Practice for 3rd quiz

1. The following two cryptograms have been obtained by substitution ciphers

PMZMRQNGRQWMSYEYGLQRCTGJPMZMRQUFMYPCRPWGLERMI
GJJWMSUFGAFGQUFWRFCWYPCCTGJDMPRSLYRCJWDMPWMSC
TCLRFMSEFRFCWYPCCTGJRFCWYPCLMRTCPWZPGEFRYLBFY

WWAOIYCVSEGVSIRLOPGDGFNIHRKRSSGFCIGIHZURSTQMA
VPDSUVHOKAOITQNGLNTOJQLWKCIFVKNGKTUQKKOBSQOYZ
PCOEHISCFTOSNEOLEAFUUMOPDEPLKLHFPEOTJOHYGRRFY

determine which of them was obtained by a monoalphabetic substitution.

2. There are two women who make the following statements

A: "I have two children. My eldest one is a girl."

B: "I have two children. At least one of them is a girl."

Assuming that the births of the two children are independent random variables, with each sex equally probable, draw a crippled wheel for each of the two women and deduce from the resulting pictures which of the two women is more likely to have two girls.

3. Suppose you are given a ciphertext containing 1000 letters which you know has been obtained by a polyalphabetic substitution. Suppose that your letter counts reveal that the sum of the squares of the letter frequencies is 41796. Give an estimate of the period of the cipher used.

3.5 Decrypt one of the cryptograms given in problem 1.

4. The text below is the initial portion of a certain ciphertext obtained by rectangular transposition with period 5.

A L C R H B B E A S G I B E A H U S E T I P N S D

Suppose that the program "breakrt" described in class produces the matrix of statistics shown to the right. Decrypt the cryptogram.

Matrix of statistics is:

0.0000	12.0360	13.7375	18.0705	10.7388
9.9680	0.0000	13.1482	11.0133	10.1024
10.4562	13.5256	0.0000	12.1575	17.1928
13.8223	19.5247	11.3581	0.0000	12.3376
17.9408	13.1287	12.3990	12.4562	0.0000

5. The following two cryptograms have been obtained by substitution ciphers.

LWVMF DWKKL ZWKUJ WWFKM XXWJK GDTGM JFWUG EHMLW JAFUX WTJMS JQTSU CYSEE GFYSE WKSFV
TSUCY LKESQ ZGJJW FVGMK ESDSV QSDKG SFQHG HLAGF WAYFG JWVIM AUCJW XWJWF UWOZW FTSUC

VMFJR YWLQX IYVXR TFXIZ QWTSH TODVM BWHER UXQEY WWFZU FANXK AXPSN XRWTL UIUYQ ICPVW
ACBFU EVSMP DVEGH VYNRR VPQME YWGOY VMSER JNORR TLVOF ZUVUW HWOCL RSEUY CELSN

Find by means of repeating letter statistics which of them was obtained by a plurialphabetic substitution?

The index of coincidence for the first message is approximately 0.054 and the index of coincidence for the second message is approximately 0.037. What conclusions can you draw from these numbers?