Cryptology

Homework 1

1. Suppose you are using a box cipher with 4 rows and 10 columns. Your plaintext is 31 characters long, so you have to fill in 9 dummy letters. If you want your cipher to be secure, why is it important to use different dummy letters instead of simply repeating one dummy letter 9 times?

2. It might seem that a shuffle cipher is “better” if no letter of the alphabet is encoded to itself; for example, the letter A in the ciphertext could never represent the letter A in the plaintext. Let's call such cipher alphabets “super-shuffled.” Explain why our intuition is wrong: it's (theoretically, anyway) easier for a cryptanalyst to break a “super-shuffle” cipher than a general shuffle cipher. A rough explanation is fine; you don't need to do specific calculations.

3. There is a variation of the Shuffle Cipher where you use a keyword to create your cipher-alphabet. Start with a keyword, such as TOPOLOGY, and remove any repeated letters; in this case that leaves us with TOPLGY. Write this down as the beginning of your cipher alphabet; then fill in the remaining letters in order:

   plain: abcdefghijklmnopqrstuvwxyz
   cipher:  TOPLGYABCDEFHIJKLMNOPQRSTUVWXYZ

Describe how you might pick a good keyword for this system. (Hint: why would ACE be a very bad choice?)
4. Decrypt the following ciphertext, which was created using a shuffle cipher. The letter frequencies are given below to help you out. It is not known if the person who created the ciphertext chose a letter to represent a space or if the spaces were left out; you have to decide which.

GAFSFWDSDFWZXJFWGAFXSFJZWBGHAWDWESXX
MWBAHRAWHZWXZAXSGWDQYWFCFTDQGWGAD
GWHGWZFFJZWNQCHVFCPWGADGWDKFGGFSWX
QFWBHCCWFUFWSKFWMXNQYWDFQFIDJEFCWHZ
WFNRCHYZWESXXMWGADGWGAFSFWDWHSQHQMHQ
HGFCPWFJDQPWESHJFWQJNKFSZWBFWBCCWZFS
FWGADGWESXXMWCDFSHQWGAHZWRCDZS

18% - W
12% - F
8% - G
6% - D, H
5% - S, Z
4% - A, C, Q, X
2% - B, E, J, M
1% - K, N, P, R, Y