

MCS 425 Exercise Set #1 — Spring Semester, 2008

This assignment is due in class on Monday, Feb 4. Page and section numbers refer to the textbook, Trappe and Washington, 2nd Ed.

Sec 2.13, pages 55–56, exercises 2, 4, 8.

Sec 2.14, page 59, exercise 1.

This doesn't require a computer. You might start by considering the just the first three letters of the ciphertext. Write down the 26 possibilities for the first three letters of the plaintext. All but a few are very unlikely (assuming the plaintext is English language text). For the few remaining possibilities, decrypt more letters from the ciphertext.

Exercise A Consider a channel with white noise, with $p = 0.2^1$. We want to use a repetition code R_m (m odd) to correct errors, so the probability that an uncorrected error occurs in transmitting a bit of the original message is less than 10^{-2} . What is the smallest value of m that works?

Exercise B The 930–letter cipher text below was encrypted using a substitution cipher. You may find a copy of this same ciphertext in file **exerB-ciphertext.txt** on the MCS 425 web site. Using a frequency analysis, possibly together with other means, break this substitution cipher. Find the key and write at least the first three lines of corresponding plaintext.

You will find links on the web site to tables of letter and digram frequencies in this ciphertext.

```
ZRGGBRABFJRAPZKIZQYNRYQAFJKRTADKAZTISRGGRXPIITIYXDQXRI PZRTKRK
IXJIWORXZKRPIBAFJZADYAPZTACBIYCWQZQRJXQXKRSQJQZIIYXBIYCDRTRZK
RYIZQAYJDQZKDKAJRBIYYRTJIIYXWFJZABJKRDIJIWLFIQYZRXBATRASRTKRJ
FPPRTRXBFWKHCJRIDKQGRZTCQYNZAJISRKQJADYGQPRIYXHTQYNKQJBRYJIP
RGCKABRHFZXDADKIZKRBQNKZKRWAFGXAZJISRKQJBRYPATZKRCURTQJKRXXZK
TAFNKZKRQTADYJKRRTPAGGCQYRIZQYNZKRWIZZGRAPZKRJFYNAKXCURTQAYJ
AZKRNAXUTRSRYZRZXKRBPTABRSRTTRIWKQYNKABRZRGGBRZAAIHAFZIGGZKR
JRZKQYNJAKXIFNKZRTAPMASRPTABDKIZJARSRTJAFTWRCAFBI COYADZKRBJA
YADIGGDKARJWIURXXRIZKQYHIZZGRATHCJQUDTRWOKIXNAZJIPRGCKABRRV
WRUZFGCJJRJIYXKRZKAFNKKRDIJGAYNQYNZATRZFTYZAKQJDQPRIYXWAFYZT
CDIJXRZIQYRXHCZKRNAXXRJJWIGCUJADKAKIXNAZKQBQYZAIGITNRWISRIYX
DIYZRXZABITTCQQBHFZIJCRITJDRYZHCZKRTRWIBRIZQBRDKRYZKRNAXJJRZ
ZGRXZKIZKRJKAFGXNAHIWOZAQZKIWIRSRYZKRYKADRSRTDKRYKRDIJIBAYNK
QJADYURAUGRKQJZTAFHGRJDRTRYAZCRZASRTYRSRTZKRGRJJIGGZKRNAXJKI
XYADHRNFYZAUQZCKQBRVWRUZYZRUFYRDKAJZQGGURTJRWFZRXXKQBDQZKAFZW
RIJQYNIYXDAFGXYAZGRZKQBNRZKABR
```

¹ p is the probability that an individual bit is flipped (0 to 1, or 1 to 0) during transmission.