

LING 106: Homework 3

Due: Friday, February 6, 2009

1. CRYPTOGRAPHY

1.1. *Deciphering Texts*

The three texts in (a)-(c) on the next page, presented in alphabetical order and with their letter frequencies in boxes to their right, represent three different encoding methods. Each one is a 365-letter paragraph from the same best-selling novel from which spaces and punctuation were removed, an encryption performed, and the resulting string broken into 73 five-letter chunks. The three encryption methods, in no particular order, were:

- (i) A rearrangement encryption
- (ii) A monoalphabetic substitution cipher
- (iii) A polyalphabetic cipher

For this assignment, *you do not need to decipher the texts*. Instead, answer the following question: which encryption method produced each of the three ciphertexts? How can you tell? (Full sentences, please.)

a. CBWRP TWIFE IGQBR TQEJN TWZCC JEHVG KFLDY XUGFN
 JLHRK GMENP NVZMC TVVPX YGHWN URGSM LRTVY GXQNP
 PJTOI YUFDX GZBNM CBXRG VYMJL EAFJM UHTHU UCXFI
 ZDVPH TVROR PGBIQ JRTTY EZKCG TLEAF UMVHH FYFPZ
 BRGJV GGHAA EFKBN RVVZC HHXUG IQRAS BUVJX OIFQW
 YHVG KTGHF AVVYG CHYEE CMXLX RTVBG XWVHV LRXLN
 NCQIA IFGTF DBGRU RPTII EUFLP EFHVV TTKCB PVGCH
 THUUC XLLNT VQIAI TQRJD YFRVK CGBRT VYCLH VYFSW
 SHMAI KFTPS EMFDV HHFWI CARXU KJGHT RNFDG GTFYG
 HSTLX

27: GV	13: EL
25: T	12: BNP
24: F	11: J
23: H	10: AM
21: R	9: KQ
17: C	8: W
16: I	7: DZ
15: X	6: S
14: UY	3: O

b. LOFNT BRTCI ECPIE EUSNH ESERH DTNIO PEEDL SDEHL
 WPUIT DOAEH NOYVL FREIB YSHRT RAERU NTRAN EGHUT
 EODWO TDNLS OEANL XIEEE NVFAE MIOLO WEDER NNWHR
 NNEEN BIETE DSOCE ADHEY RISEH FNWEA ITUAI EANHN
 TYTMW DTIPN HNREI DRMSD GANEW ABODT I I IDT CCSSES
 HEATS LLSRB EASEE TAEAG ALNNF NNNNS CEOIT AEHSH
 FLGII CCTIA BAEIN VDOSO FLENS EESOT MIIEN COYOA
 AVUYL TBDBT SCDSI YGOAD CCAED TRRSO OPIEO TDNOT
 YSTLN OEGIT RAFOY RETSV TNIAN BOPHH MGSTA TAWHU
 JEHUE

50: E	14: L
33: N	12: C
31: T	9: BY
27: AI	8: FUW
25: O	7: G
24: S	6: P
20: D	5: MV
18: H	1: JX
17: R	

c. QAYYW ECQGY ITQAB PGEIT RJIMY CEGGY RCJMM YCQGX
 VEOEM JSIRP BPQYY IASIR MYRPY YQQAY GYITQ AJPQA
 MYYVE OABIT QJIHJ ISHYI QOGEB RYIRQ JYIRY LSEGG
 XNMYE QAQEF BITVE OQAYC JMMBR JMOV B RQAVA BCAYE
 OBGXC JSGRA EUYEC CJHHJ REQYR OBRYN XOBRY KEOOY
 ITYMQ MEBIO QAYCY IQYMJ PQAYA EGGVE XVEOR JQQYR
 NXQAY JCCEO BJIEG OQEQS YJMCJ GJOOE GKJMC YGEBI
 SMIVA BCAOY MUYRE OEQEO QYPSG RBUBR YMEIR FYKQQ
 AYPGJ VJPQM EPPBC HJUBI TRJVI JIYVE GGEIR SKQAY
 JQAYM

45: Y	16: C
33: Q	11: PV
32: E	9: S
26: J	7: T
25: I	6: X
23: R	5: H
22: A	4: KU
21: G	3: N
20: M	2: F
19: BO	1: LW

1.2. Enciphering Texts

Two people—call them LN and MDN—are sending each other encrypted messages. You’ve figured out how to intercept the first message of the week, from LN to MDN, and you would like to send an encrypted message back to convince LN that you, in fact, are MDN.

Unfortunately, their encryption method changes weekly, and always leaves out punctuation. Fortunately, the method is never complicated, and always includes spaces. Even more fortunately, your sources have informed you that the first two messages sent each week are the same. (You’d think LN would know better.) They are:

- (1) **the quiz is ready in the secret mailbox. we need to make copies before wednesday.**
- (2) **give me the key and i’ll do the job.**

Below are the first messages posted on Monday morning of five consecutive weeks. Your task for each message is:

- (i) Give the enciphering function, or otherwise describe the enciphering procedure;
- (ii) Give the appropriate reply, i.e. the result of enciphering (1) via the method in (i).

Week 1

eht iquz is adery in eht ceerst abilmox ew deen ot aekm ceiops beefor addeenswy

Week 2

htq eiui zr saeyd ni hts eceerm tiablxo ew ende ot amek ocipse ebofer ewndseady

Week 3

geb nrfw fp obxav fk qeb pbzobq jxfiyly tb kbba ql jxhb zlmfbp ybclob tbakbpaxv

Week 4

ht4 l13b 3j k45xc 3n ht4 j4yk4h p53qz2d f4 n44x h2 p5r4 y2m34j z4w2k4 f4xn4jx5c

Week 5

ord jsea cs inkob xs ord dobmoc hylvskw og noox yd oukw coszym obypol ikncoxnog

2. LINEAR B

Below are ten Japanese words, written first in a writing system called “Brae Nil”, and then (in random order) in the English alphabet along with their rough translations.¹ **Please note!** Brae Nil bears a strong resemblance to Linear B—in fact, it uses the same symbols, but they have different values. Do not attempt to look up their Linear B values; it’ll go badly.

⊕ ⊥ ⊥

⊕ ⊕ ⊕ ⊗

⊕ ⊗ ⊕ ⊕

⊥ ⊥ ⊗

⊕ ⊕ ⊕ ⊥

⊥ ⊕ ⊕ ⊗

⊗ ⊥ ⊕ ⊥

⊕ ⊕ ⊗

⊥ ⊥ ⊗

⊕ ⊥ ⊕ ⊥

kimono ‘robe’

orikami ‘paper-folding’

satori ‘enlightenment’

kamikaze ‘divine-wind’

samurai ‘warrior’

karate ‘martial art’

ikepana ‘flower arranging’

tamari ‘soy sauce’

karaoke ‘empty-orchestra’

katakana ‘writing system’

Question 1: Write the following non-Japanese words in Brae Nil.

Naomi _____ mimosa _____

Question 2: What five-letter English word is $\oplus \oplus \oplus \oplus \oplus$ intended to represent, and why is it wrong?

¹ Note: the words written as *ikepana* and *orikami* are actually *ikebana* and *origami* respectively. As Linear B (and thus also Brae Nil) uses *p* to represent *b* and *k* to represent *g*, I’ve written them here with *p* and *k* for simplicity.