

José Ouin

Ingénieur INSA Toulouse

Ancien élève de l'ENS Cachan

Professeur Agrégé de Génie civil

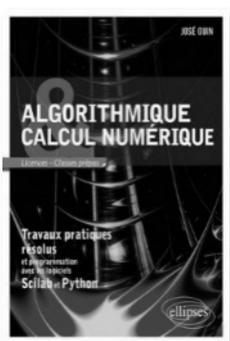
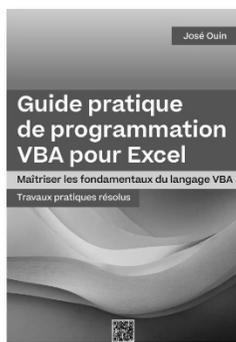
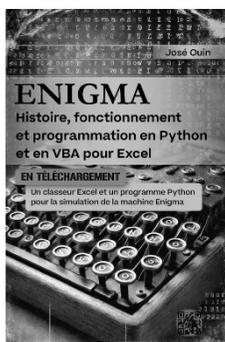
Professeur Agrégé de Mathématiques

Cryptographie et stéganographie appliquées :

Concepts et programmation en
Python



Du même auteur aux Editions Ellipses et sur Amazon



ISBN : 978-2-9593648-9-1

© 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

Depuis toujours, la cryptographie et la stéganographie m'émerveillent par leur capacité à transformer et dissimuler l'information, comme si un voile de mystère enveloppait les messages, rendant leur contenu inaccessible à tous sauf aux initiés. Mon intérêt pour cet art remonte à l'enfance, lorsque je découvrais avec fascination les énigmes et les codes dans les livres d'aventure. Ces jeux de l'esprit m'ont conduit à explorer des concepts bien plus profonds et techniques à l'âge adulte.

Ce qui me passionne particulièrement dans la stéganographie, c'est son côté presque magique : le simple fait de cacher un message ou même un fichier entier dans une image banale me semble être une prouesse digne des meilleurs prestidigitateurs. Ce processus, qui repose à la fois sur des mathématiques élégantes et sur une maîtrise des outils numériques, m'a souvent donné l'impression de manipuler l'invisible.

Ce livre est né de cette passion et de l'envie de partager avec d'autres cet univers fascinant. Il ne s'agit pas seulement d'un manuel technique ou d'un guide pratique ; c'est aussi une invitation à plonger dans un monde où les bits et les pixels peuvent devenir des gardiens de secrets.

Que vous soyez curieux de comprendre comment fonctionne un chiffre de César, désireux de chiffrer des messages avec AES, ou intrigué par l'idée d'insérer un fichier dans une image sans que cela soit détectable, cet ouvrage est conçu pour vous guider pas à pas. J'ai voulu l'écrire comme un compagnon de route, qui vous aidera à maîtriser les bases tout en vous donnant envie d'explorer encore davantage.

En lisant ces pages, j'espère transmettre non seulement des connaissances, mais aussi une part de cet émerveillement qui m'habite à chaque fois que je découvre une nouvelle technique pour coder, crypter ou cacher l'information.

Bonne lecture et bienvenue dans l'univers fascinant des secrets numériques !



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.....	9
1-1. Pourquoi apprendre la cryptographie et la stéganographie ?.....	9
1-2. Une approche pratique et pédagogique.....	9
1-3. Ce que ce livre n'est pas.....	10
1-4. Pour qui est cet ouvrage ?.....	10
2- Installation de Python et de l'éditeur PyScripter	11
2-1. Installation de Python.....	11
2-1.1 Télécharger Python.....	11
2-1.2 Installer Python.....	11
2-1.3 Gestionnaire de paquets pip.....	12
2-2. Editeur PyScripter.....	12
2-2.1 Étapes d'installation.....	12
2-2.2 Installation d'une bibliothèque Python :.....	14
2-2.3 Pourquoi choisir PyScripter ?.....	15
3- Bases binaires : comprendre bits, octets et encodages.....	16
3-1. Bit.....	16
3-2. Octet.....	16
3-3. Byte.....	16
3-4. Binaire.....	16
3-5. Str.....	17
3-6. ASCII.....	17
3-7. Hexadécimal.....	17
3-8. Encodage.....	17
3-9. Table ASCII.....	17
3-10. Opérations logiques.....	17
3-11. Encodage UTF-8.....	18
3-12. Encodage Base64.....	18

4- Prérequis essentiels en Python	19
4-1. Introduction à <code>if __name__ == '__main__':</code> : rôle et utilisation.....	19
4-2. Les bibliothèques Python	22
4-2.1 cryptography	22
4-2.2 pycryptodome	23
4-2.3 hashlib	23
4-2.4 hmac	23
4-2.5 base64	23
4-2.6 pillow	24
4-2.7 numpy	24
4-2.8 scipy	24
4-2.9 bitarray	24
4-2.10 matplotlib	25
4-2.11 scikit-image	25
4-2.12 random et secrets	25
4-3. Les fonctions Python	26
4-3.1 f-string	26
4-3.2 ord	27
4-3.3 chr	27
4-3.4 zip	27
4-3.5 enumerate	28
4-3.6 len	30
4-3.7 join	30
4-3.8 split	30
4-3.9 range	31
4-3.10 map	31
4-3.11 filter	32
4-3.12 reversed	32
4-3.13 random.choice	33
4-3.14 random.sample	33
4-3.15 hashlib	34
4-3.16 itertools.cycle	35
4-3.17 all et any	35
4-3.18 Counter	36
4-3.19 zip_longest	36

4-4.	Notions sur les nombres binaires et hexadécimaux	37
4-4.1	Bases numériques : concepts essentiels	37
4-4.2	Conversion entre bases numériques	37
4-4.3	Opérations binaires essentielles	38
4-5.	Gestion des bytes et des encodages	42
4-5.1	Les concepts de base	42
4-5.2	Pourquoi encoder une chaîne en bytes ?	43
4-5.3	Manipulation des bytes	44
4-5.4	Conversion entre formats	45
5-	Prérequis essentiels en cryptographie et stéganographie	49
5-1.	Bases numériques appliquées à la cryptographie	49
5-1.1	Représentation en base 2 (binaire)	49
5-1.2	Représentation en base 16 (hexadécimale)	51
5-2.	L'opérateur XOR : principe et utilisation	54
5-2.1	Définition et fonctionnement	54
5-2.2	XOR comme outil cryptographique	55
5-2.3	Propriétés fondamentales de XOR	57
5-3.	Encodage Base64 : introduction et utilisation dans la transmission de données	60
5-3.1	Définition de l'encodage base64	60
5-3.2	Fonctionnement de l'encodage Base64 :	60
5-3.3	Rôles et applications pratiques	61
5-3.4	Limites et particularités du codage Base64	63
5-4.	Concepts mathématiques de base pour la cryptographie	64
5-4.1	Théorie des nombres	64
5-4.2	Algèbre modulaire	67
5-4.3	Génération aléatoire des clés	71
5-5.	Principes de la stéganographie	73
5-5.1	Distinction entre cryptographie et stéganographie	73
5-5.2	Introduction aux formats de fichiers courants	74
5-5.3	Techniques basiques de dissimulation	79
6-	Chiffrements classiques	84
6-1.	Chiffrement de César	84
6-1.1	Comprendre les bases du chiffrement	84
6-1.2	Implémentation en Python	84

6-2.	Chiffrement de Vigenère	86
6-2.1	Description.....	86
6-2.2	Implémentation en Python.....	86
6-3.	Chiffrement par transposition	91
6-3.1	Transposition en tableau à colonnes fixes.....	91
6-3.2	Implémentation en Python.....	92
6-4.	Carré de Polybe	95
6-4.1	Présentation du principe	95
6-4.2	Implémentation en Python.....	96
6-5.	Chiffrement affine.....	98
6-5.1	Description de la méthode.....	98
6-5.2	Implémentation en Python.....	99
7-	Chiffrements modernes simplifiés	102
7-1.	Chiffrement XOR.....	102
7-1.1	Principe du chiffrement XOR	102
7-1.2	Implémentation en Python.....	103
7-1.3	Applications modernes du XOR.....	105
7-2.	Chiffrement XOR et encodage Base64.....	106
7-2.1	Chiffrement XOR et représentation binaire.....	106
7-2.2	Encodage Base64 pour lisibilité et transmission.....	107
7-3.	Chiffrement par blocs (exemple simplifié d'AES).....	110
7-3.1	Concepts clés	110
7-3.2	Implémentation en Python.....	110
7-4.	Chiffrement de Hill.....	114
7-4.1	Principe du chiffrement de Hill	114
7-4.2	Implémentation en Python.....	114
7-5.	Chiffrement de Vernam.....	121
7-5.1	Introduction au chiffrement parfait	121
7-5.2	Implémentation en Python.....	121
8-	Concepts de chiffrement : asymétrique et symétrique.....	126
8-1.	Chiffrement RSA	126
8-1.1	Détermination d'une clé publique et d'une clé privée	126
8-1.2	Processus de chiffrement et de déchiffrement d'une lettre.....	127
8-1.3	Implémentation en Python.....	128

8-2.	Echange de clés Diffie-Hellman	134
8-2.1	Les bases théoriques.....	134
8-2.2	Implémentation en Python	135
8-2.3	Transformation d'une clé partagée en une clé AES utilisable.....	138
8-3.	Chiffrement symétrique avec AES	140
8-3.1	Introduction au chiffrement symétrique.....	140
8-3.2	Présentation de l'algorithme AES	140
8-3.3	Implémentation en Python	141
8-3.4	Chiffrement et déchiffrement d'un fichier avec AES en mode CBC ..	143
8-3.5	Générateur de clés AES sécurisé.....	146
9-	Stéganographie : L'art de dissimuler des messages	149
9-1.	Introduction à la stéganographie	149
9-1.1	Qu'est-ce que la stéganographie ?	149
9-1.2	Cryptographie vs Stéganographie	149
9-1.3	Applications pratiques de la stéganographie	150
9-1.4	Pourquoi choisir les images comme support ?	150
9-1.5	Limitations et défis de la stéganographie.....	150
9-2.	Principe de la stéganographie dans les images.....	151
9-2.1	Structure des fichiers images numériques.....	151
9-2.2	Utilisation des bits de poids faible (LSB).....	152
9-2.3	Exemple illustratif.....	152
9-3.	Algorithme de base : Cacher un message texte dans une image BMP	154
9-3.1	Étapes de l'algorithme	154
9-3.2	Implémentation en Python pour cacher un message.....	155
9-3.3	Implémentation en Python pour extraire un message.....	158
9-4.	Étendre le concept aux images PNG	162
9-4.1	Gestion de la compression sans perte : caractéristiques et contraintes	162
9-4.2	Adaptation de l'algorithme pour le format PNG.....	162
9-4.3	Implémentation en Python : Dissimuler un message dans une image PNG	163
9-4.4	Implémentation en Python : Extraire un message depuis une image PNG	167

9-5.	Cas pratique N°1 : Ecriture et extraction d'une image cachée.....	170
9-5.1	Introduction à l'idée d'un « payload » plus complexe.....	170
9-5.2	Comment chaque pixel de l'image cachée est-il intégré dans une image porteuse ?	170
9-5.3	Implémentation en Python	170
9-5.4	Gestion de la transparence dans les images PNG	175
9-6.	Cas pratique N°2 : Intégration et extraction d'un fichier dans une image PNG	181
9-6.1	Ecriture : description des différentes étapes.....	181
9-6.2	Implémentation en Python : Intégration d'un fichier dans une image PNG	181
9-6.3	Extraction : description des différentes étapes	185
9-6.4	Implémentation en Python : Extraction d'un fichier depuis une image PNG	186
9-7.	Cas pratique N°3 : Intégration et extraction d'un fichier chiffré par XOR dans une image PNG.....	189
9-7.1	Script pour chiffrer et intégrer un fichier dans une image PNG.....	189
9-7.2	Script pour extraire et déchiffrer un fichier depuis une image PNG..	192
9-8.	Cas pratique N°4 : Intégration et extraction d'un fichier chiffré par AES dans une image PNG.....	195
9-8.1	Script Python pour chiffrer et intégrer un fichier dans une image PNG	195
9-8.2	Script Python pour extraire et déchiffrer un fichier depuis une image PNG	199
10-	Annexes	203
10-1.	Table ASCII.....	203
10-2.	Table Base64	207
11-	Téléchargement des ressources de cet ouvrage	209