The Solitaire Cipher—Part II

Please refer to Lab 9, The Solitaire Cipher—Part I, where you’ve implemented step one of the encryption, as well as created a class for your deck of cards.

The Deck of Cards

Presumably you already have a deck of cards (contained in the collection of your choosing) which, initially unsorted would be in the following order:

1 2 3 ... 52 A B

We now must prepare the deck for the encryption process. We begin by using the deck to generate a keystream letter for each letter in the message.

1. Move the A joker down one card. If the joker is at the bottom of the deck, move it to just below the first card, that is, consider the deck to be circular. The deck order becomes:

   1 2 3 ... 52 B A

2. Move the B joker down two cards, again assuming a circular deck. The deck order becomes:

   1 B 2 3 ... 52 A

3. Perform a triple cut around the two jokers: all cards above the top joker move to below the bottom joker and vice versa. The cards between the jokers remain unchanged. The deck order becomes:

   B 2 3 ... 52 A 1

4. Perform a count cut using the value of the bottom card: cut the bottom card’s value in cards off the top of the deck and reinsert them just above the bottom card. If the card is a joker, do nothing for this step. The deck order becomes:

   2 3 4 ... 52 A B 1 (the 1 tells us to move just the B)
5. Find the output letter: count down \( n \) cards starting with the top card, where \( n \) is the value of the top card. Look at the card immediately after your count. Convert it to a letter. This is the next letter in the keystream. If the output card is a joker, no letter is generated. For our deck, the output letter is

\[
\text{D (the 2 tells us to count down to the 4, which is a D).}
\]

6. Repeat these steps as many times as is needed to generate an output letter for each letter in your message encoded using step one from last week. That is, for the message

CODEI NJAVA LIVEL ONGER

we should have to generate 20 letters, the first few of which are

\[
\text{D(4) W(49) J(10) Skip Joker (53) X(24) H(8) Y(51) R(44) F(6) D(4) etc.}
\]

yielding the keystream

\[
\text{DWJXH YRFDG TMSHP UURXJ}
\]

**The Remaining Encryption**

1. Convert the formatted message (see lab 9) into numbers, A = 1, B = 2, etc:

\[
3 15 4 5 9 14 18 21 2 25 12 9 22 5 12 15 14 7 5 18
\]

2. Convert the keystream letters using the same method:

\[
4 23 10 24 8 25 18 6 4 7 20 13 19 8 16 21 21 18 4 10
\]

3. Add the message numbers to the keystream numbers and subtract 26 from the sum if it is greater than 26. That is, \( 26 + 1 = 1 \) \((27 - 26)\). You may also use the modulo operator for this step.

4. Convert the numbers from the sum back to letters.

\[
\text{GLNCQ MJAFF FVOMB JIYCB}
\]

Congratulations, your message is encrypted!
Decryption

1. Use Solitaire (the above deck) to generate a keystream for the letters in the message to be decoded.

2. Convert the keystream letters to numbers.

3. Convert the message to be decoded to numbers.

4. Subtract the keystream numbers obtained in step 3 from the message numbers obtained in step 2. If the result is negative, add 26: 1-22 = 5.

5. Convert the resulting numbers back to letters.