Introduction à la Sécurité **Licence Informatique 2022–2023**

Travaux pratiques 1

1 Introduction

Le site https://www.root-me.org/est utilisé en France par les entreprises et les administrations pour évaluer le niveau et le principal domaine d'intérêt d'un candidat. Si vous voulez travailler dans le domaine de la cybre-sécurité, c'est LE domaine sur lequel il faut passer du temps.

Principe de fonctionnement Le site propose un certain nombre de challenges, organisés par type de challenge, et chaque challenge rapporte des points quand on trouve la solution. En résolvant des challenges, on montre ses compétences, et on gagne des points.

Inscription Si ce n'est pas déjà fait, inscrivez vous sur le site https://www.root-me.org/

2 Description des TPs

Il y a 5 séances de TP. On verra des **introductions** à certains des types de challenges disponibles sur https://www.root-me.org/

- *Cryptanalyse* : bases de la cryptanalyse (analyse fréquentielle sur des anciens codes (TP1) ;
- *Forensics* : c'est la recherche de traces sur un ordinateur. On verra la récupération de clefs de chiffrement basée sur l'entropie et sur l'analyse de code (TP2) ;
- *App-script* : analyse de la sécurité d'un script écrit en bash (TP3) ;
- réseau (TP4 et TP5, notés) : recherche de failles dans un protocole cryptographique.

3 TP 1

Analyse fréquentielle Historiquement, l'analyse fréquentielle consiste à regarder le nombre de fois qu'un caractère apparaît dans un texte. On suppose ensuite que le texte est du français (où une autre langue normale). Dans tous les langages, il y a des caractères qui apparaissent plus souvent que d'autres. Par exemple, en français, e est la lettre qui apparaît le plus souvent.

Dans le paragraphe précédent, il y 48 e, 32 a, et 26 s. En général, il y a plus de s que de a, donc il faut accepter que le bon résultat n'est pas forcément trouvé du premier coup.

Question 1. Que veut dire le message suivant ?

```
QJ HTWGJFZ JY QJ WJSFWI
Rfnywj Htwgjfz, xzw zs fwgwj ujwhmj,
Yjsfny js xts gjh zs kwtrflj.
Rfnywj Wjsfwi, ufw q'tijzw fqqjhmj,
Qzn ynsy f ujz uwjx hj qfslflj :
Jy gtsotzw, Rtsxnjzw iz Htwgjfz,
Vzj atzx jyjx otqn ! vzj atzx rj xjrgqje gjfz !
Xfsx rjsynw, xn atywj wfrflj
```

Xj wfuutwyj f atywj uqzrflj,
Atzx jyjx qj Umjsnc ijx mtyjx ij hjx gtnx.
F hjx rtyx qj Htwgjfz sj xj xjsy ufx ij otnj,
Jy utzw rtsywjw xf gjqqj atnc,
Nq tzawj zs qfwlj gjh, qfnxxj ytrgjw xf uwtnj.
Qj Wjsfwi x'js xfnxny, jy iny : Rts gts Rtsxnjzw,
Fuuwjsje vzj ytzy kqfyyjzw
Any fzc ijujsx ij hjqzn vzn q'jhtzyj.
Hjyyj qjhts afzy gnjs zs kwtrflj xfsx itzyj.
Qj Htwgjfz mtsyjzc jy htskzx
Ozwf, rfnx zs ujz yfwi, vz'ts sj q'd uwjsiwfny uqzx.
Hjqzn vzn jxy gnjs fnxj i'jywj qtzj ufw ijx ufwtqjx ywtrujzxjx, js jxy xtzajsy
uzsn ufw zs wjujsynw mtsyjzc.

Analyse du code de Vigenère Ce code était réputé "incassable" car il prend en entrée 2 textes inconnus. Le premier est le message qu'on veut transmettre. Le second, beaucoup plus court pour être mémorisable, sert de clef de chiffrement. On associe à chaque lettre un numéro ($a = 0$, $b = 1$, ..., $z = 25$). Par exemple :

- message : "message", de valeur (12,4,18,18,0,6,4)
- clef 1 : "clef", de valeur (2,11,4,5)

Puis on répète la clef autant de fois que nécessaire pour aller jusqu'à la fin du texte : La clef devient (2,11,4,5,2,11,4). Et on renvoie la somme lettre par lettre (modulo 26), qu'on traduit en entier. Des fonctions C pour chiffrer et déchiffrer avec ce chiffrement sont données à la fin du TP comme indication. L'idée pour déchiffrer est de supposer que la clef a une longueur de n lettres (on commence avec $n = 1$, et on augmente pour trouver la bonne valeur). On découpe le texte chiffré en prenant une lettre sur n, ce qui donne n textes qui sont n fois plus cours. Pour le bon n, on doit avoir des analyses fréquentielles qui ressemblent à celle du langage cible (le français). Si on est satisfait du n trouvé, l'analyse fréquentielle permet de retrouver le décalage.

Question 2. Retrouvez le livre dont est issu ce texte, et la clef de chiffrement, et envoyez le résultat à votre enseignant.

(1) (1) Ll f u duzml dlm dnpgdue kx'ou usplfoe lfdnz. Fhuy zrrty ve yuspyifhl xh clfoe k'oqe jbhvyy ; llz iqt su seho wajbhtly, papm oa aullsy xn wyx psov hhowe. Pfv svhw shhv cvlqez, yw llous qupblm, vaum mophwuyyv np uutpwxlhnloum ; (2) llz hh sl wrujbhna jriun sobl goyglr, ln vi xohlxoh ajwldlhw llm iapn wotvhr, pfv nl jhucyqt zy vobfhvll qi zy ueklhszyu. (3) Llm drilhs syxr zyuvlhw dl fltz ; cos z's dpwoleun ht wlhnuyqt syxr yysoz, ulnzc lnjflnlm oenyuetyqt. (4) Siusxo'd llous aldclm oez wkazmhuym gejixvyyqt syv lpyxx xo'llz zuexohnayqt, pfv y kyuajcqeun wobm oez uubyyv, ob fhs jixplhw a mfhuy xh tllue, ky pauchrl kx'ism foumhrcyqt lhfoyy wobnh l'hjsayyqcl xh lh mrlpxltl. (5) Whs hhlmhoa vpyqnlhw s'f uspbshr, zyoou fhuy wruaope, yyqvllveun fe mlhll uspbc say fhuy jrikm, ht aipblhw acyf l'hlerl.