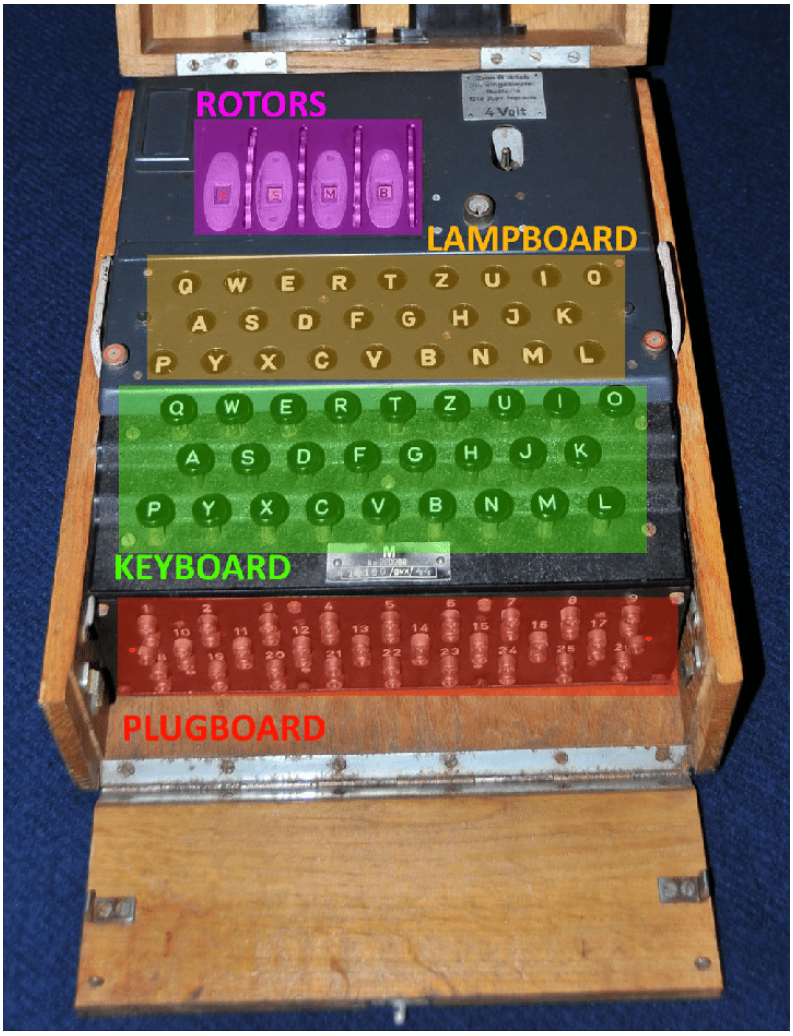


Projet Enigma :

Introduction et description :

Dans le cadre du module 242, il va vous être demandé de reproduire la machine Enigma qui a été utilisée par les Allemands pour chiffrer les communications pendant la WW2.

Tout au long du labo, vous allez devoir documenter vos étapes et répondre à certaines questions. Cette partie correspond à la première partie du projet et sera noté.

Spécifications techniques :

Voici les différents points à respecter pour ce labo :

- Développement en python uniquement en utilisant la librairie **python-enigma**.
- Respecter les différentes étapes du projet et les documenter.

1ère étape fonctionnement Enigma :

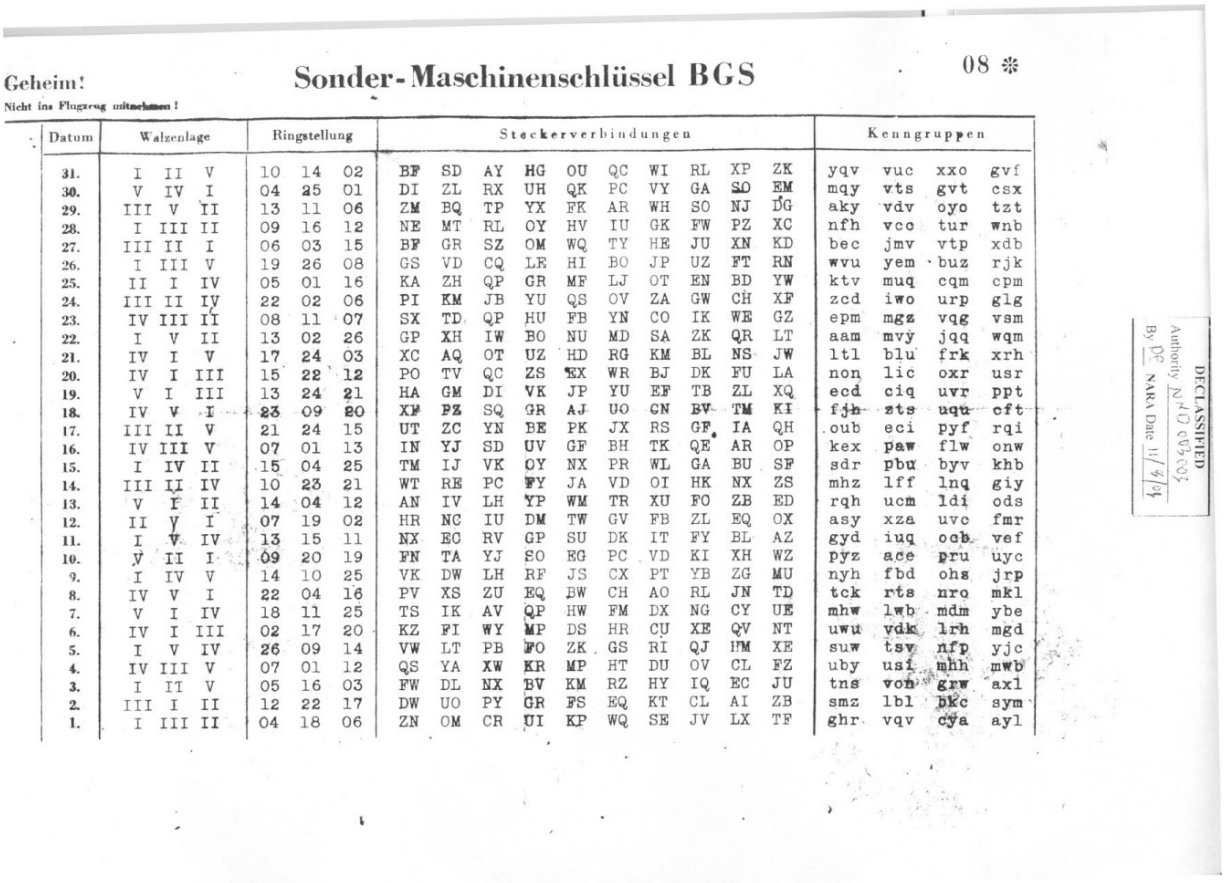
Expliquer le fonctionnement de la machine Enigma.

- Qu'est-ce que l'entrée et la sortie de la machine Enigma?
- Comment fonctionne le tableau de connexion ? Combien y'a-t-il de paires de lettre qui sont reliées entre elles ?
- Qu'est-ce qu'un rotor ? Combien y'en a-t-il ? Combien sont utilisé pour chiffrer / déchiffrer les messages ?
- À quoi sert le réflecteur ? Quel était son problème ?

2ème étape création d'une fonction de chiffrement avec Enigma :

Voici un exemple de configuration de la machine Enigma qui a été utilisé pendant la 2ème Guerre mondiale.

- Expliquer à quoi correspond Walzenlage, Ringstellung, Stockerverbindungen et Kenngruppen.



Geheim!
Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

08 ❊

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mqy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vco tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LE HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvy jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XP PZ SQ GR AJ UO GN BV TM KI	fjh zts uqu cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub eci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EC RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ HM XE	suw tsv nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usi mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

3ème étape création d'une fonction chiffrer avec Enigma :

Pour la partie 3 & 4 nous utiliserons la configuration de la machine ci-dessus en sachant que les tests se feront avec la ligne 11 qui correspond à la date du 11 novembre. De plus nous utiliserons la première colonne de la Kenngruppen (nous nous situons donc entre minuit et 6h du matin). Pour finir nous utiliserons toujours le réflecteur B.

Vous trouvez de la documentation sur l'utilisation de la libraire ici :
https://readthedocs.org/projects/py-enigma/downloads/pdf/latest/

Créer une fonction python chiffrer() qui prend en paramètres les rotors, le réflecteur, disposition des rotors, le tableau de connexion entre les lettre, la clé et le texte en clair. Cette fonction retourne le résultat chiffré.

Chiffrer le message suivant : « Les troupes britanniques sont entrees a Cuxhaven a quatorze heures le six mai Desormais tout le trafic radio cessera je vous souhaite le meilleur Fermeture pour toujours tout le meilleur au revoir. »

À rendre :

- screenshot du message chiffré dans la documentation.

4ème étape création d'une fonction déchiffrer avec Enigma :

Créer une fonction python dechiffrer() qui prend en paramètres les rotors, le réflecteur, disposition des rotors, le tableau de connexion entre les lettre, la clé et le texte chiffrer. Cette fonction retourne le texte en claire.

À rendre :

- screenshot du message déchiffré dans la documentation (on devrait avoir le même message)

5ème étape décrypter ce message par bruteforce :

Voici le message que vous avez subtilement entendu à la radio :

GRWYGBHCZRZKAOQDWJYKQSLNKGINIKUAHAUFKUKGRNVKUWOFTVNCKHDAYWKJBJYVWFFWNVXM
LDGXARISRQJQOJGLEAYWNUWVDYUACPBMSJGRSOHAYRLINRHIPCBHJAZO

Ce que vous savez :

- Les allemands commencaient toujours le premier message de la journée en annonçant le Wetterbericht soit la météo. Dans ce message ça correspond au mot « meteorologie ».
- La disposition des rotors est la suivante : 19 6 8
- Les lettres sont branchées de la façon suivante : GH QW TZ RO IP AL SJ DK CN YM

Vous allez devoir créer une fonction bruteforce qui va tester toutes les possibilités restantes afin de tester toutes les combinaisons de rotors différentes (3 parmi les 5) en testant toute les clés possibles (3 caractères). La seule façon va donc d'être de comparer une partie de l'entrée avec un bout de la sortie qui est connu. Une fois que vous aurez trouvé les rotors utilisés & la clé vous pourrez déchiffrer tout le message.

À rendre :

- Combien de possibilités peut-on tester au maximum avec un tel système (détaillez les calculs)
- Quelle est la clé et quels sont les rotors utilisés (screenshot)
- Quel est le message en claire (screenshot)

6ème étape déploiement sur le Raspberry

Déployez votre programme python (fonction chiffrer(), dechiffrer(), bruteforce() avec les tests)sur le Raspberry et vérifier son bon fonctionnement, merci de m'indiquer dans la documentation sur quelle carte SD et où (path) se trouve votre programme.

Informations sur le rendu :

Suite « au progrès » de ce que certain humain appelle « intelligence artificielle », je me réserve le droit d'interroger oralement certains binômes sur le résultat produit. Une note de 1 sera attribuée si votre rendu n'est pas le fruit de votre propre travail.

Quand : à définir selon l'avancement des binômes.

Combien : par groupe de 2.

Quoi : Documentation et informations concernant la carte SD + path du Raspberry.