Cryptology
Problems

To be discussed Monday, February 21, 2000.

1. This was encrypted using a Caesar cipher. Decipher it.
YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

2. This was entitled "Cold Country". It was encrypted using a monoalphabetic substiution cipher. Decipher it. TOWWJPHJC ZY RXW PHOTWYR ZYPHJC ZJ RXW SFOPC. UFYR FB ZR ZY QFIWOWC SZRX ZQW RXFMYHJCY FB BWWR CWWD.

3.Suppose you had two examples of ciphertext, both enciphered using periodic polyalphabetic ciphers. How would you make an intelligent guess as to whether or not the same sequence of substitution alphabets was used, without making any attempt at deciphering? Is the assumption that the ciphers are periodic necessary?

4. During lecture I stated that a linear feedback shift register sequence produced by a recurrence of degree n has period at most $2^n - 1$. Prove that the period cannot be longer than this. (Hint: consider the set of different values which could be in the register while the sequence is being produced.)

5. Give a linear recurrence of degree 4 and a seed which produce a sequence with period 15.

6. Suppose that a linear feedback shift register sequence is produced by a recurrence of degree n and has period $2^n - 1$. In general, exactly how many zeros are there among the first $2^n - 1$ bits produced. Prove your answer.

7. Choose some system which should have some security properties. Identify those properties and explain in what ways they might be violated.