Université de Perpignan - L3 Info 2016 C. Negre

Mini-projet Enigma

L'ojectif de ce mini-projet est de programmer en C le chiffrement d'Enigma vu en cours. Rappelons qu'Enigma consiste chiffre un message alphabétique en appliquant la séquence d'opérations qui suvient :

— Substitution initiale S_I permute 6 paires de lettres, implémenté dans enigma par 6 fiche reliant 5 paires de lettres.

— Trois substitutions consistant en trois rotors $R1$ puis $R2$ puis $R3$. Ces trois rotors sont décrits ci-dessous :

Table 1 – Rotor 1

Entrée	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
Sortie	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

Table 2 – Rotor 2

Entrée	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
Sortie	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

Table 3 – Rotor 3

Entrée	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
Sortie	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

Les rotors bougent comme suit : R1 avance d'un cran après chaque lettre chiffrée, R2 avance d'un cran après 26 lettres chiffrées et R3 avance d'un cran après 26×26 lettres chiffrées.

— Le réflecteur permutte les lettres deux à deux comme suit :

$$\begin{aligned} A &\leftrightarrow Y \\ B &\leftrightarrow R \\ C &\leftrightarrow U \\ D &\leftrightarrow H \\ E &\leftrightarrow Q \\ F &\leftrightarrow S \\ G &\leftrightarrow L \\ I &\leftrightarrow P \\ J &\leftrightarrow X \\ K &\leftrightarrow N \\ M &\leftrightarrow O \\ T &\leftrightarrow Z \\ V &\leftrightarrow W \end{aligned}$$

— Ensuite les rotors inverses sont appliqués dans l'ordre inverse : $R3^{-1}$ puis $R2^{-1}$ puis $R1^{-1}$.

— Enfin la permutation initiale inverse est appliquée S_I^{-1}

Le but du mini-projet est le suivant :

1. Faire un programme qui chiffre un fichier contenant du texte français. Vous ne chiffrerez que les lettres alphabétiques minuscules ou capitales, vous laisserez la ponctuation et les espaces inchangés.

2. Pensez à structurer votre code avec des fonctions et à le rendre suffisament clair et compréhensible. Pensez aussi à le commenter.
3. Vous testerez l'attaque décrite dans l'exercice 6 de la feuille de TD1 de crypto.