

José Ouin

Ingénieur INSA Toulouse

Ancien élève de l'ENS Cachan

Professeur Agrégé de Génie civil

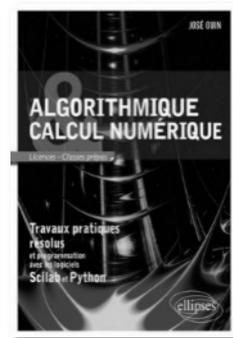
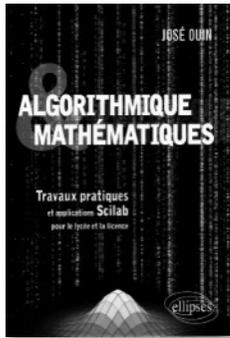
Professeur Agrégé de Mathématiques

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

© José OUIN – 2024 – <https://www.joseouin.fr>

Tous droits de traduction, de reproduction et d'adaptation réservés pour tous pays.

La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective" et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause, est illicite" (alinéa 1^{er} de l'article 40).

Cette représentation ou reproduction, par quelque procédé que ce soit, sans autorisation de l'auteur ou du Centre français du droit de copie (20, rue des Grands-Augustins 75006 Paris), constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal

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.....	9
1-1. Présentation de l'intérêt du chiffrement et de la sécurité des communications.....	9
1-1.1 Un besoin qui traverse les âges.....	9
1-1.2 La cryptographie comme rempart face aux menaces.....	9
1-1.3 Enigma : un cas d'école.....	10
1-1.4 L'importance croissante de la sécurité dans un monde numérique	10
1-2. Pourquoi l'étude d'Enigma reste pertinente aujourd'hui ?	11
1-2.1 Un trésor historique	11
1-2.2 Une étude pédagogique essentielle.....	11
1-2.3 Un modèle pour les systèmes de sécurité actuels.....	12
1-2.4 Un pont entre le passé et l'avenir	12
2- Exemples de cryptographie classique et quantique	13
2-1. Le code de César.....	13
2-1.1 Exemple de script Python du chiffrement de César	13
2-2. Cryptographie quantique :	15
2-2.1 L'intrication quantique :	15
3- Rappels historiques sur la naissance de la machine Enigma.....	16
3-1. Origines de la cryptographie avant Enigma : une vue d'ensemble des méthodes de chiffrement avant la création de la machine	16
3-1.1 Les débuts de la cryptographie : les méthodes classiques.....	16
3-1.2 Les cryptogrammes avancés de la Renaissance et au-delà.....	17
3-1.3 L'ère industrielle et la montée de la cryptographie mécanique	17
3-1.4 Le contexte de l'invention de l'Enigma.....	18
3-2. Le rôle d'Arthur Scherbius et l'invention de la machine Enigma.....	19
3-2.1 Qui était Arthur Scherbius ?.....	19
3-2.2 L'invention de la machine Enigma	19
3-2.3 Les composants de la machine Enigma	20
3-2.4 Un visionnaire en avance sur son temps	24
3-2.5 L'impact de l'invention de Scherbius.....	24
3-2.6 L'héritage de Scherbius	25
3-3. Les différentes versions de la machine Enigma (commerciale et militaire) .	25
3-3.1 La version commerciale	25
3-3.2 Les versions militaires.....	26
3-3.3 Les versions adaptées à d'autres pays.....	26

3-3.4	Autres versions et variantes	27
4-	L'armée allemande et l'utilisation d'Enigma	30
4-1.	L'adoption de la machine Enigma par les différentes branches de la Wehrmacht.....	30
4-1.1	L'adoption par l'Heer (armée de terre).....	30
4-1.2	L'adoption par la Luftwaffe (armée de l'air).....	31
4-1.3	L'adoption par la Kriegsmarine (marine de guerre)	31
4-1.4	Pourquoi l'armée allemande a adopté Enigma ?	32
4-2.	L'organisation des communications cryptées au sein de l'armée allemande ..	33
4-2.1	Procédures d'utilisation de la machine Enigma	33
4-2.2	Transmission et réception des messages.....	34
4-2.3	Hierarchie et centralisation des communications.....	35
4-2.4	Sécurité et gestion des carnets de clés	35
4-2.5	Problèmes et failles dans l'organisation des communications.....	36
4-3.	Failles humaines dans l'utilisation d'Enigma (erreurs de configuration, répétition de messages, etc.)	37
4-3.1	Erreurs de configuration des machines	37
4-3.2	Répétition de messages ou de configurations	38
4-3.3	Indicateurs faibles ou prévisibles	39
4-3.4	Utilisation non standardisée des protocoles	39
4-3.5	Failles dans les messages de routine	40
4-3.6	Capture de matériel et carnets de clés	40
4-4.	L'impact des modifications apportées par l'armée (nouveaux rotors, changements de procédure)	41
4-4.1	L'introduction de nouveaux rotors.....	41
4-4.2	Changements dans les procédures de chiffrement	42
4-4.3	L'impact de ces modifications sur la cryptanalyse alliée.....	42
4-4.4	Limites des modifications et erreurs humaines.....	43
5-	Principe de fonctionnement de la machine Enigma.....	44
5-1.	Description détaillée des composants : rotors, réflecteurs, tableau de connexions.....	44
5-1.1	Les rotors (ou rotors de chiffrement).....	44
5-1.2	Les anneaux des rotors (Ringstellung)	47
5-1.3	Les encoches des rotors.....	48
5-1.4	Effet du réglage de l'anneau sur l'avancement des rotors	51
5-1.5	Le réflecteur.....	52
5-1.6	Vue éclatée d'un rotor et de ses composants.....	53

5-1.7	Le tableau de connexions (plugboard).....	54
5-1.8	Interaction entre les composants	55
5-2.	Explication mathématique du fonctionnement d'Enigma (permutations et cycles)	56
5-2.1	Les permutations dans Enigma	56
5-2.2	Cycles et propriétés des permutations.....	57
5-2.3	Chiffrement dynamique et effet combiné	58
5-2.4	Nombre total de permutations.....	58
5-3.	Visualisation graphique du chiffrement d'une lettre.....	63
5-3.1	Description des connexions des différents rotors	63
5-3.2	Exemple N°1 : sans connexion au tableau de connexions.....	64
5-3.3	Exemple N°2 : avec connexion au tableau de connexions.....	65
5-3.4	Exemple N°3 : avec double avancée (double stepping).....	66
5-4.	Analyse des forces et des faiblesses du système Enigma.....	67
5-4.1	Forces du système Enigma :	67
5-4.2	Faiblesses du système Enigma	68
6-	Développement d'un simulateur Enigma en langage Python	71
6-1.	Description générale de la programmation de la machine Enigma	71
6-1.1	Composants fondamentaux de la machine Enigma.....	71
6-1.2	Structuration du programme en Python	71
6-2.	Script Python du simulateur de la machine Enigma	74
6-3.	Description des différentes fonctions de ce script Python	79
6-4.	Exemple d'utilisation de ce simulateur Enigma	82
7-	Développement d'un simulateur Enigma en langage VBA pour Excel	83
7-1.	Description générale de la programmation de la machine Enigma	83
7-2.	Macros VBA du simulateur de la machine Enigma	84
7-3.	Description des fonctions et procédures des macros en langage VBA.....	96
7-4.	Exemple d'utilisation de ce simulateur Enigma	101
8-	Exemples de messages chiffrés avec Enigma.....	102
8-1.	Définition des clés journalières et de message	102
8-1.1	Clé journalière.....	102
8-1.2	Clé de message.....	104

8-2.	Mode opératoire pour chiffrer et déchiffrer un message avec Enigma	104
8-2.1	Chiffrement par l'opérateur	104
8-2.2	Déchiffrement par le récepteur	105
8-3.	Pourquoi ce mode opératoire est-il particulièrement efficace ?.....	106
8-3.1	Clé de message non transmise directement.....	106
8-3.2	Calcul intermédiaire	106
8-3.3	Complexité accrue pour un attaquant.....	106
8-3.4	Renouvellement de la clé de message pour chaque transmission ...	106
8-4.	Message chiffré de Karl Dönitz	107
8-5.	Messages authentiques	108
8-5.1	Déchiffrement de la première partie du message	109
8-5.2	Déchiffrement de la deuxième partie du message.....	111
9-	Carnet de clés.....	113
10-	Outils et méthodes pour casser les codes Enigma	126
10-1.	Introduction aux techniques de cryptanalyse utilisées par les Alliés	126
10-1.1	Le travail pionnier des cryptanalystes polonais	126
10-1.2	Exploitation des faiblesses structurelles d'Enigma	127
10-1.3	La méthode « Banburismus »	127
10-1.4	Le « crib » ou repérage de mots prévisibles	127
10-1.5	La méthode du « rodding »	127
10-1.6	Utilisation de machines électromécaniques : la bombe de Turing	128
10-2.	La bombe de Turing : explication du fonctionnement et de la logique derrière cet outil de cryptanalyse	129
10-2.1	Origine et concept de la bombe	129
10-2.2	Problème à résoudre : casser Enigma.....	129
10-2.3	Principe de fonctionnement : « cribs » et répétitions	129
10-2.4	Structure et fonctionnement de la bombe	129
10-2.5	La logique derrière la bombe	130
10-2.6	Améliorations apportées par Gordon Welchman : le circuit diagonal	131
10-2.7	Impact et utilité de la bombe	131
11-	Les simulateurs de la machine Enigma.....	132
11-1.	py-Enigma	132
11-1.1	Procédure d'installation de la bibliothèque py-Enigma :	132
11-1.2	Exemple de script Python	133
11-1.3	Description du script	134

11-2. Simulateur Enigma pour Excel	135
11-2.1 Caractéristiques principales.....	135
11-2.2 Capture d'écran	136
11-3. Simulateur Cryptii.....	137
11-4. Enigma Simulator.....	138
11-5. Enigma Emulator.....	139
11-6. Enigma Machine Emulator	140
11-7. dCode – Machine Enigma	141
12- Déchiffrer Enigma : Exercices pratiques	142
12-1. Introduction aux exercices pratiques de déchiffrement	142
12-2. La table de clés journalières : outil essentiel pour déchiffrer les messages	
.....	143
12-3. Message : « Il changeait la vie »	144
12-3.1 Enoncé de l'exercice.....	144
12-3.2 Solution de l'exercice	145
12-4. Message : « Puisque tu pars ».....	146
12-4.1 Enoncé de l'exercice.....	146
12-4.2 Solution de l'exercice	147
12-5. Message : « 06 Juin 1944 »	148
12-5.1 Enoncé de l'exercice.....	148
12-5.2 Solution de l'exercice	149
12-6. Message à un officier sur le front	151
12-6.1 Enoncé de l'exercice.....	151
12-6.2 Solution de l'exercice	152
13- Les liens utiles.....	154
14- Téléchargement des ressources de cet ouvrage.....	155