CRYPTOGRAPHIE
TP N°1

Objectif du TD: Voir quelques algorithmes très élémentaires et faire un peu de cryptanalyse.

ENONCE :

Il s'agit d'implémenter le chiffrement par substitution monoalphabetique simple. Dans ce type de chiffrement, une lettre est remplacée par une autre (il y a bijection entre les deux alphabets).

Faire une classe permettant d'utiliser ce type de chiffrement.
Voici quelques indications (non exhaustives). Il faut :

- une table de correspondance lettre a lettre.
- Une méthode chiffrant un texte clair (si un caractère ne fait pas partie de la table, on le laisse intact dans la version chiffrée)
- Une méthode de déchiffrement (si un caractère ne fait pas partie de la table, on affiche un « _ » a sa position.
- Une méthode d'aide a la cryptanalyse qui compte la fréquence d'occurence de chaque lettre.
- une méthode d'ajout de correspondance lettre a lettre

Exercice 1 :

- Testez votre classe avec un chiffrement / déchiffrement d'un texte de votre choix en utilisant une table de votre choix.
- Utilisez votre classe pour implémenter le code de Cesar (décalage de 3 lettres). Tester votre classe pour le chiffrement et le déchiffrement d'un texte de votre choix.

Exercice 2 :

Déchiffrez le message suivant :
Notez que les lettres les plus fréquentes dans un texte en francais sont dans l'ordre ESANTIRULO.

LVJB DJ BVX YHMSJ LM XHSXRMB LSBYVAVCMB: DJM YRKCK CADZDMM, YASBM LVJB DJ BCDLSK L'VCHVJCSX XSCO LVJB HM XKDAVJC LMB VJJMMB ZDVAVJCM. SH B'O CAKDEM MJ YHDBSMDAB MGMIYHVSAMB VBBSB VDCKDA L'DJM CVWHM, XRVZDM SIVQM BVSBSM BKDB DJ VJQHM YVACSXDHSMA LM BKACM ZD'KJ XAKSC L'VWKAL ZD'SH B'VQSC L'DJ QAKDYM L'SJLSESLDB LSNNMAMJCB. H'KWBXDASCM ZDS HMB MJCKDAM, H'SIIKWSHSCM XKIYHMCM LM HMDAB YKBM LKJJMJC H'SIYAMBBSKJ ZD'SHB BM BKJC AMDJSB HV YKDA DJM BMVJXM LM BYSASCSBIM. MC YDSB BS KJ AMQVALM WSMJ KJ B'VYMAXKSC ZDM XMB RKIIMB BKJC CKDB HM IMIM RKIIM. HV BMVJXM LMESMJC EAVSIMJC IMLSDIJSZDM, XKIIM B'SH JM B'O MCVSC AMJLD ZDM YKDA B'MEKZDMA HDS-IMIM, YKDA BM AVYYMHMA L'MJCAM HMB IKACB, XKIIM BS, MJ BM IDHCSYHSVJC, SH B'MCVSC SJXKJBSLMAMIMJC NVSC LSBYVAVSCAM. SH MBC HV XSJZ NKSB, IVSB HV JVCDAM LD CADXVQM AMJL SIYKBBSWHM CKDC MXRVJQM LM AMQVALB MJCAM HMB YMABKJJVQMB. XRVXDJ MBC XKJLVIJM V NSGMA HM ESLM, XKIIM BKDB HMB OMDG LMB VDCAMB, IVSB BVJB ASMJ EKSA, V TVIVSB SJXVYVWHM LM JM ASMJ EKSA. X'MBC DJM AMYAMBMJCVCSKJ LM HV IKAC, HM YKACAVSC L'DJ RKIIM SJESBSWHM.

MGCAVSC LM CRM SJEMJCSKJ KN BKHSCDLM LM YVDH VDBCMA.