Cryptology
Problems

To be discussed Wednesday, February 14, 2001.

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. This is from some material from the NSA. First they wrote, "The history of cryptography dates to the Caesar cipher, where each letter is replaced by the letter three positions away in the algphabet."... Then this followed. What system was used for encryption and what does it say?

VRRQ SHRSOH EHJDQ VOLGLQJ WKH DOSKDEHW EB DPRXQWV GLIIHUHQW WKDQ WKUHH WR GHWHUPLQH FLSKHU HTXLYDO-HQWV.

4. 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?

5. 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.)

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.

8. Try using Maple. To get started, you can use the weekly note for week 43, which I wrote for the students who took the IT course last semester. That note can be found at http://www.imada.sdu.dk/~joan/IT/notes.html. It was written for the WINDOWS system for the Faculty of Science and Engineering, so you can use your accounts on their system. Otherwise, those machines we have using the newest version of LINUX also have Maple and you can use that. It works for me to `xon octavian` and run `xmaple`.