Dr. R. Beezer
Practicum #3
Solitaire Stream Cipher

Math 133
Fall 2003

Solitaire (a.ka. "Pontifex") is an example of a stream cipher. A key is used to start a list of seemingly random information (numbers, or bits or characters), which are combined simply with the plaintext. The recipient of the ciphertext uses the same key to generate the same list and it is then a simple matter to recover the plaintext. So the security of this scheme relies on how the key is used to create the "stream" of information that appears random.

Procedure

1. Obtain the Solitaire algorithm description off the Counterpane WWW site (see course page for a link). You'll probably want to print it off. Or find it in the Appendix of *Cryptonomicon* (p. 1131).

2. Obtain a deck of playing cards, making certain it has two Jokers (and verify that somehow the two are really different).

3. Read the algorithm and practice generating the "keysteam" (the list of seemingly random information) by following the steps in the "Sample Output" section.

4. Everyone will receive a 10-letter messsage by email, which has been encrypted with your pass phrase (i.e. the key, see next item). Your message is guaranteed to be two legitimate 5-letter English words.

5. Your pass phrase will be the first letter of your first name, followed by the first letter of your last name. So my pass phrase would be RB. Check with me if you go by a nickname, prefer your middle name, or if there may be some other confusion about which letters you will be using. Note that a two-letter pass phrase is a very bad idea in practice! (Why?)

6. Key the deck using a pass phrase, as described in the third part of the section titled "Keying the Deck."

7. Send me the decrypted version of the message in an email, stating "Practicum 3" in the subject.

Grading

1. Once a day, you may submit an encryption to me for grading (include "Practicum 3" in the subject). I will tell you how much of it is correct. This is limited to once per day, for as many days until this is due. I'll try to reply promptly.

2. Full credit for a correct decryption. This will require twelve trips through the algorithm.

3. Once you make a single mistake, anything that follows will likely be incorrect.

Notes

1. Schneier's "Operational Notes" are superb. Read them, and the bit that precedes them about "Real Security..."

2. This entire algorithm can be described without reference to a deck of cards. Any set of 54 different symbols could be used. The real beauty of this algorithm is that the key can be transported (or saved) as a deck of cards, never arousing any suspicion. With just a pass phrase, the algorithm can be performed with a commonly available device, a simple deck of playing cards.