GRETA Card Cipher

by Karl Zander

Abstract: GRETA is an easy to use card cipher modeled after the operation of rotor machines of old. It's purpose is provide a system secure against cipher text only attacks and some known plaintext attacks and is easy enough for anyone to use and remember.

GRETA:

GRETA or Gated Rotor Encryption Table Algorithm is an easy to use card cipher. The cipher is easy enough for the average person to use and resembles a card game. It does generate a pseudo-random sequence although it is not designed to be entirely secure although it's operation. GRETA S (Secure) should be used if secure transmission is desired.

A brief description of the card cipher:

GRETA is a linear 2 rotor ciphering machine that is easily emulated with ordinary playing cards. It is composed of a cipher rotor or deck and a stepping rotor or deck. The cipher rotor provides the encipherment of plaintext and decipherment of ciphertext by acting as a standard S-Box lookup table. Operation is usually carried out with cards facing up. The discard of the first card to the rear or the deck is the stepping operation.

The GRETA state is 52 letters (the cards in the 2 decks).

Specification:

1 x Standard 52 card deck (26 cards used for the cipher rotor and 26 cards used for the index stepping rotor)

Key is the arrangement of the cards in two decks of 26. The order of cards may be completely random but suite or color do not matter, all that matters is that each deck separately represents the values {0-25}. A typical card cipher numbers cards by ascending values and one could use the following value for cards.

AS 2S 3S 4S 5S 6S 7S 8S 9S 10S JS QS KS AH 2H 3H 4H 5H 6H 7H 8H 9H 10H JH QH KH

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

AC 2C 3C 4C 5C 6C 7C 8C 9S 10C JC QC KC AD 2D 3D 4D 5D 6D 7D 8D 9D 10D JD QD KD

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Cipher Rotor Card Values – {0-25} {A-Z}

Index Stepping Card Values – {0-25} {A-Z}

Encryption Usage:

- Arrange the cards in the order of the key (cipher deck on top, stepping deck on bottom)
- Step the cipher deck by the first stepping card value
- Substitute the first letter using the cipher deck
  Example - (if the plaintext is A (value is 0) take the value of the first card)
  Example – (if the plaintext is G (value is 6) take the value of the seventh card)

- Remove one card from the stepping deck to the rear

- Repeat above steps until the message is encrypted

Decryption Usage:

- Arrange the cards in the order of the key (cipher deck on top, stepping deck on bottom)
- Step the cipher deck by the first stepping card value
- Step the step
- Substitute the first letter using the cipher deck
  Example - (if the plaintext is A (value is 0) find the card valued as zero (the “A” card) and take the value of its position in the deck (“A” card in position 10 is the letter “K”)
  Example – (if the plaintext is G (value is 6) take the value of the seven card (the “H” card) and take the value of its position in the deck (“G” card in position 23 is “X”)

- Repeat above steps until the message is decrypted

Glossary:

Stepping – Removing a card from front of the deck and placing it in the rear

Schroeder