CSE 599R, Cryptanalysis, Fall, 2008, Homework 3

John Manferdelli

Due: October 20, 2008

1. How many alphabets are there in the following poly-alphabetic cipher? How do you know?

```
KONKA NMRZO PHNON AYEPP FHHBF YHBTA OLDET KMBHV
WBRAT EGHYE HMFHX HPVXU FUKLE OYAAM LHIYX YNUMA
TAMHU NMUAM TAFEK ATAMI AODDM SFHPE UFYRF HDKMD
MIGHZ DALFO EKFHX ADUMO YABUX YMOQR XDMSM OUNZZ
IHBJT HXZFR XAOHX KNUMT MIGSK HXAAL WATEM YGTAA
TAMPE NHATI GNUNX CQRLL QNTUK BHKKB NAXIX KANXA
UMXVD AGVFH XYIIM OAUMP FWTZM UGABO ESKOK ATEPP
POPVD MTFNE FHDYT BZTIV XLRAA MLHGN MWALE FEHXP
EAGKY AKFMN WATEP PPOPK AUZSM SBZML EAALW HNONA
UNMOM TUVAK POUCA PEMHZ FLRHF RNLNO HRIIM OEOFL
ETKLF CALDS TZUST PPBXM ARXUA WMOQW TFFHT AFHXI
AODDU NWZGP BZFHB ZFOFH ZDFLR ONUPT ALYOG LKTAH
FTALD OUIQR LOUDB UFHXJ MVXHZ DBAYA WLGSK POHPL
SOMZU XMOAU LHZDW VXLTY EAIPQ CXHXL ZVXDB AIALH
ZAPMG LLPSH MVRMH UQYPO QNBAI ALWUL XKGPP LXLCB
PGXAT AMJTE KOQTH VWIMH ZDIBF IMVGT TAUNM LDELA
MNWPF FXAOH XKGST KALEH DAWHK AIPQC XHXLM OQYXH
DRHBZ DFVDE MOMNT IADRJ AUEKF EESIH TAFOW VIIMO
FHXDU DHDPO NNXAL ZTEMV AKFLR OKOQR LVZAG KMLEV
IEWZT EPVGL WZUVB SUZXT QBNAU TPHER HBSHE PHIGN
UNMOQ HHBEE TSXTA LFIFL OOGZU DXYUN ZOAWW PEMTS
DEZBX AKHZD WLOEG AFHXD UDHDI ALPZA ESTEK DMYLH
ZDLVI HXUUC HBXDG AETTU PIMUA LHUSE KPXIM VGTBN
ATBUF OFFAL WYMGL HZDFF EUZHD HHNEH XHPAZ HUNTU
PWTZR RXLMN WZMTB ZRIXK NUMAA MLHIY XYTEA BZTXK
YENWM NWZMI WOQWT ZSOBU STHZF AKAMB TUPOY YABUL
DSTUP IFPSH MQAIG PRIPV GLWNA BTJWT HATEP PPOPH
ZDULD ELWQC MHNLX ZAIPL ZTUHO K
```

2. Trappe and Washington, Chapter 4: 4, 5, 11.

3. Exploring the DES component permutations. In this problem, permutations are applied from the right. Let $\Omega=\{0,1,2,3\}$. $\Omega^2= \Omega \times \Omega$. Define:

   $\sigma^f{}_i$: (a,b) → ($a \oplus f(k_i \oplus b)$,b).

   τ: (a,b) → (b,a)

   a. How are wt((a,b)) and wt(τ(a,b)) related? (wt(x) is the "weight" of x, that is , the number of 1's. It is also called the "Hamming weight".)
   b. How are wt((a,b)) and wt($\sigma^f{}_i$(a,b)) related?
   c. Write τ as a permutation of S_{16} in cycle structure.
   d. Write $\sigma^f{}_i$ as a permutation of S_{16} in cycle structure, f(t)=t and k_i=0.
   e. Show τ is similar to $\sigma^f{}_i$ and thus $\tau\,\sigma^f{}_i=[\tau, \alpha]$ for some α in S_{16}.
   f. What is $C_G(\sigma^f{}_i)$ and $C_G(\tau)$, G= S_{16}.
   g. Now set $t=t_1||t_2$. $g(t)= (t_1t_2, t_1)$. $h(t)= (t_1t_2, t_1\ t_2)$, and $k=2=0010_b$. Calculate $\sigma^g{}_i$, $\tau\,\sigma^g{}_i$, $\sigma^h{}_i$, and $\tau\,\sigma^h{}_i$. Speculate on how the value of k changes the cycle structure.