Solitaire Cipher

Grace Cantarella and Anna Zhang

History

- Designed by Bruce Schneier for Neal Stephenson's novel, *Cryptonomicon*
- Requires only a deck of cards to encrypt/decrypt, as long as the sender and receiver have identically ordered decks
- Was intended to be the first truly secure hand cipher
- Was originally called Pontifex to hide that it used playing cards
- Playing cards are less incriminating (and less expensive) than electronic devices

Method

- The sender and receiver agree on an ordering of the deck (often, a keyword is used instead)
- Using the ordered deck, the sender generates a *keystream* (a list of values between 1 and 54). The keystream is the same length as the message
- One keystream value is generated in five steps (the *Keystream Algorithm*)
- Convert original message and keystream to corresponding numerical values (A=1, B=2, etc), add (mod 26), and convert back to letters. This is the ciphertext!
- The receiver receives the ciphertext and also performs the keystream algorithm, ending up with an identical keystream as the sender. The receiver subtracts the keystream from the ciphertext to find the original message.

Keystream Algorithm

1. Move **Joker A (card 53)** down one place in the deck
2. Move **Joker B (card 54)** down two places in the deck
3. **Triple cut**: exchange the sections below the bottommost joker and above the topmost joker. The jokers and everything between them stays put
4. **Count cut**: find the value of the card at the bottom of the deck (either joker = 53). Take that many cards from the top of the deck and place them above the bottom card
5. Find the value of the top card (either joker = 53). Count this many cards below the top card. The value of that card becomes the next value in the keystream!
    - If the card is a joker, disregard and repeat the algorithm (this way, each letter is represented by exactly two cards)

Disadvantages

- The security of Solitaire lies in the security of the key
- Methods of increasing security of the key:
  a. Never using the same key to encrypt two different messages. This makes the entire system insecure.
  b. The safest way to perform the encryption/decryption process is in your head—using physical cards can release vulnerabilities (ex: if you're decrypting a top-secret message using cards and the police suddenly barge in, they can deduce the deck ordering)
  c. If you must use paper, use paper that can easily be destroyed
     - Burning is the safest method of disposal. Cigarette papers burn the easiest and are therefore the safest choice

Sources

1. https://www.schneier.com/academic/solitaire/
2. https://en.wikipedia.org/wiki/Solitaire_(cipher)

Demonstration!

- Grace is the sender; Anna is the receiver
- The deck order has already been agreed upon
- Suit order: Spades (1-13), Hearts (14-26), Clubs (27-39), Diamonds (40-52), Jokers (53-54)
- Grace would like to send the message ‘NMAP’