Devoir de Modélisation Cryptographique

Version du 12 juillet 2015

Exercice 1 – Préparations

Dans cet exercice, nous allons vous présenter les étapes nous semblant nécessaires au bon commencement de votre apprentissage/révision de la programmation en `C`.

1. Installer Linux ! Que ce soit sur votre machine ou dans une machine virtuelle, vous devez tous avoir une version de linux fonctionnelle et que vous maîtrisez. La distribution Kali `https://www.kali.org` semble la plus adaptée à votre formation.
2. Avoir des bases en système Unix. Pour ce faire, je vous propose de lire et **surtout** d'expérimenter la partie 2 du cours disponible ici : `https://www-licence.ufr-info-p6.jussieu.fr/lmd/licence/2014/ue/2I015-2015fev/index.php`
3. Lire un cours de langage C et **pratiquer** la programmation avec ce langage. Pour le cours de C voici quelques liens :
   - La référence qu'il faut prendre pour commencer : `http://www.iups.org/media/meeting_minutes/C.pdf`
   - Une lecture de la partie 1 de `https://www-licence.ufr-info-p6.jussieu.fr/lmd/licence/2014/ue/2I015-2015fev/index.php` et si vous souhaitez aller plus loin, ce cours vous aidera : `http://www.btsinfogap.org/cours/progSousLinuxAvance.pdf`
   - Avoir comme livre de chevet (numérique ou physique) le lien suivant est une bonne idée : `https://www.nostarch.com/hacking2.htm`

   Pour la pratique, l'exercice qui suit vous servira de tremplin. Ne vous arrêtez pas là, programmez d'autres applications !

Exercice 2 – Carré de Polybe et chiffrement ADFGVX

Le carré de Polybe (Grèce antique, 200 ans avant J.-C.) permettait de transmettre des messages à l'aide de torches allumées. Pour cela, on écrit dans un tableau carré 5×5 les lettres de l'alphabet (privé de W que l'on pourra remplacer par V). Pour transmettre une lettre, on transmettra ses coordonnées dans ce tableau en allumant d'un côté le nombre de torches (< 5) correspondant au numéro de la ligne et de l'autre celui des colonnes.

De ce principe de base, un chiffrement utilisé pendant la première guerre mondiale est né. Le colonel allemand Fritz Nebel a mis au point le chiffrement ADFGVX (ou GEDEFU 18) qui sera utilisé à partir de 1918. Ici on utilise des tableaux de taille 6 permettant de coder l'ensemble des lettres de l'alphabet (non accentuées) et les 10 chiffres. Plutôt que d'utiliser des nombres pour identifier les lignes et colonnes, on utilise les lettres ADFGVX qui sont très éloignées dans le code morse et ainsi permet d'éviter les fautes de frappes (ou, au pire, de corriger facilement une telle erreur de transmission). Une première clé secrète consiste en la disposition des caractères dans le tableau. Une deuxième clé est représenter par une permutation permettant de mélanger le texte chiffré après application du principe de Polybe.

Par exemple, on suppose que le tableau est donné par :

	A	D	F	G	V	X
A	c	1	o	f	w	j
D	y	m	t	5	b	4
F	i	7	a	2	8	s
G	p	3	0	q	h	x
V	k	e	u	ℓ	6	d
X	v	r	g	z	n	9

Dans une première étape, on codera donc le mot `attaque` par `FF|DF|DF|FF|GG|VF|VD`.

Dans une seconde étape, on va transposer les lettres que nous venons d'obtenir (chiffrement par transposition, i.e. les lettres restent les mêmes, on échange leurs positions). Supposons que la clé de permutation π soit de longueur $n = 4$ et donnée par $pi = [3, 1, 2, 4]$ (représentée par un tableau, i.e. l'image de i par π est donnée par $pi[i]$). On dispose alors le texte codé en ligne successives de n lettres et on complète les lignes par des caractère aléatoires (ne modifiant pas le message, `XX` ici) :

```
FFDF
DFFF
GGVF
VDXX
```

Le texte chiffré sera le résultat de la permutation par π des colonnes :

```
FDFF
FFDF
GVGF
DXVX
```

et la lecture des caractères de haut en bas et de gauche vers la droite. Finalement on obtient le chiffré :

```
FFGD|DFVX|FDGV|FFFX
```

1. Chiffrer (à la main) le texte `attaquesurparisle12janvier` à l'aide du même tableau que dans l'exemple et de la permutation $[2, 1, 5, 3, 6, 4]$.
2. Déchiffrer le texte `GFFFV FFDFF DDFXG FVDVV XFVVF GXGAD AXDGV FGVFX FFVAF FVV` sachant qu'il a été chiffré à l'aide du même tableau que dans l'exemple et de la permutation $[3, 1, 6, 2, 5, 4]$.
3. Implémenter le chiffrement et le déchiffrement ADFGVX en utilisant le langage C. Vous ferez attention à bien spécifier les entrées de vos applications.

Pour l'histoire : l'ancien major de l'école polytechnique Georges-Jean Painvin entré en tant que réserviste au service du chiffre français, réussit à cryptanalyser entre avril et mai 1918, le cryptosystème ADFGVX mis en place par les allemands au début mars de la même année. En particulier, cette analyse lui permit de déchiffrer un message allemand sur l'organisation d'une attaque au nord de Compiègne. Cette attaque déjouée fût un des tournants pour la victoire des français. Le secret sur cette attaque fût classé pendant 50 ans (classique concernant le secret militaire) et le colonel allemand Nebel fût fort désappointé lorsqu'en 1967 il apprit que son cryptosystème était cassé depuis fort longtemps !

