Enigma

Épreuve pratique d'algorithmique et de programmation
Concours commun des Écoles normales supérieures

Durée de l'épreuve: 3 heures 30 minutes

Juin/Juillet 2015

ATTENTION !

N'oubliez en aucun cas de recopier votre u_0
à l'emplacement prévu sur votre fiche réponse

Important.

Il vous a été donné un numéro u_0 qui servira d'entrée à vos programmes. Les réponses attendues sont généralement courtes et doivent être données sur la fiche réponse fournie à la fin du sujet. À la fin du sujet, vous trouverez en fait deux fiches réponses. La première est un exemple des réponses attendues pour un $\widetilde{u_0}$ particulier (précisé sur cette même fiche et que nous notons avec un tilde pour éviter toute confusion!). Cette fiche est destinée à vous aider à vérifier le résultat de vos programmes en les testant avec $\widetilde{u_0}$ au lieu de u_0. Vous indiquerez vos réponses (correspondant à votre u_0) sur la seconde et vous la remettrez à l'examinateur à la fin de l'épreuve.

En ce qui concerne la partie orale de l'examen, lorsque la description d'un algorithme est demandée, vous devez présenter son fonctionnement de façon schématique, courte et précise. Vous ne devez en aucun cas recopier le code de vos procédures!

Quand on demande la complexité en temps ou en mémoire d'un algorithme en fonction d'un paramètre n, on demande l'ordre de grandeur en fonction du paramètre, par exemple: $O(n^2)$, $O(n \log n)$,...

Il est recommandé de commencer par lancer vos programmes sur de petites valeurs des paramètres et de ***tester vos programmes sur des petits exemples que vous aurez résolus préalablement à la main ou bien à l'aide de la fiche réponse type fournie en annexe***. Enfin, il est recommandé de lire l'intégralité du sujet avant de commencer afin d'effectuer les bons choix de structures de données dès le début.

L'objectif de ce sujet est d'étudier la machine Enigma, utilisée par l'Allemagne nazie et ses alliés pour chiffrer les communications entre leurs officiers afin d'en assurer la confidentialité, et sa cryptanalyse qui a contribué à assurer la victoire alliée en 1945.

Ce sujet se divise en quatre parties. Les deux dernières, présentant chacune une cryptanalyse d'Enigma, sont relativement indépendantes, même si toutes deux dépendent des deux premières parties du sujet.

Pour tous entiers a et b avec $b > 0$, on notera $a \bmod b$ le reste de la division euclidienne de a par b, autrement dit l'unique entier r avec $0 \leq r < b$ tel qu'il existe un entier q satisfaisant $a = bq + r$. De plus, pour tout $x \in \mathbb{R}$, on notera $\lfloor x \rfloor$ la partie entière de x, c'est-à-dire l'unique entier n tel que $n \leq x < n + 1$.

1 Permutations aléatoires et caractéristiques

À partir de la valeur initiale u_0 qui vous a été fournie, on définit récursivement deux familles d'entiers positifs $(u_i)_{i\geq 0}$ et $(v_{i,j})_{i\geq 0, j\geq 0}$ par

$$u_{i+1} = (2035 \cdot u_i) \bmod m \qquad \text{et} \qquad v_{i,j} = \left\lfloor \frac{(j+1) \cdot u_{i+j}}{m} \right\rfloor,$$

pour tous i et $j \geq 0$, et avec $m = 2^{20} + 7$.

Question 1 *Donnez les valeurs de u_i et $v_{i,j}$ pour les couples (i, j) suivants :*
a) $(10, 10)$, ***b)*** $(1000, 20)$, ***c)*** $(100000, 30)$.

Pour tous $n > 0$ et $i \geq 0$, on définit la fonction $\pi_{n,i}$ de l'ensemble $\{0, 1, \ldots, n-1\}$ dans lui-même comme le résultat de l'algorithme suivant, qui opère sur une fonction $x : \{0, 1, \ldots, n-1\} \to \{0, 1, \ldots, n-1\}$. Initialement, x est la fonction nulle. Pour j variant de 0 à $n-1$, on remplace $x(j)$ par $x(v_{i,j})$, puis on remplace $x(v_{i,j})$ par j. La sortie de l'algorithme est la fonction x à l'issue des n itérations.
Remarque : On admettra pour la suite que la fonction $\pi_{n,i}$ est une permutation de l'ensemble $\{0, 1, \ldots, n-1\}$, pour tous $n > 0$ et $i \geq 0$.

Question 2 *Donnez les valeurs de $\pi_{n,i}(0)$, $\pi_{n,i}(1)$ et $\pi_{n,i}(n-1)$ pour les couples (n, i) suivants :*
a) $(5, 10)$, ***b)*** $(50, 1000)$, ***c)*** $(500, 100000)$.

On rappelle que toute permutation d'un ensemble fini peut s'écrire de manière unique comme un produit de cycles à supports disjoints. Ainsi, par exemple, la permutation π de $\{0, 1, 2, 3\}$ qui envoie $0 \mapsto 3$, $1 \mapsto 1$, $2 \mapsto 0$ et $3 \mapsto 2$ se décompose en $\pi = (032)(1)$.
Pour toute permutation π d'un ensemble fini, on appelle alors caractéristique de π, que l'on note $\chi(\pi)$, la liste formée par les longueurs des cycles qui la composent (y compris les cycles de longueur 1), triée par ordre croissant. Ainsi, dans l'exemple précédent, on a $\chi(\pi) = [1, 3]$.

Question 3 *Donnez la caractéristique de $\pi_{n,i}$ pour les couples (n, i) suivants :*
a) $(5, 10)$, ***b)*** $(50, 1000)$, ***c)*** $(500, 100000)$.

Question à développer pendant l'oral 1 *Quel algorithme avez-vous utilisé pour répondre à la question précédente ? Quelle est sa complexité ?*

2 La machine Enigma

2.1 Fonctionnement général

Enigma est une machine électro-mécanique qui permet de chiffrer et déchiffrer des messages. Les messages sont des suites finies de lettres de l'alphabet usuel $\mathcal{A} = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$. On note φ la bijection de l'ensemble $\{0, 1, \ldots, 25\}$ dans $\mathcal{A}$ donnée par $\varphi(0) = \mathtt{A}$, $\varphi(1) = \mathtt{B}$, … et $\varphi(25) = \mathtt{Z}$.
La machine comporte cinq composants principaux, reliés entre eux par des nappes de 26 fils électriques (un par lettre de l'alphabet). Ces composants sont identifiés par les lettres de Ⓐ à Ⓔ sur la photographie figure 1. Les photographies de certains détails d'Enigma sont données figures 2 et 3. Enfin, la figure 4 représente schématiquement une machine Enigma avec un alphabet réduit à quatre lettres.

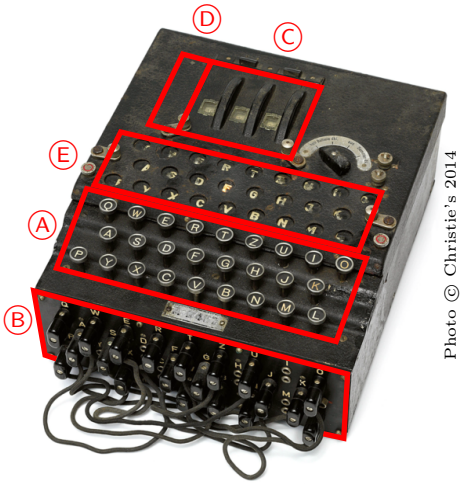


FIGURE 1 – Vue d'ensemble d'Enigma.

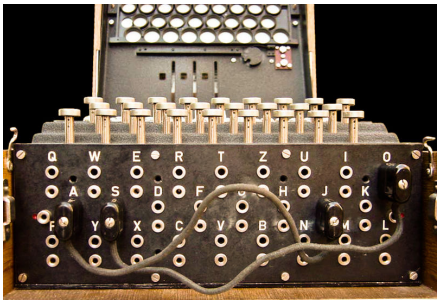


FIGURE 2 – Le tableau de connexions.

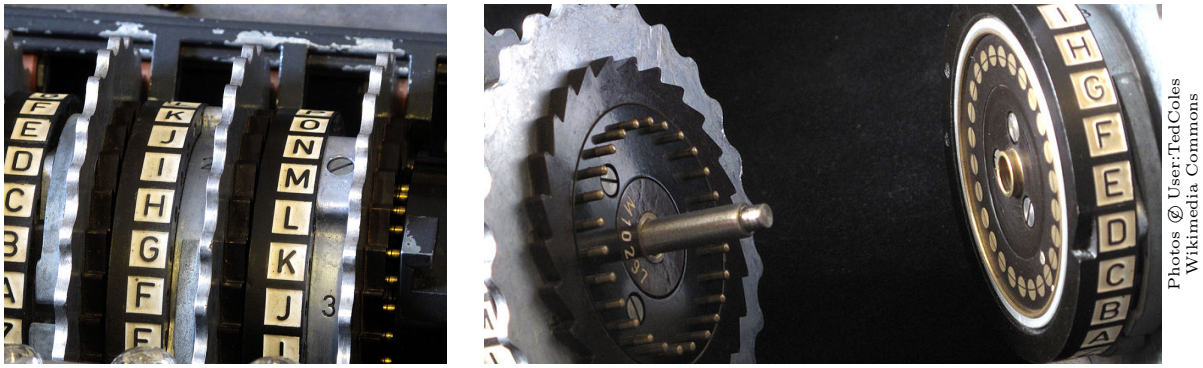


FIGURE 3 – Les rotors : groupe de trois rotors installés dans la machine (à gauche) ; interface électrique entre deux rotors (à droite).

Le chiffrement d'une lettre par Enigma s'opère de la manière suivante :

① Lorsque l'opérateur appuie sur la touche du clavier Ⓐ correspondant à la lettre qu'il souhaite chiffrer (P dans l'exemple de la figure 4), un courant électrique s'établit sur le fil correspondant à cette lettre.

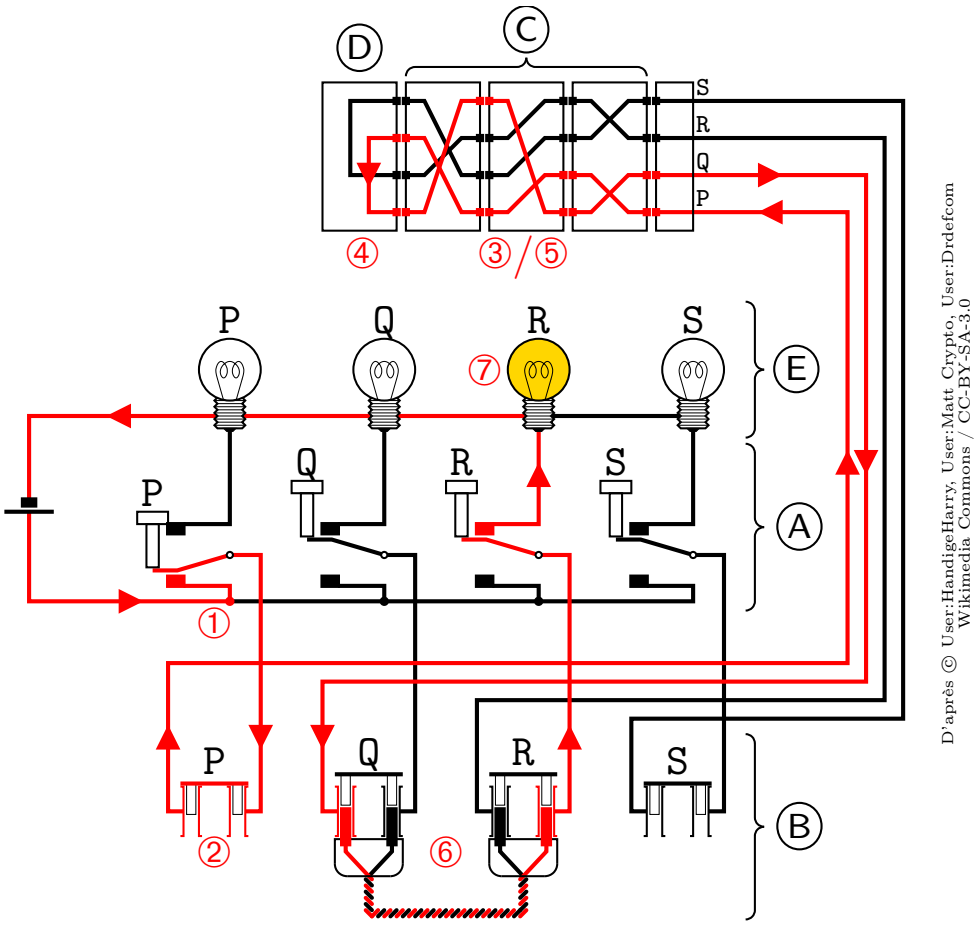


FIGURE 4 – Schéma de fonctionnement électrique d'Enigma.

② Le courant traverse alors le tableau de connexions Ⓑ (voir figure 2), qui permet, grâce à des câbles croisés, d'échanger certaines paires de lettres distinctes de l'alphabet. Dans notre exemple, la lettre `P` n'est pas affectée et ressort inchangée.

③ Le courant traverse alors une suite de m rotors Ⓒ (voir figure 3), de droite à gauche. Chacun de ces rotors réalise une permutation des lettres de l'alphabet. Dans l'exemple avec $m = 3$ rotors de la figure 4, la lettre `P` est ainsi successivement transformée en `Q`, puis en `P` et enfin en `R`.

④ Le courant traverse ensuite le réflecteur Ⓓ, qui réalise aussi une permutation fixe de l'alphabet (transformant `R` en `P` ici), et renvoie le courant à travers les rotors.

⑤ Le courant traverse à nouveau les rotors, mais en sens inverse, de la gauche vers la droite. Tour à tour, la lettre `P` devient ainsi `S`, puis `P` et enfin `Q`.

⑥ Sur son trajet de retour, le courant traverse ensuite à nouveau le tableau de connexions, qui échange ici les lettres `Q` et `R`.

⑦ Enfin, le courant atteint un panneau Ⓔ constitué de 26 lampes étiquetées par les lettres de l'alphabet, et allume l'une d'entre elles : la lampe ainsi allumée indique à l'opérateur la lettre chiffrée (`R` dans notre exemple).

Le tableau de connexions peut accueillir de 0 à 13 câbles croisés, chacun effectuant une transposition entre deux lettres. Le nombre de câbles utilisés est noté n.

Les rotors, comme leur nom l'indique, peuvent tourner sur eux-mêmes autour d'un axe. La position de chaque rotor r est dénotée par une lettre $p \in \mathcal{A}$ de l'alphabet. Si l'on note σ_r la permutation de l'alphabet réalisée par le rotor r en position $p = \texttt{A}$ lorsque le courant le traverse de droite à gauche, alors le même rotor en position `B` réalisera la permutation $\rho^{-1} \circ \sigma_r \circ \rho$, et ainsi de suite pour les positions suivantes, où $\rho : \mathcal{A} \to \mathcal{A}$ désigne la permutation circulaire qui à chaque lettre associe la suivante, et qui à `Z` associe `A`.
La machine Enigma est livrée avec cinq rotors, nommés I, II, III, IV et V, parmi lesquels les m rotors utilisés pour le chiffrement sont choisis. On note $\mathcal{R} = \{\text{I}, \text{II}, \text{III}, \text{IV}, \text{V}\}$ l'ensemble de ces rotors, et on les numérote de 0 à 4 grâce à la bijection ψ telle que $\psi(0) = \text{I}$, $\psi(1) = \text{II}$, … et $\psi(4) = \text{V}$.
Les permutations réalisées par ces rotors (lorsqu'ils sont en position `A` et que le courant les traverse de droite à gauche) ainsi que celle réalisée par le réflecteur (nommé B) sont données dans le tableau suivant :

	Perm.	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 I	σ_{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
Rotor II	σ_{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
Rotor III	σ_{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
Rotor IV	σ_{IV}	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B
Rotor V	σ_{V}	V	Z	B	R	G	I	T	Y	U	P	S	D	N	H	L	X	A	W	M	J	Q	O	F	E	C	K
Réflecteur B	σ_{B}	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T

2.2 Configuration

On appelle configuration de la machine la donnée des informations suivantes :

- une suite $R = (r_0, r_1, \ldots, r_{m-1}) \in \mathcal{R}^m$ de m rotors distincts parmi les cinq disponibles ; ces rotors seront installés dans la machine, de gauche à droite dans l'ordre donné ;
- une suite $P = (p_0, p_1, \ldots, p_{m-1}) \in \mathcal{A}^m$ de m lettres désignant les positions des rotors, de gauche à droite ;
- un ensemble $C = \{\{c_{j,0}, c_{j,1}\} \mid c_{j,0}, c_{j,1} \in \mathcal{A},\ c_{j,0} \neq c_{j,1} \text{ et } 0 \leq j < n\}$ de n paires de lettres disjointes deux à deux échangées par un câble croisé sur le tableau de connexions.

Le triplet $K = (R, P, C)$ désigne la configuration ainsi définie.
Par exemple, pour $m = 3$ rotors et $n = 10$ connexions, une configuration possible est donnée par

$$\begin{cases} R = (\text{III}, \text{II}, \text{V}), \\ P = (\texttt{T}, \texttt{H}, \texttt{X}) \text{ et} \\ C = \{\{\texttt{A}, \texttt{E}\}, \{\texttt{B}, \texttt{Q}\}, \{\texttt{C}, \texttt{H}\}, \{\texttt{D}, \texttt{U}\}, \{\texttt{F}, \texttt{L}\}, \{\texttt{G}, \texttt{P}\}, \{\texttt{I}, \texttt{X}\}, \{\texttt{J}, \texttt{O}\}, \{\texttt{M}, \texttt{N}\}, \{\texttt{W}, \texttt{Y}\}\}. \end{cases}$$

Pour présenter les résultats, on pourra aussi utiliser la notation suivante, plus compacte :

$$K = (\text{III-II-V},\ \texttt{THX},\ \texttt{AE BQ CH DU FL GP IX JO MN WY}).$$

Question à développer pendant l'oral 2 *Donnez le nombre de configurations possibles pour R, P et C en fonction de m et n. Donnez un ordre de grandeur du nombre total de configurations (R, P, C) possibles pour $m = 3$ et $n = 10$. Cela vous semble-t-il possible pour un ordinateur d'énumérer toutes ces configurations ? En combien de temps ?*

À m et n fixés, nous considérerons dans la suite les configurations pseudo-aléatoires $K_i = (R_i, P_i, C_i)$, pour tout $i \geq 0$, générées comme suit :

$$\begin{cases} R_i = (\psi(\pi_{5,i}(0)), \psi(\pi_{5,i}(1)), \ldots, \psi(\pi_{5,i}(m-1))), \\ P_i = (\varphi(u_{i+5} \bmod 26), \varphi(u_{i+6} \bmod 26), \ldots, \varphi(u_{i+m+4} \bmod 26)) \text{ et} \\ C_i = \{\{\varphi(\pi_{26,i+10}(2j)), \varphi(\pi_{26,i+10}(2j+1))\} \mid 0 \leq j < n\}. \end{cases}$$

2.3 Étude de la permutation

Afin de distinguer les différentes permutations de l'alphabet réalisées au sein de la machine Enigma, nous notons, pour toute configuration $K = (R, P, C)$:

- σ_C la permutation de $\mathcal{A}$ réalisée par le tableau de connexions,
- $\sigma_{R,P}$ la permutation réalisée par le groupe de m rotors R en position P lorsque le courant les traverse de droite à gauche, et
- σ_K la permutation complète réalisée par la machine Enigma en configuration K.

Question à développer pendant l'oral 3 *Étant donnée une configuration $K = (R, P, C)$ de la machine avec m rotors et n connexions, avec $R = (r_j)_{0 \leq j < m}$, $P = (p_j)_{0 \leq j < m}$ et $C = \{\{c_{j,0}, c_{j,1}\} \mid 0 \leq j < n\}$, montrez que*

$$\sigma_C = \prod_{j=0}^{n-1} (c_{j,0} c_{j,1}),$$

$$\sigma_{R,P} = \rho^{-\varphi^{-1}(p_0)} \circ \sigma_{r_0} \circ \rho^{\varphi^{-1}(p_0)} \circ \cdots \circ \rho^{-\varphi^{-1}(p_{m-1})} \circ \sigma_{r_{m-1}} \circ \rho^{\varphi^{-1}(p_{m-1})}, \text{ et}$$

$$\sigma_K = \sigma_C^{-1} \circ \sigma_{R,P}^{-1} \circ \sigma_{\mathrm{B}} \circ \sigma_{R,P} \circ \sigma_C.$$

Dans la suite, on notera aussi $\hat{\sigma}_{R,P} = \sigma_{R,P}^{-1} \circ \sigma_{\mathrm{B}} \circ \sigma_{R,P}$, ce qui donne $\sigma_K = \sigma_C^{-1} \circ \hat{\sigma}_{R,P} \circ \sigma_C$.

Question 4 *Pour cette question, on fixe $n = 0$ afin d'ignorer l'influence du tableau de connexions (c'est-à-dire, on prend $\sigma_C = \mathrm{Id}$). Pour chacun des couples (m, i) suivants, donnez la valeur des lettres $x = \sigma_{R_i,P_i}(\mathtt{A})$, $y = \sigma_{\mathrm{B}}(x)$, et enfin $z = \sigma_{R_i,P_i}^{-1}(y) = \sigma_{K_i}(\mathtt{A})$.*
a) $(1, 10)$, ***b)*** $(2, 100)$, ***c)*** $(3, 1000)$.

Question 5 *Pour chacun des triplets (m, n, i) suivants, donnez la valeur des lettres $x = \sigma_C(\mathtt{A})$, $y = \hat{\sigma}_{R_i,P_i}(x)$, et enfin $z = \sigma_C^{-1}(y) = \sigma_{K_i}(\mathtt{A})$.*
a) $(1, 5, 20)$, ***b)*** $(2, 8, 200)$, ***c)*** $(3, 10, 2000)$.

Question à développer pendant l'oral 4 *Montrez que la permutation σ_K est une involution, c'est-à-dire que $\sigma_K^{-1} = \sigma_K$, et qu'elle n'admet pas de point fixe, c'est-à-dire qu'il n'existe pas de lettre $x \in \mathcal{A}$ telle que $\sigma_K(x) = x$.*

2.4 Avancement des rotors

Si la position initiale des rotors est choisie par l'opérateur, ceux-ci ne restent néanmoins pas fixes au cours du chiffrement d'un message.
En effet, à chaque fois que l'opérateur appuie sur une touche du clavier, le rotor de droite avance d'un cran, c'est-à-dire que sa position est remplacée par la lettre qui suit dans l'alphabet. Ainsi, si le rotor de droite était en position p, il passera en position $\rho(p)$.
De plus, à la manière d'un odomètre (compteur kilométrique), à chaque fois qu'un rotor r passe d'une certaine position d'entraînement κ_r à la suivante, le rotor situé directement à sa gauche avance aussi immédiatement d'une position. Les positions d'entraînement κ_{I}, κ_{II}, … et κ_{V} des cinq rotors sont `Q`, `E`, `V`, `J` et `Z`, respectivement.
Pour un choix de rotors R donné, ce mécanisme d'avancement est modélisé par une fonction $\delta_R : \mathcal{A}^m \to \mathcal{A}^m$, qui à une position P associe la position $\delta_R(P)$ où le rotor de droite, ainsi qu'éventuellement un ou plusieurs rotors à sa gauche, ont avancé d'une position. Par exemple, pour $m = 3$ et $R = (\mathrm{III}, \mathrm{II}, \mathrm{I})$, on a :

$$\delta_R(\mathtt{A},\mathtt{D},\mathtt{P}) = (\mathtt{A},\mathtt{D},\mathtt{Q}), \qquad \delta_R(\mathtt{A},\mathtt{D},\mathtt{Q}) = (\mathtt{A},\mathtt{E},\mathtt{R}) \qquad \text{et} \qquad \delta_R(\mathtt{A},\mathtt{E},\mathtt{Q}) = (\mathtt{B},\mathtt{F},\mathtt{R}).$$

On note aussi δ la fonction modélisant l'évolution de la configuration complète de la machine : pour $K = (R, P, C)$, on a $\delta(K) = (R, \delta_R(P), C)$.

Question à développer pendant l'oral 5 *À quoi sert ce mécanisme d'avancement des rotors ?*

Question 6 *Donnez la valeur de la position $\delta^k_{R_i}(P_i)$ pour chacun des triplets (m, i, k) suivants :*
a) $(3, 30, 100)$, ***b)*** $(4, 300, 1000)$, ***c)*** $(5, 3000, 10000)$.

Il est à noter que, lorsque l'opérateur appuie sur une touche, les rotors avancent immédiatement, c'est-à-dire avant que la lettre ne soit chiffrée.

2.5 Chiffrement et déchiffrement d'un message

Afin d'envoyer un message de manière confidentielle à l'aide d'Enigma, il faut que l'expéditeur et le destinataire du message connaissent tous deux une configuration initiale $\tilde{K}$ de la machine, appelée clé de chiffrement. L'expéditeur met alors sa machine Enigma dans la configuration initiale $\tilde{K}$, puis tape le message en clair sur le clavier. Les lampes qui s'allument durant cette opération représentent le message chiffré. Ce message chiffré est alors envoyé au destinataire par un moyen classique (télégraphe, radio, etc.).

Question à développer pendant l'oral 6 *Montrez que, si le message en clair est la suite de lettres $M = (m_0, m_1, m_2, \dots)$, alors le message chiffré est la suite de lettres $M' = (m'_0, m'_1, m'_2, \dots)$ avec $m'_i = \sigma_{\delta^{i+1}(\tilde{K})}(m_i)$ pour $i \geq 0$. Quelles opérations doit effectuer le destinataire du message chiffré afin de le déchiffrer ? La clé de chiffrement $\tilde{K}$ doit-elle être confidentielle ?*

Question 7 *Pour chacun des triplets (m, n, i) suivants, chiffrez le message en clair* `MESSAGE` *à l'aide de la clé de chiffrement $\tilde{K} = K_i$:*
a) $(1, 5, 40)$, ***b)*** $(2, 8, 400)$, ***c)*** $(3, 10, 4000)$.

3 Méthode des caractéristiques de Rejewski

3.1 Clé de message et indicateur

Afin que les opérateurs militaires allemands puissent communiquer entre eux grâce à Enigma, des listes de clés journalières étaient distribuées à tous les opérateurs d'un même réseau de communication : ces listes spécifiaient quelle clé de chiffrement $\tilde{K}$ utiliser en fonction du jour d'envoi du message.
Cependant, utiliser une même clé pour chiffrer tous les messages envoyés un même jour est une vulnérabilité potentielle. Pour la contrer, la procédure suivante fut utilisée jusqu'en 1938 :

1. L'expéditeur récupère la clé journalière $\tilde{K} = (\tilde{R}, \tilde{P}, \tilde{C})$ dans la liste, et place sa machine dans la configuration spécifiée par cette clé.
2. Il choisit au hasard une chaîne P de m lettres de l'alphabet, appelée clé de message.
3. Il saisit deux fois la chaîne P sur le clavier et note les $2m$ lettres chiffrées correspondantes, appelées indicateur du message.
4. Il place ensuite les rotors en position P : la machine se retrouve alors dans la configuration $(\tilde{R}, P, \tilde{C})$ (car l'ordre des rotors et les connexions ne changent pas).
5. Il saisit alors son message en clair et note le message chiffré correspondant.
6. Enfin, l'expéditeur envoie l'indicateur suivi du message chiffré au destinataire.

Question à développer pendant l'oral 7 *Décrivez la procédure que le destinataire doit suivre afin de déchiffrer le message ainsi reçu.*

3.2 Analyse

Si l'on note $\tilde{K}$ la clé journalière et $P = (p_0, p_1, \ldots, p_{m-1})$ la clé de message choisie par l'expéditeur, l'indicateur envoyé est donc $(p'_0, p'_1, \ldots, p'_{m-1}, p''_0, p''_1, \ldots, p''_{m-1})$ avec

$$\begin{cases} p'_i = \sigma_{\delta^{i+1}(\tilde{K})}(p_i) \text{ et} \\ p''_i = \sigma_{\delta^{m+i+1}(\tilde{K})}(p_i), \end{cases}$$

pour tout $0 \leq i < m$. Ainsi, chaque lettre p_i de la clé de message est chiffrée deux fois par des positions différentes de la machine : $\delta^{i+1}(\tilde{K})$ et $\delta^{m+i+1}(\tilde{K})$.
L'idée des cryptanalystes polonais, dont Marian Rejewski, a donc été d'étudier le lien qui existe entre p'_i et p''_i afin d'essayer d'en déduire de l'information sur $\tilde{K}$.
Le tableau suivant donne l'exemple de 32 indicateurs interceptés un même jour (pour des machines à $m = 3$ rotors) :

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

Considérons donc les fonctions suivantes, pour toute configuration $K = (R, P, C)$:

$$\hat{S}_K = \hat{\sigma}_{R,\delta_R^m(P)} \circ \hat{\sigma}_{R,P}^{-1} \qquad \text{et} \qquad S_K = \sigma_C^{-1} \circ \hat{S}_K \circ \sigma_C.$$

Question à développer pendant l'oral 8 *Montrez que $\hat{S}_K$ et S_K sont des permutations de $\mathcal{A}$, et que, pour tout $0 \leq i < m$, on a $p_i'' = S_{\delta^{i+1}(\tilde{K})}(p_i')$. Déduisez-en une méthode pour calculer les permutations $S_{\delta^{i+1}(\tilde{K})}$ à partir de suffisamment d'indicateurs interceptés un même jour, comme dans le tableau précédent. Donnez par exemple la permutation $S_{\delta(\tilde{K})}$ qui définit le lien entre la première et la quatrième lettre des indicateurs du tableau précédent.*

Si la permutation $\hat{S}_K$ ne dépend pas de la configuration C du tableau de connexions, la connaissance de C est par contre nécessaire pour calculer $\hat{S}_K$ à partir de S_K. Néanmoins, Marian Rejewski remarqua que ces deux permutations ont la même caractéristique : ainsi, la connaissance de S_K permet de calculer $\chi(\hat{S}_K)$.

Question à développer pendant l'oral 9 *Justifiez cette remarque de Rejewski : montrez que, pour toute configuration K, on a $\chi(S_K) = \chi(\hat{S}_K)$.*

Question 8 *Pour chacun des triplets (m, n, i) suivants, donnez la caractéristique de la permutation S_{K_i} correspondante :*
a) $(1, 5, 50)$, ***b)*** $(2, 8, 500)$, ***c)*** $(3, 10, 5000)$.

L'idée des cryptanalystes polonais fut donc de précalculer dans une grande table les caractéristiques des permutations $\hat{S}_K$ pour toutes les configurations possibles $K = (R, P, \varnothing)$, c'est-à-dire pour toutes les combinaisons possibles R de rotors et toutes les positions possibles P de ces rotors.
Ainsi, une fois que suffisamment d'indicateurs d'un même jour avaient été interceptés, les cryptanalystes pouvaient reconstruire les permutations $S_{\delta^{i+1}(\tilde{K})}$ pour $0 \leq i < m$, calculer leur caractéristique, puis chercher dans la table une configuration $K = (R, P, \varnothing)$ telle que les m permutations $\hat{S}_{\delta^{i+1}(K)}$ aient les mêmes caractéristiques. Une fois une telle configuration trouvée, les cryptanalystes peuvent alors partir de l'hypothèse que la clé journalière $\tilde{K}$ est de la forme $\tilde{K} = (R, P, \tilde{C})$ puis tenter, par d'autres moyens, de retrouver la configuration $\tilde{C}$ du tableau de connexions.
Afin de construire des caractéristiques pseudo-aléatoires, nous définissons la fonction χ' qui à toute permutation π associe la liste obtenue en triant par ordre croissant sa caractéristique $\chi(\pi)$ concaténée à elle-même. En pratique, cela revient à doubler l'occurrence de chaque longueur de cycle dans la liste $\chi(\pi)$. Ainsi, si $\chi(\pi) = [1, 3]$, alors $\chi'(\pi) = [1, 1, 3, 3]$.

Question 9 *Pour chacun des couples (m, j) suivants, donnez le nombre de configurations $K = (R, P, \varnothing)$ telles que $\chi(\hat{S}_{\delta^{i+1}(K)}) = \chi'(\pi_{13,13i+j})$, pour tout $0 \leq i < m$, et indiquez la plus petite de ces configurations par ordre lexicographique (en considérant pour les rotors que I < II < III < IV < V), si elle existe :*
a) $(1, 10)$, ***b)*** $(2, 100)$, ***c)*** $(3, 1000)$.

Question à développer pendant l'oral 10 *En utilisant le fait qu'une lettre ne peut jamais être chiffrée en elle-même, montrez que, pour toute configuration K, les longueurs des cycles de S_K apparaissent toutes un nombre pair de fois dans $\chi(S_K)$. En vous aidant*

de cette propriété, retrouvez les caractéristiques des trois permutations $S_{\delta(\tilde{K})}$, $S_{\delta^2(\tilde{K})}$ et $S_{\delta^3(\tilde{K})}$ pour les 32 indicateurs donnés dans le tableau précédent. Parmi les 13 configurations $K = (R, P, \varnothing)$ pouvant donner ces caractéristiques, donnez la plus petite par ordre lexicographique.

4 La Bombe de Turing

Dans cette partie, nous aurons besoin de chaînes de caractères pseudo-aléatoires. Pour tous ℓ et $i \geq 0$, nous définissons donc la chaîne de ℓ caractères $\mu_{\ell,i}$ comme

$$\mu_{\ell,i} = (\varphi(u_i \bmod 26), \varphi(u_{i+1} \bmod 26), \ldots, \varphi(u_{i+\ell-1} \bmod 26)).$$

4.1 *Cribs* et *menus*

Les Allemands s'étant rendus compte que l'utilisation d'indicateurs rendait possible l'attaque de Rejewski, ils abandonnèrent ce fonctionnement en 1938, et se mirent à chiffrer toutes leur communications en utilisant uniquement les clés journalières. Ainsi, tout message envoyé un même jour était chiffré avec la même clé de chiffrement $\tilde{K}$.
L'attaque contre Enigma mise au point par les cryptanalystes britannique de Bletchley Park, dont Alan Turing, repose sur l'interception d'un message chiffré dont on suppose connaître un *crib*, c'est-à-dire une partie du message en clair correspondant. Par exemple, si les Anglais interceptaient un message chiffré envoyé depuis une station météorologique, il y avait de fortes chances pour que le message en clair correspondant contienne le *crib* `WETTERBERICHT`, qui signifie « bulletin météo » en allemand.
Dans la suite, on notera $M' = (m'_0, m'_1, \ldots, m'_{\ell-1})$ le message chiffré intercepté, de longueur ℓ, et $Z = (z_0, z_1, \ldots, z_{k-1})$ le *crib*, de longueur k.
La première étape de cette attaque est de parvenir à retrouver la position exacte du *crib* dans le message en clair original, et donc son alignement par rapport au message chiffré. Pour cela, on peut utiliser le fait que, pour toute configuration K et pour toute lettre $x \in \mathcal{A}$, $\sigma_K(x) \neq x$ afin d'éliminer certains alignements invalides.

Question 10 *Pour chacun des triplets (k, ℓ, i) suivants, donnez le nombre d'alignements valides du crib $Z = \mu_{k,i}$ par rapport au message chiffré $M' = \mu_{\ell,i+k}$, ainsi que le premier alignement valide (on donnera un alignement comme la distance entre le début du message chiffré et le début du crib) :*
a) $(20, 100, 50)$, ***b)*** $(50, 1000, 500)$, ***c)*** $(100, 10000, 5000)$.

Une fois le *crib* Z aligné à une distance d du début du message chiffré M', l'idée est de considérer les liens qui existent entre les k lettres du *crib* et les k lettres correspondantes $(m'_d, m'_{d+1}, \ldots, m'_{d+k-1})$ du message chiffré. Pour cela, on construit un *menu* : il s'agit d'un multigraphe (c'est-à-dire que plusieurs arêtes peuvent relier une même paire de sommets) (V, E) dont chaque arête est étiquetée par un entier positif entre d et $d + k - 1$. Ce *menu* est construit de la manière suivante :

— on prend $V = \mathcal{A}$ comme ensemble de sommets ;

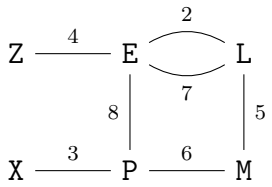
— pour tout $0 \leq i < k$, on ajoute une arête étiquetée par $d+i$ entre les sommets correspondant aux lettres z_i et m'_{d+i} :

$$E = \left\{ (\{z_i, m'_{d+i}\}, d+i) \;\middle|\; 0 \leq i < k \right\}.$$

Par exemple, l'alignement

$$\begin{array}{rc} & \texttt{0 1 2 3 4 5 6 7 8 9} \\ M' = & \texttt{HQLPZLMEPA...} \\ Z = & \texttt{\quad EXEMPLE} \end{array}$$

donnera le *menu* suivant (on ne représente pas les sommets de degré 0) :



Question 11 *Pour chacun des couples (k, i) suivants, construisez le menu correspondant au premier alignement valide du crib $Z = \mu_{k,i}$ par rapport au message chiffré $M' = \mu_{100,i+k}$. Dans chaque cas, donnez le sommet de degré maximal du menu (prenez le premier par ordre alphabétique en cas d'égalité) ainsi que la liste de ses arêtes adjacentes.*
a) $(10, 50)$, ***b)*** $(15, 500)$, ***c)*** $(20, 5000)$.

Question à développer pendant l'oral 11 *Montrez que le menu ainsi obtenu est indépendant de la configuration $\tilde{C}$ du tableau de connexions, à renommage des sommets près.*
En d'autres termes, si l'on note (V', E') le menu que l'on aurait obtenu si le message avait été chiffré avec la clé de chiffrement $(\tilde{R}, \tilde{P}, \tilde{C}')$ au lieu de $\tilde{K} = (\tilde{R}, \tilde{P}, \tilde{C})$, montrez que, pour tout $\tilde{C}'$, (V', E') est isomorphe au menu (V, E), c'est-à-dire qu'il existe une bijection $f : V \to V'$ telle que l'arête $(\{x, y\}, i)$ est dans E si et seulement si l'arête $(\{f(x), f(y)\}, i)$ est dans E'. Quelle est cette bijection f ?

Cette dernière observation permet donc de se débarrasser de l'influence du tableau de connexions. Il « suffit » donc de trouver une configuration initiale des rotors succeptible de produire un tel *menu*. Or, le test de chaque configuration initiale candidate est en fait une instance du problème d'isomorphisme de sous-graphe, qui est NP-complet dans le cas général. Néanmoins, en 1939, Alan Turing mit au point une machine électro-mécanique permettant de le résoudre de manière instantanée dans le cas d'Enigma : la Bombe.

4.2 La Bombe

Attention : cette partie est difficile. Il est fortement recommandé de ne pas chercher à l'aborder avant d'avoir résolu le reste du sujet.

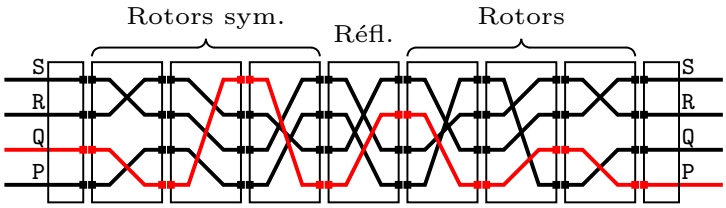
À l'instar d'Enigma, la Bombe fonctionne en propageant un courant électrique dans un circuit. La manière dont celui-ci se propage permet de déterminer si une configuration de rotors est compatible ou non avec un *menu* donné.

La Bombe est constituée de 26 groupes (appelés bus) de 26 fils électriques chacun. Chaque bus est étiqueté par une lettre de l'alphabet (de `A` à `Z`), et les 26 fils d'un même bus représentent eux-mêmes chacun une unique lettre de l'alphabet. La présence de courant dans le fil x du bus y signifie que, d'après la configuration courante, on peut déduire que $\sigma_{\tilde{C}}(x) = y$.

Les bus de la Bombe peuvent ensuite être inter-connectés par des « groupements rotors/réflecteur symétrisés ». Un tel groupement, placé entre deux bus x et y et en configuration (R, P), va ainsi relier les 26 fils du bus x aux 26 fils du bus y de sorte que, pour toute lettre $z \in \mathcal{A}$, le fil z du bus x soit relié au fil $\hat{\sigma}_{R,P}(z)$ du bus y. Intuitivement, ce groupement va réaliser la même permutation que les rotors d'Enigma dans la même configuration, si ce n'est que les rotors seront dédoublés et symétrisés afin que la permutation puisse être effectuée en une seule traversée de droite à gauche (ou de gauche à droite) du groupement.

Les explications suivantes sur le fonctionnement de ces groupements symétrisés sont facultatives. Il n'est pas nécessaire de les lire si vous en avez compris le principe.

> Les rotors utilisés dans ces groupements sont les rotors classiques I, II, … et V d'une part, mais aussi leurs symétriques, notés $\overline{\text{I}}$, $\overline{\text{II}}$, … et $\overline{\text{V}}$, et tels que, pour tout rotor $r \in \mathcal{R}$, on ait $\sigma_{\overline{r}} = \sigma_r^{-1}$. En d'autres termes, lorsqu'ils sont parcourus par le courant de droite à gauche, ces rotors symétriques réalisent la même permutation que les rotors originaux parcourus de gauche à droite.
>
> Dans ces groupements, le réflecteur B est aussi remplacé par une version symétrisée (c'est-à-dire qui applique sa permutation de gauche à droite et de droite à gauche, sans réfléchir le courant).
>
> En configuration (R, P), avec $R = (r_0, r_1, \ldots, r_{m-1})$ et $P = (p_0, p_1, \ldots, p_{m-1})$, le groupement symétrisé sera donc composé, de la droite vers la gauche :
>
> — des m rotors r_{m-1} (en position p_{m-1}), puis r_{m-2} (en position p_{m-2}), … et enfin r_0 (en position p_0) ;
>
> — du réflecteur B symétrisé ;
>
> — des m rotors symétriques $\overline{r}_0$ (en position p_0), puis $\overline{r}_1$ (en position p_1), … et enfin $\overline{r}_{m-1}$ (en position p_{m-1}).
>
> Par exemple, l'équivalent « symétrisé » des trois rotors et du réflecteur représentés figure 4 sera ainsi le groupement suivant :



Enfin, tous les bus sont connectés entre eux grâce à la *diagonal* board, que Gordon Welchman ajouta en 1940 au modèle de Turing. Ainsi, pour toute paire de lettres x et y distinctes, la *diagonal board* connecte électriquement le fil x du bus y au fil y du bus x. Cela revient à dire que, si $\sigma_{\tilde{C}}(x) = y$, alors $\sigma_{\tilde{C}}(y) = x$.

Pour une configuration (R, P) de m rotors donnée, un cryptanalyste peut alors utiliser la Bombe afin de vérifier si cette configuration initiale est compatible avec le *menu* (V, E) de la manière suivante :

— il configure la Bombe suivant le *menu* en plaçant, pour chaque arête $(\{x, y\}, i) \in E$, un groupement rotors/réflecteur symétrisé en configuration $(R, \delta_R^{i+1}(P))$ entre les bus x et y ;

— il choisit une lettre b du *menu* (par exemple, la lettre correspondant au sommet de degré maximal) ;

— il choisit une lettre $t \in \mathcal{A}$ et fait l'hypothèse que, dans la configuration $\tilde{C}$ du tableau de connexions, les lettres b et t sont échangées (ou, s'il choisit $t = b$, que la lettre b est fixée par le tableau de connexions) ;

— il relie le fil t du bus b au courant puis, après propagation du signal électrique au travers de la Bombe, il observe le contenu des 26 fils du bus b.

En effet, après propagation du courant, trois cas de figure peuvent se présenter :

— soit t est le seul fil du bus b relié au courant, auquel cas la configuration (R, P) est déclarée valide avec l'hypothèse $\sigma_{\tilde{C}}(b) = t$;

— soit tous les fils du bus b sont reliés au courant, sauf un (noté t'), auquel cas la configuration (R, P) est déclarée valide avec l'hypothèse $\sigma_{\tilde{C}}(b) = t$;

— dans tout autre cas, la configuration (R, P) est rejetée.

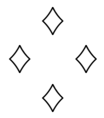
Question à développer pendant l'oral 12 *Expliquez pourquoi la configuration initiale $(\tilde{R}, \tilde{P})$ qui a effectivement servi à chiffrer M' sera bien détectée comme configuration valide par la Bombe.*

Afin de tester de cette manière toutes les positions initiales P possibles rapidement (à b et t fixés), la Bombe dispose d'un système d'avancement automatique et synchronisé des groupements rotors/réflecteur symétrisés : après un laps de temps suffisant pour avoir permis au courant de se propager (quelques millisecondes, en pratique), la fonction d'avancement δ_R est appliquée de manière synchrone à tous les groupements de la Bombe, et le test de validité peut alors être effectué de la même manière sur la position suivante $\delta_R(P)$. Au bout de 26^m tels essais, l'ensemble des positions initiales a pu être parcouru pour une combinaison de rotors R donnée.

Question à développer pendant l'oral 13 *Décryptez le message intercepté*

$$M' = \texttt{CBMKAENHLXXYBAXPLWFGKQCOUNDQAZPIYABGQQFFQYIHR}$$

en vous servant du crib $Z = \texttt{ALANXTURINGXSERAITX}$*, pour une machine à* $m = 3$ *rotors.*



Fiche réponse type: Enigma

$\widetilde{\mathbf{u_0}}$ **:** 42

Question 1

a) 394295, 6

b) 162957, 20

c) 41202, 18

Question 2

a) 1, 3, 0

b) 42, 16, 36

c) 193, 251, 171

Question 3

a) $[5]$

b) $[1, 3, 11, 35]$

c) $[1, 1, 30, 119, 349]$

Question 4

a) P, I, B

b) C, U, H

c) E, Q, V

Question 5

a) A, E, C

b) Q, U, C

c) J, Z, Z

Question 6

a) $(\mathtt{N}, \mathtt{U}, \mathtt{J})$

b) $(\mathtt{U}, \mathtt{H}, \mathtt{D}, \mathtt{T})$

c) $(\mathtt{B}, \mathtt{G}, \mathtt{K}, \mathtt{R}, \mathtt{K})$

Question 7

a) TTMOHPQ

b) ZOELRYB

c) NBNEQZL

Question 8

a) $[1, 1, 3, 3, 4, 4, 5, 5]$

b) $[1, 1, 1, 1, 2, 2, 9, 9]$

c) $[1, 1, 3, 3, 9, 9]$

Question 9

a) 38, (I, B, $\varnothing$)

b) 5, (I-III, YY, $\varnothing$)

c) 0

Question 10

a) 36, 6

b) 138, 2

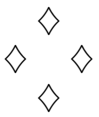
c) 194, 48

Question 11

a) W, $\{(\mathtt{I}, 3), (\mathtt{I}, 7), (\mathtt{U}, 5)\}$

b) I, $\{(\mathtt{H}, 7), (\mathtt{K}, 1), (\mathtt{R}, 10), (\mathtt{U}, 2)\}$

c) Q, $\{(\mathtt{E}, 16), (\mathtt{F}, 7), (\mathtt{T}, 0)\}$



Fiche réponse: Enigma

Nom, prénom, u_0: .....

Question 1

a)

b)

c)

Question 2

a)

b)

c)

Question 3

a)

b)

c)

Question 4

a)

b)

c)

Question 5

a)

b)

c)

Question 6

a)

b)

c)

Question 7

a)

b)

c)

Question 8

a)

b)

c)

Question 9

a)

b)

c)

Question 10

a)

b)

c)

Question 11

a)

b)

c)