TP3 : Cryptanalyse de chiffrements affines (problèmes)

Vous déchi□rerez les deux textes ci-dessous. Pour *justifier* la solution de ces problèmes de cryptanalyse vous pouvez utiliser :

1. les programmes disponibles sur le site

   `http : //www.apprendre en ligne.net/crypto/menu/index.html`

2. des calculs e□ectués à la main ;
3. des calculs e□ectués avec des programmes que vous avez conçus.

Dans votre rapport (max 2 pages), vous expliquerez la méthode de cryptanalyse utilisée et vous joindrez éventuellement en annexe les programmes utilisés. Une démonstration à l'ordinateur sera possible lors de la soutenance.

Hypothèses

On peut faire les hypothèses suivantes :

1. Les textes clairs sont en anglais ou en français.
2. Dans le texte clair, les espaces, la ponctuation et les accents ont été éliminés.
3. Les espaces dans les textes chi□rés servent uniquement à améliorer la lisibilité.
4. Si nécessaire, on associe à la lettre 'A' la valeur 0, à 'B' 1, jusqu'à 'Z' 25.
5. Les méthodes de chi□rement a□ne utilisées sont parmi les suivantes (voir cours) :
   (a) chi□rement par permutation (ou transposition) ;
   (b) chi□rement de Vigenère ;
   (c) une composition des deux méthodes précédentes (pas forcément avec la même période) ;
   (d) chi□rement par décalage (César) ;
   (e) chi□rement de Hill ;
   (f) une composition des deux méthodes précédentes.
6. Dans l'un des deux cas le chi□rement du texte :

   ```
   LATOUTNESTQUORDREETBEAUTELUXECALMEETVOLUPTEVOISSUR
   CESCANAUXDORMIRCESVAISSEAUXDONTLHUMEURESTVAGABONDE
   ```

   produit le texte :

   ```
   LVARU ZLFRE HIPJW UHKXL WRBCL NLOVQ RFYWS RORPB LWJVT MATCK
   RVVHV MXQVP AGKZF YPBUZ NBTPD FTGDF TDZEP QOFJX GUNIF GXGUA
   ```

Texte chi□ré 1

```
VXWGG BFMEW MESZZ TVMAM IKXIP XABIJ CPHOH ALALM UMEWT SQLKP
APLEX CYKLP GVIJN ZLHLX GSBEP FDTEG AIIOL KPQLC QXQNP SEERP
PSZTI ISHRH MIDLL TLXFW LGOCX WTXHW ZPAFJ FUOPX GAIXX GQXRP
DIYXO MONGO MWFPZ YBYZJ JLLIA QGVNL ZSSOQ NXWEU LDVED AZXGL
SCLRK XLRFR USPRD UKMFH MJURS SCLRK KYRSE BXWPM QTOUW TNYJQ
CISSQ LGVFT PYNVX VNXBV ALKUQ ZFODV RSPUF SUSGQ WUWVQ AWUVF
QPLYD ENCGM OHDWP QNQRY FJDTJ HCNYR CYCGH RODDZ EOYTV ESKSW
UDOEG UPBAL BIMCL SUSVV MZGZU NXWBK HGNKN HVTPW CKBAH KGEPE
QYIIB GIRVJ FLGMR OHMYM SCSGA MVSUM KBEGS NVRMC KTYHX BTWSH
GHOMY ARDSP XHCWE ZFANW UCKWN CXZSJ CFNGX PMRRD AWUEZ IGIGA
KAJPX ABLSV ONPXM RDQAY KSHAR OMDML URYEG WSGLN HAVQL QMMWN
VUHMX ZVKPF WGKRW FLPKM UQIQC GLMYU JQFVL GPWPM DONBU USGPD
JQQBE NQZNT IYFXZ UTSTE PIASG RBEVZ AMJCU QPTCH BJNML TLZBQ
TYZYH PRKAE QBTFW SCTZZ DDEHK GNQZG UAXCZ GGRCF WLYTA JDCHT
NCZIJ RDGUU KPEJI SPALV FEXDM AJMCA BUUCO VRXJI GFLRU MELLT
KPQLC VIXOF FVCTR BRRTH FOFCF GSIEH AIIZP CXACS CDQLE VHONG
YGOHI XSLPT SQPDL FVNSY CSWIK FXLTK SIXQO DZKSK KGWHJ LPPAS
VNPUM MKGJM ZBDVO ZBXFN VLOOB
```

Texte chi□ré 2

```
BOQJV TWYUW BUYJX DSIIY RCBNP GQKIY MRSIZ YWWQQ DDIUV YAFTO
ZOIBM FHGDO ICVRX SJPIU AHJCI YWAQY DIRFW PQQAU DGHFW ZSOUY
VZIIX WFMTC IRYQB OZOMB HOTLM WVHDQ JGXTM NTBHX FFQFC HBVPP
MYBSB OVTID DSIMZ FMKQO NYQJC AUHUI VZQZJ ATIVL IEXIC PNZAR
PRYOV PYPHI VFYPI FBRJC QYIHT FYYRP INCUB OIPBD PSVWP ZBHJH
WHICM ZISDC IEBAB EHOXP AYUSU XYPMK NSUMW PFQJF UCRFA GKFJI
VNMRJ BSXRP YRJFI OZDMB UCVMY YMHGN JNNTM CJCEL PCTHT GBPIP
MBCWB XIFKF CBDHS ZVADB UYZUV CJCUR XYWVI SJFYN VWTOU RIBDH
TSGOG PMIJX QOMZA OXSTN QWIYT WGMVF AIQSE REJMH BIUYB EWZUB
YOVZZ BPITG
```