant à sécuriser les messages stratégiques de l'armée allemande pendant la Seconde Guerre mondiale.

Cette représentation sous forme de tableau permet de mieux visualiser comment chaque position du rotor transforme une lettre en une autre selon un schéma fixe.

```
alphabet  = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
rotor_III = "BDFHJLCPRTXVZNYEIWGAKMUSQO"
```

	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
ROTOR	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O

Quelques exemples de contacts entre plusieurs rotors :

- Rotors I, II et III sur la position [01, 01,01] ou [A, A, A]
  La sortie « J » du Rotor III est en contact avec l'entrée N°10 du rotor II (qui est connectée avec la sortie « B ») et la sortie « L » du rotor II est en contact avec l'entrée N°12 du rotor I (qui est connectée avec la sortie « T »).

		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 1	ROTOR	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	I	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J

		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 1	ROTOR	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	II	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

		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 1	ROTOR	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O

- Rotors I, II et III sur la position [03, 06,10] ou [C, F, J]
  La sortie « J » du Rotor III est en contact avec l'entrée N°1 du rotor II (qui est connectée avec la sortie « I ») et la sortie « L » du rotor II est en contact avec l'entrée N°7 du rotor I (qui est connectée avec la sortie « V »).

		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
C 3	ROTOR	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2
	I	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	E	K

		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
F 6	ROTOR	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5
	II	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E	A	J	D	K	S

		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
J 10	ROTOR	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9
	III	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	B	D	F	H	J	L	C	P	R

Remarque :
Les couples « Q-R », « E-F » et « V-W », respectivement pour les rotors I, II et III, indiquent la position des encoches pour chaque rotor. Par exemple, lorsque le rotor III affichera la position « V », il entraînera le rotor II lors de la prochaine frappe de touche sur le clavier d'Enigma (en passant de « V » à « W »).

- **Fonction du réflecteur**

Une fois que le signal a traversé tous les rotors, il arrive au réflecteur. Celui-ci renvoie le signal à travers les rotors dans la direction opposée, en le dirigeant vers une autre lettre de l'alphabet. Cela signifie que le courant fait un aller-retour à travers les rotors, ce qui double la complexité du chiffrement. Par exemple, si la lettre « A » est entrée, elle pourrait être codée en « C » après le passage à travers les rotors, puis être reflétée en une autre lettre, comme « D », après le retour à travers les rotors.

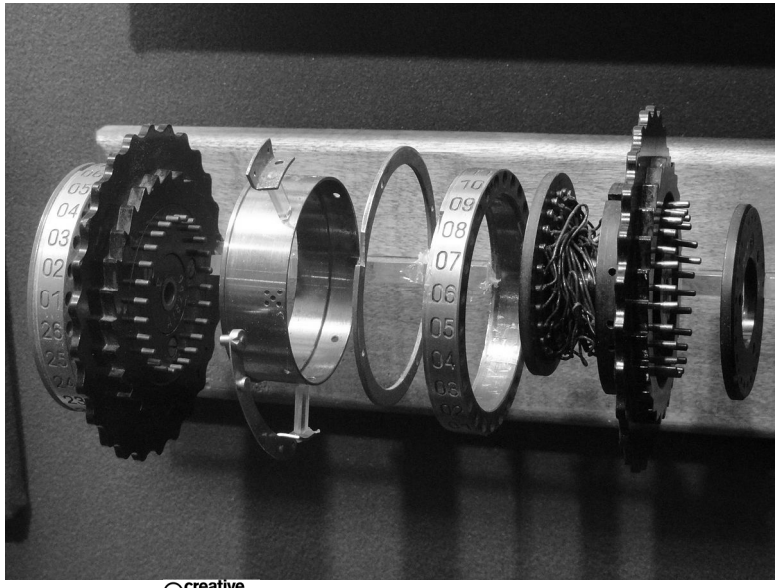
- **Caractéristiques du réflecteur**

Le réflecteur présente une faiblesse importante dans le système de chiffrement d'Enigma, car il empêche une lettre d'être codée en elle-même. C'est-à-dire qu'une lettre comme « A » ne peut jamais être codée comme « A », ce qui fut un des points faibles exploités par les cryptanalystes alliés lors de leurs tentatives de déchiffrement des messages Enigma.

- **Types de réflecteurs**

Le réflecteur B était le plus courant et largement utilisé dans la plupart des machines Enigma militaires. Le réflecteur C a été introduit plus tard et était principalement utilisé pour des communications navales spécifiques, offrant des configurations supplémentaires pour accroître la sécurité.

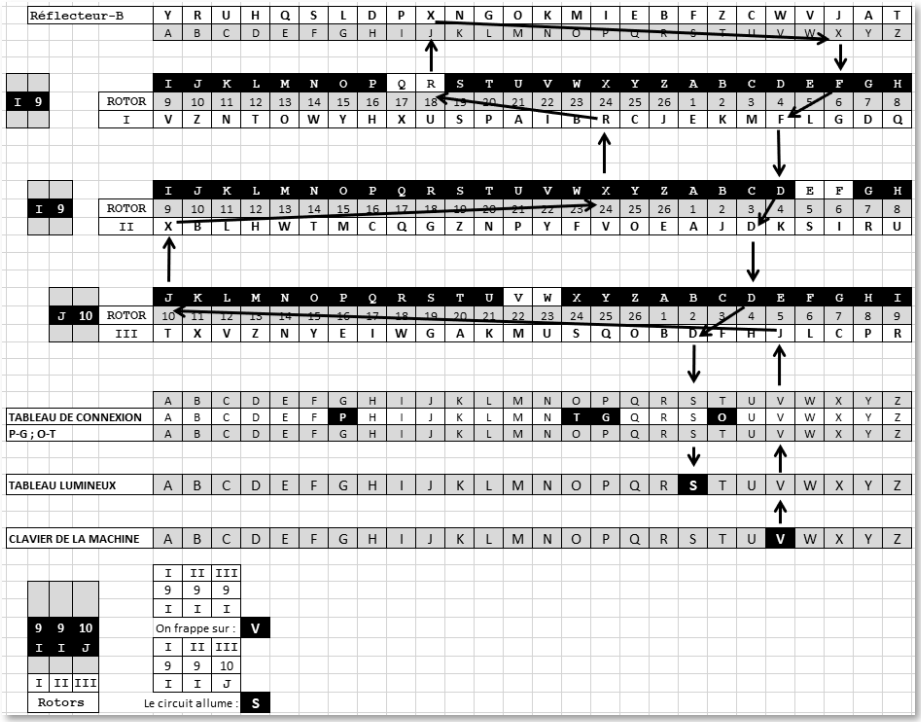
5-1.6 Vue éclatée d'un rotor et de ses composants



5-3.2 Exemple N°1 : sans connexion au tableau de connexions

On se place dans le cas où les anneaux ne créent pas de décalages (position [1,1,1]). La feuille Excel ci-dessous permet de dessiner à la main le parcours dans les différents rotors.
Au départ les rotors sont réglés sur la position [9,9,9] (ou [I,I,I]). Lorsque l'on frappe sur la lettre « V », le rotor III avance d'un cran et le chiffrement de la lettre « V » s'effectuera avec la position [9,9,10] (ou [I,I,J]). On obtient la lettre « S ».

Description du cheminement du courant dans la machine Enigma :
1/ Tableau de connexions (plugboard) : pas de transformation de la lettre « V »
2/ Rotor III : un contact s'effectue avec la lettre « J »
3/ Rotor II : contact avec la lettre « X »
4/ Rotor I : contact avec la lettre « R »
5/ Le passage par le Réflecteur B transforme « J » en « X »
6/ Rotor I : contact avec la lettre « F »
7/ Rotor II : contact avec la lettre « D »
8/ Rotor III : contact avec la lettre « D »
9/ Tableau de connexions : pas de transformation de la lettre « S »
10/ Tableau lumineux : le contact électrique s'effectue avec la lettre « S »



Ces tables indiquaient les positions de départ des rotors, les réglages du plugboard (tableau de connexions) et, parfois, d'autres paramètres nécessaires pour assurer le chiffrement. Ce procédé constituait un manque de sécurité car les réglages, identiques pour tous les messages de la journée, fournissaient aux cryptanalystes des indices constants à exploiter. En étudiant plusieurs messages chiffrés avec la même configuration initiale, les cryptanalystes pouvaient ainsi déceler des schémas récurrents et affaiblir progressivement le chiffrement.

- **Problème de sécurité dû au double chiffrement des clés de message**

⇨ **Clés journalières**

Chaque opérateur recevait une table qui lui indiquait les paramètres spécifiques à utiliser chaque jour. Cependant, avant d'envoyer un message, un opérateur devait choisir arbitrairement une clé de message pour le chiffrement, correspondant à une position initiale spécifique des rotors. Le choix de cette clé de message était chiffré et indiqué en début de message, ce qui introduisait une vulnérabilité.

Extrait d'un carnet de clés journalières (carnet factice) pour le mois de janvier 1940

GEHEIM! TRITON JANUAR 1940

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	III IV V	08 02 09	AI BR FP HU JK LW MS NQ OT VX	NJN BYN DLK QHN
30	V IV III	25 04 09	AR BG CD EP IY JO KU MN QZ VX	ZBI QDN DWV QRX
29	I II IV	13 14 26	AT EO FY GV HM IU KQ NW PR SZ	SKC ADB QCW DUV
28	III II IV	18 25 25	AD BZ EF GO HJ IY LX PW QU ST	CBW VKI PCL YCB
27	III II I	09 09 04	BM CE DS FU GX IJ KO LV QR TY	QLQ MIK DFO NPP
26	II I V	16 19 12	AL BS CD EU GK JO MR NV PQ WY	EMA NGH VPR EOF
25	IV I III	15 03 14	AB EP GJ HI KY LU NS OZ QT VW	ZAY TRG YDM BXF
24	V II III	12 19 06	AW BH CD EU GM IO LS NR PX TV	OVQ JYI JTK NMP
23	III IV I	14 25 12	AP CL EM FW GS IN JR KO TU XY	KIY FJP WGZ TPA
22	II V IV	14 19 21	AR BT CK DX FO GN HQ JY MZ UW	NGN CGU WLJ ENG
21	I III IV	03 23 16	AY EV FZ GX IO JN KL MP QU SW	UNT SMB MDV MBX
20	II IV III	05 24 26	AM BJ CT GQ HO IX KV LP NW YZ	XAY VEJ QBX DPS
19	IV II III	12 02 11	BT CX EF HJ IY KW LR MS NQ UV	WZR IBY ONF NUD
18	III II I	16 01 11	AU BV CN DM EZ FY GP IQ JW SX	SLE ZQS TLW HGL
17	IV I V	10 21 06	AI BY CS DQ EK GT HN MX OV UW	AXC DGO KNJ PIZ
16	IV V III	17 21 19	AD BK CU EL FX IP MZ NV OS RW	UQB SXA YYS JXL
15	II III V	05 23 03	BD CQ EZ FL HU IM KP NS OW XY	OKU EVB MDC DCI
14	IV II III	24 25 13	AZ BF CX DM GT IV JS NU QR WY	JWQ FUH HPW RSV
13	IV III II	19 12 19	AR BF CL DM EY IW OV PU QZ ST	DXL OUN HJU KZM
12	V IV III	07 22 22	AB CJ EY GQ HV IN KO MT RU SX	BUC EAL VFJ GAE
11	I II III	18 22 25	AY BR CG DT EH IJ KM LX NZ QS	CLI AFK PBW NGJ
10	IV I III	07 25 25	AB EY FR GI HO JP KU LW MS QT	VUC ESX LHB AXW
09	V IV II	17 10 15	BL CQ EZ FH GI KN MP OV RX UW	VPY EEX NLV UNQ
08	I IV III	05 13 24	AO BQ CD EJ FG IZ MR NY PT UW	PCL GRQ WWI FQO
07	IV I II	10 09 08	BZ CV DW FN GK IT JS MU OX QR	MKH BHZ VTJ LUM
06	IV V III	07 22 21	AD BN CR EI FK GT HM JO SZ VY	YUX LFT AID PXQ
05	III II IV	18 16 08	BX CT EW FH GY JZ KO LR MU NS	DBL JAY RLX EMQ
04	III II I	20 01 06	AC BQ DT EP FY HI LS MR NU VX	SWW BMB BDF BRX
03	IV I V	14 17 20	AO CF DQ EZ HR IX KL PY SV TU	OPT VNO GLS FBV
02	III II I	10 21 15	AN CR DT EP FH IJ KY OS QU WX	YZQ VJH BUC QRC
01	I IV V	10 22 11	BM CO DY EG FK HU LP NZ QR TV	LUY JFJ BVV YJJ

6- Développement d'un simulateur Enigma en langage Python

6-1. Description générale de la programmation de la machine Enigma

Pour introduire la programmation des principes de base de la machine Enigma en Python, il est essentiel de bien comprendre les composants et leur fonctionnement, puis de les traduire en éléments programmables.

6-1.1 Composants fondamentaux de la machine Enigma

La machine Enigma repose sur plusieurs éléments clés qui seront modélisés dans le programme :

- Clavier : Permet de saisir une lettre à chiffrer.
- Rotors : Les rotors transforment chaque lettre de manière à ce que le signal électrique soit redirigé selon un chemin spécifique. Chaque rotor a une configuration différente, et tourne après chaque lettre saisie.
- Réflecteur : Réfléchit le signal renvoyé par les rotors, redirigeant le flux électrique dans le sens inverse.
- Tableau de connexions (plugboard) : Permet de permuter certaines lettres avant et après leur passage dans les rotors.
- Position initiale des rotors : La position initiale des rotors change la configuration des lettres en entrée.
- Position initiale des anneaux : les anneaux déterminent comment les lettres sur les rotors sont alignées avec les contacts internes des rotors. Cette position influence comment les signaux électriques traversent les rotors.

6-1.2 Structuration du programme en Python

L'objectif est de simuler chaque composant en tant que module ou fonction pour reproduire le processus de chiffrement.

- **Création des rotors**

Les rotors peuvent être représentés par des listes ou des dictionnaires Python où chaque lettre est mappée à une autre selon une permutation spécifique. Par exemple :

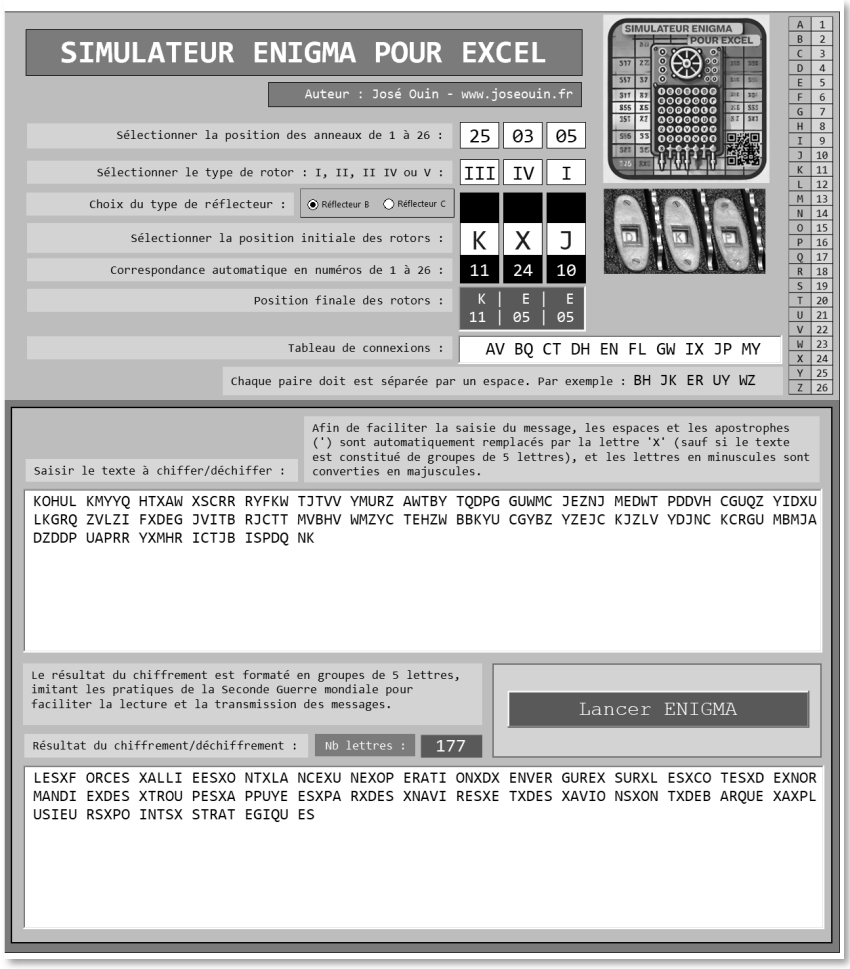
```
rotor_I = "EKMFLGDQVZNTOWYHXUSPAIBRCJ"
rotor_II = "AJDKSIRUXBLHWTMCQGZNPYFVOE"
rotor_III = "BDFHJLCPRTXVZNYEIWGAKMUSQO"
rotor_IV = "ESOVPZJAYQUIRHXLNFTGKDCMWB"
rotor_V = "VZBRGITYUPSDNHLXAWMJQOFECK"
```

7- Développement d'un simulateur Enigma en langage VBA pour Excel

7-1. Description générale de la programmation de la machine Enigma

La description générale de la programmation de la machine Enigma en langage VBA pour Excel est la même que celle du chapitre précédent sur le développement avec le langage Python.

Capture d'écran du simulateur Enigma pour Excel :



10- Outils et méthodes pour casser les codes Enigma

10-1. Introduction aux techniques de cryptanalyse utilisées par les Alliés

Les Alliés, et plus particulièrement les cryptanalystes polonais, britanniques et américains, ont développé plusieurs techniques novatrices pour casser les codes chiffrés par la machine Enigma, en s'appuyant sur des méthodes combinant analyse mathématique, ingénierie et exploitation des erreurs humaines. Voici les principales techniques qu'ils ont utilisées :

10-1.1 Le travail pionnier des cryptanalystes polonais

Marian Rejewski

Jerzy Różycki

Henryk Zygalski

Avant même la Seconde Guerre mondiale, les cryptanalystes polonais avaient déjà fait des percées importantes dans le déchiffrement d'Enigma. Trois cryptanalystes polonais, Marian Rejewski, Jerzy Różycki et Henryk Zygalski, ont joué un rôle crucial :

- **1/ Reconstitution des rotors :**

Marian Rejewski a réussi à recréer le fonctionnement des rotors de la machine Enigma en utilisant des mathématiques pures et des messages interceptés.

- **2/ Utilisation de la "grille cyclique" :**

Cette méthode a permis d'identifier les répétitions dans les configurations des rotors et d'en déduire leur disposition.

En 1939, avant l'invasion de la Pologne, les cryptanalystes polonais ont partagé leurs découvertes avec les Britanniques et les Français, ce qui a donné une base cruciale aux travaux ultérieurs.

12- Déchiffrer Enigma : Exercices pratiques

https://www.nationalmuseum.af.mil/Upcoming/Photos/igsearch/enigma/

12-1. Introduction aux exercices pratiques de déchiffrement

Dans ce chapitre, vous trouverez une série de messages chiffrés avec la machine Enigma que vous êtes invités à déchiffrer vous-même.

Pour réaliser ces déchiffrements, vous pouvez utiliser l'une des deux méthodes suivantes :

- **Le script Python ou le classeur Excel fourni dans ce livre**

Ce script Python et le classeur Excel simulent fidèlement la machine Enigma avec ses différents rotors, réflecteurs et configurations de tableau de connexions (plugboard). Vous pourrez les utiliser pour reproduire les étapes de déchiffrement et obtenir ainsi les messages en clair.

- **Un simulateur Enigma**

Comme présenté dans un chapitre précédent, il existe plusieurs simulateurs d'Enigma accessibles en ligne ou en tant que logiciels. Ces outils offrent une interface intuitive pour configurer les rotors, ajuster les anneaux, et manipuler le tableau de connexions. Ils constituent une alternative pratique au script Python et sont tout aussi efficaces pour les exercices proposés ici.

12-2. La table de clés journalières : outil essentiel pour déchiffrer les messages

La table de clés journalières est un élément fondamental utilisé par les opérateurs de la machine Enigma pour configurer chaque jour les paramètres de chiffrement et de déchiffrement. Cette table contient l'ensemble des réglages à appliquer pour les rotors, positions des anneaux, et le tableau de connexions (plugboard), et elle était partagée entre les opérateurs pour garantir que tous les messages envoyés et reçus le même jour puissent être chiffrés et déchiffrés correctement.

Chaque jour, les opérateurs sélectionnaient une nouvelle configuration basée sur cette table, garantissant que les communications resteraient sécurisées et cohérentes. Vous utiliserez donc cette table pour configurer vos outils (le script Python, le classeur Excel ou le simulateur Enigma) et ainsi déchiffrer tous les messages des exercices pratiques de ce chapitre.

Voici la table de clés journalières à utiliser pour tous les exercices (mois d'octobre 2024)

GEHEIM! JOSEOUIN OKTOBER 2024

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	IV V III	13 07 12	AP BG CQ DX EO FR HJ IZ LY MN	MSL PPC LLV HLZ
30	V IV II	17 26 14	BY CU DH ES FV GK IW JR MP QZ	WKX NZS IJG KUO
29	I III II	24 18 24	AV BR DY FG HP IL JO KZ MQ ST	WAZ NQF BNU GPG
28	I IV V	24 13 13	AU CM EV FX JP LR NS OZ QT WY	ZNX QXE TWH EWP
27	V III IV	07 10 04	CF DS ET GV HW IL JY NU OQ RZ	CPX OBM INW QNH
26	V III IV	17 02 19	AH BJ CY DK EO FX GI MU PR SZ	JIC SIN OMU WLL
25	I IV III	18 13 11	BF CE DR GL IJ MO NU PX TZ VY	FXH AAO MPC XRG
24	IV II I	10 07 19	CO DW GU HS JL KT NZ PV QX RY	IZO SQV WTZ UKB
23	III I V	05 09 14	BG CO DN EH FL IV KW PU RX YZ	OTY VDZ RVT KYW
22	III II IV	14 18 20	AB CM DT EO FH GL JR KP NY SZ	RCI YXU GHV OWA
21	II V IV	05 08 12	AK BN CT DP EZ HL MQ RW SY UV	SWC TFO REY XLU
20	III IV V	04 19 21	BU DF EK GV HQ IZ JO NR PW TY	WCL HKP DXT GLO
19	I II III	21 07 22	CW DJ EY FG HK IO LU MV NX TZ	GQK QAO ZBK UQI
18	I II III	16 08 26	AL BW CQ EN FU GT JX KZ RV SY	MZV TGX VUH PJL
17	V II I	05 02 09	AF BD EU GI HY JS MR NQ PX WZ	SAQ RKR RSH LJY
16	V II IV	23 25 22	AJ BF DH EZ GM OY PV QT RX SW	ILI LTC VDO JCA
15	IV I III	26 07 05	AD BC EX FI GL HP JN KR QV SW	OAI TAJ GKD IUT
14	III II I	21 15 08	BE DY FJ GK HT LO MN PR QX UV	SEK WEN JER XVZ
13	I III IV	23 20 09	CW EY FM HQ IL JZ NS OV PX TU	BUA ZNM YMQ UHY
12	V III IV	12 12 17	CM DK EG FP HZ IU JN LS QW VY	MWH SBF OJA XUU
11	IV I II	16 16 04	BM CU DZ FI GH JW KO QV RY SX	FRP LDO DOY AKZ
10	I V IV	18 25 13	AG BR CX DI ES FL HK NY QU VZ	MLZ SDH BRB KMM
09	IV I II	25 15 21	CN DZ ER FJ GI HU KS LP MT XY	ZXG PHE FRO EAG
08	I II III	14 08 08	AZ BU EY FK GM IJ NW OR PQ TX	OAJ ENZ CJI UDB
07	V II I	10 22 09	BN CR DW FL GO IZ JQ KU MV ST	QZN YQF KWP MMI
06	III V I	25 03 05	AV BQ CT DH EN FL GW IX JP MY	VJL LFG EIN WXL
05	II I IV	25 17 24	AJ BI CS DU FN KO LM PQ TY VW	ROX HSM HBW CMK
04	I V III	13 17 03	AT BH ES GX IY JN MZ OP QW RV	YLO PUB RUA IOP
03	IV III II	12 03 09	AE BY CO DH GI JP LU NQ RZ TW	EDD RRS JDC DGM
02	III IV II	04 13 17	BN CW DH EL FP GI JQ KM SY VZ	YYT APH YVF TAP
01	V I IV	07 06 11	AR BU CS DH EV FX GO IY LN MZ	KFS ZAP AZM WJQ

14- Téléchargement des ressources de cet ouvrage

L'archive « zip » disponible en téléchargement contient le classeur Excel simulant la machine Enigma ainsi que le programme Python de simulation de cet ouvrage.

Pour télécharger les ressources de cet ouvrage, merci de suivre les différentes étapes suivantes :

- Rendez-vous sur le site `www.joseouin.fr` ;
- Dans le menu, cliquez sur l'onglet « `Publications` », puis sélectionnez cet ouvrage pour ouvrir la page dédiée.
- Suivez les instructions de téléchargement affichées sur cette page dédiée.

Important : pour finaliser le téléchargement, vous devrez saisir l'un des codes de téléchargement indiqués dans le tableau de la page suivante.

Ressources complémentaires sur YouTube :
Des ressources complémentaires sont disponibles sur ma chaîne YouTube « Mathématiques Magiques **»**, dans la playlist intitulée **«** Enigma **»**.

Playlist « Enigma » sur la chaîne Mathématiques Magiques	
https://www.youtube.com/playlist?list=PLqWU5M-XIbA9tHAm0d6evdYnHcHiGWWTx	

Lien : `https://www.youtube.com/c/MathematiquesMagiques`

Cet ouvrage a été achevé en novembre 2024
Dépôt légal : novembre 2024
Déposé auprès de la BnF (Bibliothèque Nationale de France)