GRETA Card Cipher

by Karl Zander

Abstract: GRETA S is a card cipher modeled after the operation of rotor machines of old. It's purpose is provide secure communications in the field.

GRETA:

GRETA or Gated Rotor Encryption Table Algorithm (Secure/Ultra) is a card cipher that is designed to be relatively secure with a strength of approximately 172 bits or (52!). The design is most similar to the US Military SIGABA system and also inspired by the Dragon eStream cipher.

A brief description of the card cipher:

GRETA S is a 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 cipher text 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 S state is 54 letters (the cards in the 2 decks plus Gate letters G and Q). Gates G and Q are both set to A (zero) at the beginning of operation and in the first round become the first two letters in either decks. The act of substituting G and Q through the cipher and stepping rotors gives irregularity to the stepping and provides pseudo-random output. The round counter provides uniform stability and allows GRETA to be used for extremely long streams of data. Without the round counter GRETA is still a pseudo-random function.

The GRETA S non-linear operation is the Gate permutation and the round stepping, the linear operation.

The only weakness I can find in GRETA is that the key should be pseudo-randomly or randomly generated. GRETA is not a pseudo-random function when the cipher deck is neutral {0-25} or near neutral. The number of insecure keys is 26.

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}

Two Gate Letters (G, Q) {both initialized to zero}

Round Counter Mod 26 (for every letter that is enciphered, it is considered a round. They are numbered {0-25} and repeat every 26 letters)

Encryption Usage:

- Arrange the cards in the order of the key (cipher deck on top, stepping deck on bottom)
- Substitute Gate G using the cipher rotor (find the position of G in the cipher deck and take the value of that card) – this step is the same as the encryption lookup
- Substitute Gate Q using the stepping rotor (find the position of Q in the stepping deck and take the value of that card) – this step is the same as the encryption lookup
- Step the stepping rotor by G cards (remove G cards from the front of the stepping deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- Step the cipher rotor by Q cards (remove Q cards from the front of the cipher deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- Step the cipher rotor by the round counter value and increment the counter
- 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)

- 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)
- Substitute Gate G using the cipher rotor (find the position of G in the cipher deck and take the value of that card) – this step is the same as the encryption lookup
- Substitute Gate Q using the stepping rotor (find the position of Q in the stepping deck and take the value of that card) – this step is the same as the encryption lookup
- Step the stepping rotor by G cards (remove G cards from the front of the stepping deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- Step the cipher rotor by Q cards (remove Q cards from the front of the cipher deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- Step the cipher rotor by the round counter value and increment the counter
- 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

Test Vector:

Cipher Deck: WQUKIBGTYJPOEAVRLXSFHCNZMD
Stepping Deck: HCNLFOIRWSYJEBTDKAMQVXZUGP

Plaintext: DONOTUSEPC

Ciphertext: PTYNTWYGEJ

Optional Key Scheduler:

Before the encryption or decryption an optional key scheduler may be applied. The advantage the key scheduler gives is it provides separation between the key stream and actual key and make it more difficult for the attacker to obtain the key under various attack scenarios.

- Remove the card in the position of the value of the key letter
- Step the stepping deck by the cipher key card
- Step the cipher deck by the stepping key card

Additionally, a nonce may be applied in the same manner as above with a minimum length of 26 (13 for each deck) and a maximum length of 52.

Ultra Mode:

Ultra mode is another mode of operation not requiring the round stepping, however, the round stepping can be used in addition to the below instructions.

Ultra Mode Encryption Usage:

- Arrange the cards in the order of the key (cipher deck on top, stepping deck on bottom)
- Substitute Gate G using the cipher rotor (find the position of G in the cipher deck and take the value of that card) – this step is the same as the encryption lookup
- Substitute Gate Q using the stepping rotor (find the position of Q in the stepping deck and take the value of that card) – this step is the same as the encryption lookup
- Remove the card in the Q position from the stepping rotor and place it in the rear
- Remove the card in the G position from the cipher rotor and place it in the rear
- Step the stepping rotor by G cards (remove G cards from the front of the stepping deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- Step the cipher rotor by Q cards (remove Q cards from the front of the cipher deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- 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)

- Repeat above steps until the message is encrypted

Ultra Mode Decryption Usage:

- Arrange the cards in the order of the key (cipher deck on top, stepping deck on bottom)
- Substitute Gate G using the cipher rotor (find the position of G in the cipher deck and take the value of that card) – this step is the same as the encryption lookup
- Substitute Gate Q using the stepping rotor (find the position of Q in the stepping deck and take the value of that card) – this step is the same as the encryption lookup
- Remove the card in the Q position from the stepping rotor and place it in the rear
- Remove the card in the G position from the cipher rotor and place it in the rear
- Step the stepping rotor by G cards (remove G cards from the front of the stepping deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- Step the cipher rotor by Q cards (remove Q cards from the front of the cipher deck and place them in the rear of the deck or if operating on a table, move them from left (front) to right (rear))
- 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

Ultra Test Vector:

Cipher Deck: WQUKIBGTYJPOEAVRLXSFHCNZMD
Stepping Deck: HCNLFOIRWSYJEBTDKAMQVXZUGP

Plaintext: DONOTUSEPC

Ciphertext: PXZXNMZAOA

Glossary:

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