Cycle Fondamental
2A S2 Math/Info (MAT2053)
21/01/2019

ESIEA Paris/Ivry-sur-Seine
Année Académique 2018/2019

Cryptographie

Intervenant : Michael FRANÇOIS (francois@esiea.fr)

TD1_1 -- Chiffrement par substitution mono-alphabétique

A. Travail à faire sur papier

- **1.** Quelle est la différence entre la cryptographie et la cryptanalyse ?
- **2.** Que signifie le texte en clair ou *plaintext* ?
- **3.** Quelle est la différence entre la cryptographie symétrique et la cryptographie asymétrique ?
- **4.** Quels sont les inconvénients de la cryptographie asymétrique ?
- **5.** Dans un procédé de substitution mono-alphabétique, chaque lettre du texte en clair est remplacée par une autre lettre du même alphabet dans le texte chiffré. On considère la substitution suivante :

Clair ⟹	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
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Chiffré ⇒	g	r	q	y	u	o	e	p	w	n	s	a	d	f	h	j	i	k	l	x	c	z	m	v	b	t

Remplir le tableau suivant, selon la permutation donnée :

Texte clair	Texte chiffré
normandie	
	qkhwlwukulckagluwfu

B. Travail à faire sur ordinateur (prog. C)

Créer un fichier `cle.txt` contenant la clé de chiffrement suivante :

```
grqyuoepwnsadfhjiklxczmvbt
```

Cette clé signifie que la lettre 'a' (resp. b, ...) du texte clair sera remplacée par la lettre 'g' (resp. r, ...) lors du chiffrement.

- **1.** Écrire une fonction `CHARGER_CLE`, qui permet de charger la clé depuis un fichier donné en argument. Cette fonction prend en paramètres le tableau dans lequel sera chargé la clé et le nom de fichier contenant la clé. Voilà le prototype de la fonction :

```
void CHARGER_CLE (char cle[26], char * nom_fic_cle) ;
```

Vous pouvez utiliser la fonction `fgetc` pour récupérer les caractères depuis le fichier. Tester cette fonction en remplissant la fonction `main`.

► **2.** Écrire une fonction `CHIFF_MONO_ALPHA`, qui permet de chiffrer le contenu d'un fichier `clair.txt` selon la clé chargée. Les paramètres de cette fonction sont le tableau de clé, le nom du fichier en clair et le nom du fichier qui va contenir le texte une fois chiffré. Voilà le prototype de la fonction :

```
void CHIFF_MONO_ALPHA (char cle[26], char * nom_fic_clair, char * nom_fic_chiff) ;
```

Tester cette fonction en utilisant un fichier `clair.txt` contenant le message de votre choix. Le fichier `clair.txt` contient un message tout attaché et constitué uniquement de lettres en minuscule.

► **3.** Écrire une fonction `DECHIFF_MONO_ALPHA`, qui permet de déchiffrer le contenu chiffré d'un fichier selon la clé chargée. Les paramètres de cette fonction sont le tableau de clé, le nom du fichier chiffré et le nom du fichier qui va contenir le texte une fois déchiffré. Voilà le prototype de la fonction :

```
void DECHIFF_MONO_ALPHA (char cle[26], char * nom_fic_chiff, char * nom_fic_dechiff) ;
```

Tester cette fonction sur le chiffré précédemment obtenu.

► **4.** Déchiffrer le message suivant :

```
aulhfluyujagquicwftuohwljaclkgjwyudufxygflauoukicuygflagwk
```