

Solitaire Cipher (Part 1)

The Solitaire Cipher Scheme by Bruce Schneier

Solitaire is an output-feedback mode stream cipher. Sometimes this is called key-generator (KG in U.S. military speak). To encrypt a text message, Solitaire uses a key to generate a stream, often called a "keystream," of integers between 0 and 25, converts the characters in the original text message to integers between 1 and 26 (A=1, B=2, etc.) and combines these two sets of integers to produce a new set of integers. Decryption is essentially this process in reverse. The scheme depends on both the sender and the receiver knowing the original key used to generate the keystream. The name Solitaire comes from the use of a deck of cards to generate the key.

Encrypting with Solitaire

For example, to encrypt "Do not use PC":

1. First, remove the spaces in the plaintext message and convert all characters to upper case.

DONOTUSEPC

2. Use Solitaire to generate one keystream letter for each message letter. (Details follow the description of Decrypting.) For this example, assume they are:

KDWUPONOWT

3. Convert the plaintext message from letters into numbers where A=1, B=2, etc:

4 15 14 15 20 21 19 5 16 3

4. Convert the keystream letters similarly:

11 4 23 21 16 15 14 15 23 20

5. Add the plaintext number stream to the keystream numbers, modulo 26. [I.e. Zero is not a valid number. Modulo 26 produces a number in the range 1 to 26 inclusive. Basically, if the result of the addition is greater than 26, subtract 26 from the result.]

15 19 11 10 10 10 7 20 13 23

6. Convert the numbers back to letters (1=A, 2=B, etc.) and the message is encrypted.

OSKJJJTMW

Decrypting with Solitaire

The basic idea for decrypting is that the receiver, starting with the same key, generates the same keystream, and then subtracts the keystream letters from the ciphertext letters.

1. Take the ciphertext message.

OSKJJJGTMW

2. Use Solitaire to generate ten keystream letters. If the receiver uses the same key as the sender, the keystream letters will be the same:

KDWUPONOWT

3. Convert the ciphertext message from letters into numbers:

15 19 11 10 10 10 7 20 13 23

4. Convert the keystream letters similarly:

11 4 23 21 16 15 14 15 23 20

5. Subtract the keystream numbers from the ciphertext numbers, modulo 26. For example, $22-1=21$, $1-22=5$ (I. e. If the first number is less than or equal to the second number, add 26 to the first number before subtracting. So $1-22=?$ becomes $27-22=5$.)

4 15 14 15 20 21 19 5 16 3

6. Convert the numbers back to letters.

DONOTUSEPC

As you can see, decryption is the same as encryption, except that you subtract the keystream from the ciphertext message.

The Key and Class Card

When the program starts, a deck of 54 cards (including 2 jokers) will be loaded from the text file “key.txt” (the data file provided during setup) into a data structure of your own choosing. The first card read from the file into your data structure will be the first “top” card and the last card read from the file into your data structure will be the first “bottom” card. Each line in the file contains two characters. The first character represents the suit of the card, the second character represents the value of the card. Suit are as follows:

'C' – clubs, 'H' – hearts, 'D' – diamonds, 'S' – spades, 'J' – joker

Start suit card values are represented as follows:

'A' (ace), '2', '3', '4', '5', '6', '7', '8', '9', 'T', 'J' (jack), 'Q' (queen), 'K' (king)

One joker will have the value 'A', then other will have the value 'B'. (This allows the algorithm to distinguish between the two jokers when needed.)

Each card is represented in the program by an object of class Card. Class Card must represent one card. It must include private data members of a character (char) type to represent the suit and value of a card. (See suit and value description above). Class Card must contain constructors and / or method functions to set and retrieve the the values of the private data members (i.e. constructors, getters and setters).

In addition, class Card must include a method function that returns an integer value from 1 to 26 based on the combination of the stored suit and value. If the card is a club or a heart, it is the value shown [note: ace=1, Jack=11, Queen=12, King=13]. If the card is a diamond or a spade, it is the value of the card plus 13. Jokers have a value of -1, which will be used only to determine when to skip jokers. [The jokers values of 'A' and 'B' will be used at a later time.]

Generating the Keystream Values (version for solution to problem #14)

This is the heart of Solitaire. The above descriptions of encryption and decryption work for any output-feedback mode stream cipher. For this version, a very primitive keystream algorithm will be used.

1. The first time a keystream value is required, the “top” card in the data structure is selected. Each time following the first time that a keystream value is required, the next card in the data structure is selected. If all the cards are used, the keystream starts over with the first card.
2. Unless the selected card is a joker, the integer value [from 1 to 26, see discussion of method function in class Card] of the selected card is returned as the keystream value. If the selected card is a joker, the next card in the data structure is selected.

Solution

Write a program to implement the Solitaire Cipher Scheme as described above. The user may select to encrypt plaintext to ciphertext or to decrypt ciphertext to plaintext. Note that encryption and decryption rely on starting with the same key.

Example run #1:

1-Encrypt, 2-Decrypt: 1

Enter plaintext in caps with no spaces: DONOTUSEPC

RQQQSHPNRC

1-Encrypt, 2-Decrypt: 2

Enter ciphertext in caps with no spaces: RQQQSHPNRC

DONOTUSEPC

Run your program with the following test data. Encrypt plaintext, then decrypt the ciphertext:

Test Run: IAMREADYTOBEASPY

Submit a printout of your program code and a printout of the runs of your program using the test data. [A printout of a screen dump is OK. “Copy and Paste” of text output to an editor, then print from the editor is also OK.]