UNIVERSITÉ LAVAL

Travail pratique N^o 1

Cours : GLO-3100 Cryptographie et sécurité informatique

Objectif

Le but de ce travail est de vous faire pratiquer différents systèmes cryptographiques étudiés en classe ainsi que quelques techniques de cryptanalyse.

Remarques

— Pour les exercices 2 et 3, les caractères seront mappés sur des nombres compris entre 0 et 127. Le mappage est le système de code ASCII standard.

Le texte à utiliser pour le chiffrement est donné ci-dessous :

When commands are read from a tty, the interpreter is said to be in interactive mode. In this mode it prompts for the next command with the primary prompt, usually three greater-than signs (>>>); for continuation lines it prompts with the secondary prompt, by default three dots (...). The interpreter prints a welcome message stating its version number and a copyright notice before printing the first prompt.

— Pour l'exercice 5, vous aurez besoin du programme *Vigenere.jar* (le fichier est disponible sur le site web du cours) qui vous aidera à faire vos calculs.

— Pour simplifier votre code, vous pouvez utiliser la méthode brute pour inverser une valeur a dans $\mathbb{Z}_n$ comme suit :

```
int modInverse(int a, int n)
{
    a = a % n;
    for (int i = 1; i < n; x++) {
        if ((a*i) % n == 1) {
            return i;
        }
    }
}
```

1 Exercice 1 : Briser le chiffrement par décalage (2 pts)

Le chiffrement d'un texte m écrit en français a donné le résultat suivant :

```
Xihdiolvwvniomv.nvwvnion.mu
Mcvpiomvwllcp.tvwvfcl.vy.yc,vyv.mnvko.vpiomvwp.tvl.ommcvf.vjl.gc.lvybwff.ha.u
Fwvjliybwch.v.nwj.vm.lwvz.vxicl.vohvxihvj.ncnvyw
 ↪  .,vl.fwr.lv.nvjwmm.lvwovjliybwchv.r.lycy.uvZ.mif.vjiolvf.mv won.mvzvilnialwjb.u
```

Pour les questions suivantes, nous vous demandons de **bien justifier vos réponses en donnant toutes les étapes intermédiaires qui vous amènent à la conclusion**. À noter que l'utilisation d'outils en ligne ou des réponses sans justifications ne vous donneront aucun point.

1. **(1 pt)** Utilisez la cryptanalyse par recherche exhaustive de clés afin de décrypter le message.
2. **(1 pt)** Utilisez la cryptanalyse par analyse de fréquences afin de décrypter le message.

Exercice 2 : Chiffrement affine (3 pts)

Chaque lettre est cryptée séparément. Toutes les opérations arithmétiques doivent être effectuées modulo 128.

$$e_1(x) = 119x + 82$$

1. Écrire un programme permettant de chiffrer et déchiffrer des chaînes de caractères à l'aide de ce chiffrement affine.
2. Chiffrer et déchiffrer le texte exemple fourni plus haut.
3. Chiffrer et déchiffrer la chaîne "RATEAU" en utilisant le chiffrement affine $e_2(x) = 6x - 23$.

Exercice 3 : Chiffrement de Hill (3 pts)

Le message est chiffré en blocs de longueur n et le chiffrement de chaque bloc est effectué en multipliant le vecteur représentant les n lettres par la matrice clé.

$$[y_1, y_2] = [x_1, x_2] \begin{bmatrix} -1 & 2 \\ 3 & 1 \end{bmatrix}$$

1. Écrire un programme permettant de chiffrer et déchiffrer des chaînes de caractères à l'aide de ce chiffrement de Hill.
2. Chiffrer et déchiffrer le texte exemple fourni plus haut.
3. Chiffrer et déchiffrer le texte exemple fourni plus haut en utilisant la matrice clé $\begin{bmatrix} 6 & 2 \\ 3 & 1 \end{bmatrix}$.

Exercice 4 : Chiffrement par substitution monoalphabétique (2 pts)

Le chiffrement par substitution monoalphabétique consiste à remplacer une lettre par une autre lettre. Par exemple, en utilisant la permutation suivante :

$$\begin{aligned} \pi \quad = \quad & [a \mapsto u, b \mapsto n, c \mapsto v, d \mapsto a, e \mapsto b, f \mapsto c, g \mapsto d, h \mapsto e, i \mapsto f, \\ & j \mapsto g, k \mapsto h, l \mapsto i, m \mapsto j, n \mapsto k, o \mapsto l, p \mapsto m, q \mapsto o, \\ & r \mapsto p, s \mapsto q, t \mapsto r, u \mapsto s, v \mapsto t, w \mapsto w, \\ & x \mapsto x, y \mapsto y, z \mapsto z] \end{aligned}$$

la version chiffrée du message *abc* sera *unv*.

1. **(1 pt)** Écrire une fonction *chiffrement_substitution(texte, substitution)* qui retourne le résultat du chiffrement par substitution de la chaîne de caractères *texte* où l'argument *substitution* est un dictionnaire (un map) donnant la substitution pour chacun des caractères de l'alphabet. Il convient de noter que nous décidons de ne chiffrer que les lettres minuscules non accentuées de l'alphabet. Les autres lettres ou caractères seront conservés tels quels.
2. **(1 pt)** La personne qui a reçu le texte chiffré connaît le dictionnaire de substitution qui a permis de chiffrer le texte. Votre second travail sera de l'aider à retrouver le texte original. Pour ce faire, vous devez écrire une seconde fonction *dechiffrement_substitution(texte_chiffre, substitution)* qui retourne le texte original si *texte_chiffre* est le résultat du chiffrement par substitution effectué avec la fonction *chiffrement_substitution*.

Exercice 5 : Briser Vigenère (5 pts)

Le chiffrement d'un texte m écrit en anglais en utilisant Vigenère a donné le résultat suivant :

```
YHKMVMSXVVXTMGVWMRCJKSQREJYCBEJYIVODEFDSCTIRTPESMPVPITSYEGBYTNZSXWLCTLSSXBVTBOGYJ
WYFGIEZORXCEKYRHCEEBYMHWSBMENZSXCEFCINPPUZRDEBNZRDOYHZRDEPFZKSBPYKIHTGUCPODGCGLO
RXYOXNEGLPTDISHZWDHILVZORWYZRYTLYIAYRHMDSFIRAWVYMXBVYXIRNVPVIKCSPOCMJYIBTIRKFKCONFT
VAMHKIHTEWZTREVCJEZAMLFJKLKIIMDHQMKLKTGLVEDEXBVIXCVSGXSORUEHDHILVZORWCEKNEGLPTDISHK
LODINRMVEHIGIBAXCFRYFEWZTREVCJGYNXLFPVEHVFXRBCNYIKLKIIMDHQUEHSNIUTLSNWNRRMEFSROOYXB
ZWSSEMVGBEXCUIKLPSBRYWRIEPITSNYIMOQGLRSCEHKWESYUCPIAWBFVDSXLZRQOJWYEBAGNVVCWLCTLS
SRYVHODXIUIMRCJKXREGCGLORXYOXKCVSGXYSCMKIWIWNYIYRHYIINLMMKSPEPYDIXTWIWJSNMNVTYSWCS
```

```
POPPUZRDEBNJJSNMNVTYSWCSPOCCJYIBTIRKWPIRCKIZOWMZFVEOYPWKNHNYIONGLPTDISHRRNDIWICZTM
IEEVGSLZXRMWQYMMHGIIVOSTIEHDOIUTLUECEVCCAVYZQZOVNRRDAWWZTREVMNMDHSOKZKRMUSPOKISJ
GKNFYKVSVMUCPIBVIBIXWMNYSXLCNYIUNSQCINGIIWXREGCGLORYMVHKNHUIIDHILVJYRIOJIVEWMFVOVIHTS
ENXYITBOHOTXSVIZFVWOWNGYBPSMVWRIWNFVSCEFCCMITBVVCWILVSPTIHLWODHCIIMTPSWSBERWICZTMI
ESBDIWICZTMIEASTLILXKDHCKMYNEFGVYCIXLVOSWOTLKSEOKLONXCTEDISHFVSNXYXVSTCWYIMKWGVWCA
KYTPKIVY
```

Pour les questions suivantes, nous vous demandons de **bien justifier vos réponses en donnant tout le calcul intermédiaire qui vous amène à la conclusion**. À noter que des réponses sans justifications ne vous donneront pas des points.

1. **(2 pts)** Utiliser le test de Friedman pour estimer la taille de la clé sachant qu'elle est inférieure ou égale à 9.
2. **(3 pts)** Utiliser l'indice de coïncidence mutuel pour trouver la clé et décrypter le message. L'indice de coïncidence mutuel devrait être utilisé pour trouver le décalage des colonnes par rapport à la colonne 0. Par la suite, en vous basant sur la lettre la plus fréquente dans la colonne 0 et celle dans la langue d'origine, vous devez calculer la valeur K_0. À partir de K_0 et des décalages, vous devez calculer les autres valeurs de la clé et décrypter le message.

Remarques

1. Le travail est à effectuer de façon individuelle.
2. Les langages Python, C, C++ ou Java sont permis.
3. Le barème est donné à titre indicatif.
4. Attention au plagiat ! Faites vos TPs par vous-même.

À remettre

Utiliser le site web du cours pour remettre un seul fichier ".zip" (de taille maximale 40 Mb) qui porte votre nom au complet et qui contient un répertoire par exercice. Quand il s'agit d'un exercice de programmation, le répertoire en question doit contenir l'exécutable aussi bien que le code source **bien commenté**. Retourner un fichier ".pdf" pour l'exercice 1 et un fichier ".pdf" pour l'exercice 5. Les réponses doivent garder les mêmes numéros que les questions.

Échéancier

Le 27 octobre 2022 à 23h59. Une pénalité de 0,0028% de la note sera appliquée à chaque minute de retard (l'équivalent de 0.166% par heure), et ce, pour un maximum de 48 heures. Après 48 heures de retard, la note sera de zéro. Par exemple, pour un étudiant qui a eu 8 points, mais avec 5 heures de retard, sa note sera 8 - 8*0.166=6,68.