

Solitaire

Linguistics 484

Solitaire

- A practical and secure approximation to a one time pad.
- A stream cipher using a quasi-random key stream.

Encode

- Take message, break into 5s as usual
 - THEOH IOSTA TEUNIVERSITYXXX
- Convert to numbers
 - 20-8-5-15-8 9-15-19-20-1
20-5-21-14-9 22-5-18-19-9
20-25-24-24-24
- Generate key stream (random)

Encode

- 20-8-5-15-8 9-15-19-20-1
20-5-21-14-9 22-5-18-19-9
20-25-24-24-24
- 26-13-11-19-4 ...
- Add modulo 26: 20-21-16-8-12

Decipher

- Exactly the same, except subtract key stream modulo 26 rather than add

Make the key stream

- All the action is in the key generator
 - which uses a pack of 54 cards
 - and a counterpart pack in exactly same order.

Card values

- Spades = 1-13
- Hearts = 14-26
- Joker A = 27 (monochrome)
- Joker B = 28 (coloured)
- Diamonds = 29-41
- Clubs = 42-54

Solitaire

- Find the A Joker, move it below the next card in the deck (with wraparound to top if it was the last in the deck)
- Find the B joker, move it down two cards (with wraparound as before)

Solitaire

- Do a triple cut
- That is, split the deck in 3, with the jokers as the boundaries of the middle bit
- Swap the top part and the bottom part

Count cut

- Look at the bottom card, make it into a number between 1 and 53 (spades 1-13, hearts 14-26, diamonds 27-39, clubs 40-52, either joker 53)
- Count that many cards off the top of the pack, keeping them in order. Call that A
- Take all the rest of the pack except the last card and call it B. Put B on top of A and A onto the last card

Output value

- Look at the top card. Convert it to a value 1-53 as we just did. Count down and note the first card after the ones we counted.
- If its a joker, it doesn't count, don't write anything
- Convert to a number 1-26 (1-13 Spades or Hearts, 14-26 Diamonds or Clubs)

Details

- So long as you agree on something, details of how you convert cards to numbers could be varied. Provided the two packs move in the same way, the code will work.