TD 2 : ENIGMA + Chiffrement à flot

christina.boura@uvsq.fr

6 février 2018

1 ENIGMA

Les exercices de cette partie sont dus à Joachim von zur Gathen et Jérémie Detrey.

1.1 Fonctionnement de l'ENIGMA

Dans cet exercice nous allons considérer le modèle "M3" de la machine ENIGMA, utilisée par l'armée allemande. Cette machine est composée des éléments suivants :

- Un **clavier** comportant les lettres 'A' à 'Z'.
- Un **tableau de connexions** permettant de relier deux lettres du clavier entre elles.
- Trois **rotors** choisis parmi un ensemble de cinq rotors possibles (notés I, II, III, IV et V) et placés dans un ordre particulier. Sur une face d'un rotor sont disposés en cercle des contacts électriques à aiguilles. Sur l'autre face, sont disposés le même nombre de contacts plats. Les contacts plats et à aiguilles représentent l'alphabet (lettres de 'A' à 'Z'). Une fois les rotors assemblés, les contacts à aiguilles d'un rotor se positionnent en face des contacts plats du rotor voisin, formant ainsi la connexion électrique. À l'intérieur du rotor, un ensemble de 26 câbles électriques assurent les connexions entre les contacts à aiguilles et les contacts plats suivant un chemin concret pour chaque rotor. Chaque rotor représente une permutation de 26 lettres.

  Chaque fois qu'on chiffre une lettre, les rotors avancent. Plus précisément, à chaque nouvelle touche pressée, seulement le premier rotor (le rotor le plus à droite) avance d'un cran. Le rotor du milieu avance d'une position seulement quand le premier rotor se trouve à une position particulière, appelée *position d'entraînement*. Le troisième rotor avance quand le deuxième rotor se trouve à sa propre position d'entraînement.
- Un **réflecteur**, placé à gauche des trois rotors est une dernière permutation qui permet de revenir en arrière. On permute une dernière fois les lettres deux par deux, et on les fait retraverser les rotors et le tableau de connexion.
- Un **tableau lumineux**.

Les permutations décrivant les cinq rotors ainsi que celle correspondant au réflecteur sont présentées dans le tableau suivant :

	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
I	5	11	13	6	12	7	4	17	22	26	14	20	15	23	25	8	24	21	19	16	1	9	2	18	3	10
II	1	10	4	11	19	9	18	21	24	2	12	8	23	20	13	3	17	7	26	14	16	25	6	22	15	5
III	2	4	6	8	10	12	3	16	18	20	24	22	26	14	25	5	9	23	7	1	11	13	21	19	17	15
IV	5	19	15	22	16	26	10	1	25	17	21	9	18	8	24	12	14	6	20	7	11	4	3	13	23	2
V	22	26	2	18	7	9	20	25	21	16	19	4	14	8	12	24	1	23	13	10	17	15	6	5	3	11
Réfl.	25	18	21	8	17	19	12	4	16	24	14	7	15	11	13	9	5	2	6	26	3	23	22	10	1	20

Les positions d'entraînement des rotors I, II, III, IV et V sont respectivement `Q`, `E`, `V`, `J` et `Z`.

1.1.1 Taille de la clé

La configuration de l'ENIGMA est donnée par :

— Le choix (ordonné) de 3 rotors parmi 5.
— La position de départ de chaque rotor.
— Les positions d'entraînement des rotors du gauche et du milieu.
— La configuration du tableau de connexions, qui peut lier jusqu'à 13 paires de lettres.

1. Calculer le nombre de possibilités pour choisir 3 parmi les 5 rotors et les ordonner.
2. Calculer le nombre de positions de départ possibles pour les trois rotors.
3. Calculer le nombre de positions possibles pour l'entraînement des rotors du gauche et du milieu.
4. Calculer le nombre de configurations possibles du tableau de connexions quand une paire de lettres est permutée. Faire pareil pour $2, 3, \ldots, 13$ paires de lettres.
5. Calculer le nombre total de configurations possibles du tableau de connexions.
6. Calculer le nombre total de configurations possibles pour cette ENIGMA.
7. Quelle est la taille d'une clé en bits ?

1.1.2 Chiffrement et déchiffrement

Considérons une configuration simple de l'ENIGMA : Les rotors III, II et I (de gauche à droite) sont utilisés et on suppose pour l'instant qu'aucune paire de lettres n'est connectée par le tableau de connexions.

1. En quelle lettre `A` sera-t-elle chiffrée avec une telle configuration ?
2. En commençant avec la même configuration, en quelle lettre sera chiffrée la lettre `N` ?
3. Montrer que dans le cas général (*c.-à-d.* pour toute configuration des rotors), le chiffrement et le déchiffrement sont des opérations identiques.

   Supposons qu'on lie certaines lettres par le tableau de connexion.

4. En quelles lettres seront chiffrées `A` et `R` si on suppose que les lettres `A-C` et `R-X` sont liées ?
5. En quelles lettres seront chiffrées `A` et `N` si on suppose qu'elles sont liées par le tableau de connexions ?
6. Peut une lettre être chiffrée en elle-même ? Pourquoi ?

1.2 Cryptanalyse d'ENIGMA

Chaque jour, tous les opérateurs ENIGMA commençaient par taper chaque message en utilisant les mêmes réglages, comme spécifiés dans le carnet des codes pour ce jour particulier. Cependant, afin d'assurer une meilleure sécurité, ils choisissaient différents messages-clés (positions de rotors) pour chaque nouveau message.

Le mode d'utilisation pour chiffrer un message donné était le suivant :

— Régler la machine selon les réglages du jour spécifiés dans le carnet des codes.
— Taper le message-clé choisi deux fois (e.x. `BITBIT`).
— Régler les rotors à la position indiquée par le message-clé (e.x. `BIT` ici).
— Taper le message actuel.

Un opérateur qui recevait le message allait effectuer les actions suivantes afin de le déchiffrer :

— Régler la machine selon les réglages du jour spécifiés dans le carnet des codes.
— Recevoir et déchiffrer les six premiers caractères, vérifiant que la répétition a eu lieu, et extraire le message-clé.
— Régler les rotors à la position indiquée par le message-clé.
— Déchiffrer le reste du message chiffré.

Toutefois, un tel chemin comporte un point extrêmement faible que nous allons exploiter dans cet exercice.

Le tableau suivant présente un nombre de message-clés chiffrés, interceptés pendant le même jour (c.-à.-d. chiffrés avec les réglages initiaux d'Enigma pour ce jour).

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

1. Vérifier que lorsque les lettres à la position i (i étant $1, 2$ ou 3) de deux messages-clés chiffrés sont égales, ceci est également le cas pour les lettres à la position $i+3$. Par exemple, un '`H`' à la position 1, donne toujours un '`G`' à la position 4. Expliquer.
2. Dériver la permutation σ_1 qui lie une lettre x à la position 1 à la lettre $\sigma_1(x)$ à la position 4 (tableau de correspondance). Par exemple $\sigma_1(\texttt{H})=\texttt{G}$.
3. Décomposer cette permutation en produit de cycles.
4. Compter la longueur de cycles. On appellera l'ensemble de ces longueurs *caractéristique* de la permutation.

   Remarque : Rejewski a prouvé qu'on ne peut avoir qu'un nombre pair de cycles de chaque longueur.
5. Est-ce que la caractéristique change si on utilise une configuration différente pour le tableau des connexions ?
6. Donner les permutations σ_2 (positions $2-5$) et σ_3 (positions $3-6$).
7. Donner leurs caractéristiques.
8. En supposant que pendant le chiffrement de ces 6 caractères les deux derniers rotors n'ont pas avancé, décrire une façon d'utiliser ces trois caractéristiques afin de trouver l'ordre et les réglages des rotors.

2 Chiffrement à flot

2.1 Chiffrer à la main

Le définition du chiffrement à flot vu en cours peut être généralisée aux alphabets autres que l'alphabet binaire. Pour chiffrer à la main, on peut imaginer un chiffrement à flot qui opère sur des lettres.

1. Développer un chiffrement qui opère sur les lettres `a`,`b`, ...,`z` en représentant chaque lettre par un chiffre de 0 à 26 (`a` $\to$ 0, `b` $\to$ 1, ...). Donner les fonctions de chiffrement et de déchiffrement.
2. Déchiffrer le texte chiffré

   `xrjoclaoovmmyblm`

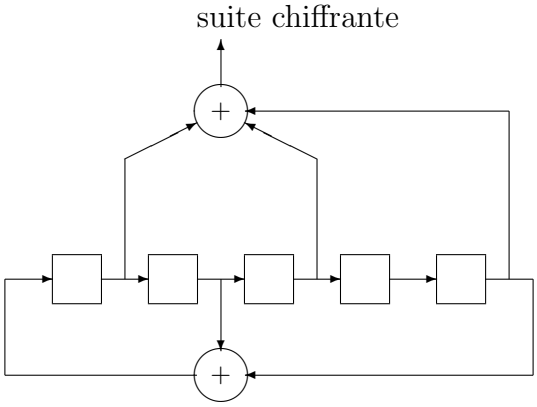
   qui a été chiffré en utilisant la clé

   `jekklrwanrvcypwh`

   A quelle adresse a été donné le rendez-vous pour samedi soir ?

2.2 Récupérer l'état initial d'un générateur des nombres pseudo-aléatoires

Soit le générateur pseudo-aléatoire suivant ayant un état interne de 5 bits.



Un attaquant observe les 5 cinq premiers bits de la suite chiffrante : 11101. Le bit le plus à gauche est le bit généré à l'instant 0. Montrer comment l'attaquant peut retrouver l'état initial $\mathtt{x}_0\mathtt{x}_1\mathtt{x}_2\mathtt{x}_3\mathtt{x}_4$ (la graine) du générateur.