G.R.E.T.A Card Cipher

(Gated Rotor Encryption Table Algorithm)

by Karl Zander

GRETA is a playing card cipher designed for use with ordinary playing cards. It's motions resemble a rotor machine. It was designed with maximum security in mind and it's output resembles an ideal cipher modulo 26. It's strength is nearly 26 factorial (26!) with a number of keys such as a neutral ordered deck being insecure.

Specification:

State = (52 cards (26 card substitution rotor + 26 card control rotor) + 2 variables (G/Q))

The state of the GRETA cipher consists of 54 numbers; 2 that are substituted before each letter is enciphered and 52 cards between the 26 substitution rotor and 26 stepping or control rotor cards. The two 26 card decks should be separated by color (red/black) for ease of use.

Operational setup:

Start by creating a lookup dictionary that converts a card into it's assigned number. Such a lookup dictionary should look like this:

AC 2C 3C 4C 5C 6C 7C 8C 9C 10C JC QC KC AS 2S 3S 4S 5S 6S 7S 8S 9S 10S JS QS KS
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
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

AH 2H 3H 4H 5H 6H 7H 8H 9H 10H JH QH KH 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

Derive a secret key consisting of the deck split in half by color; one half for the substitution rotor; the other half for the control or stepping rotor. Assign numbers to each half 0-25 and take note of this on a sheet of paper. When done, you should have two sets of 26 cards numbered 0-25. The wielder of the card cipher is encouraged to use a secure shuffling method for each such as splash and shake.

Example key:

3C 5S 3S JC AC 6C JS 7C 4S 10C 8C 8S 4C 9C 5C QS QC 10S 6S 2S 7S AS KS 9S 2C KC
2 17 15 10 0 5 23 6 16 9 7 20 3 8 4 24 11 22 18 14 19 13 25 21 1 12

4H AD 4D KD QD 9H 8D QH 3D AH 7D 7H 9D 6H 3H 8H 6D KH JH 5D 2H 5H 10H 10D JD 2D
3 13 16 25 24 8 20 11 15 0 19 6 21 5 2 7 18 12 10 17 1 4 9 22 23 14

Example message: HELLOMYNAMEISGRETA

Rotor Stepping:

Before any encryption of plain text is done, the rotors are stepped using the control variables G and Q. G permutes the control or stepping rotor and Q permutes the substitution rotor. Each variable is assigned the card value in the zero index position and is stepped by each value. Stepping consists of four actions:

- Remove the Q card and place in the back of the substitution deck
- Remove the G card and place in the back of the control deck
- Remove a card from the front and placing it in the back of the deck X number of times where X is the value of G for the substitution deck.
- Remove a card from the front and placing it in the back of the deck X number of times where X is the value of Q for control deck.

In the case of our example, G = 3 and Q = 2; the values of the first two decks. Stepping the substitution rotor forward by G (2) yields the following deck order:

JC AC 6C JS 7C 4S 10C 8C 8S 4C 9C 5C QS QC 10S 6S 2S 7S AS KS 9S 2C KC 3C 5S 3S
10 0 5 23 6 16 9 7 20 3 8 4 24 11 22 18 14 19 13 25 21 1 12 2 17 15

Stepping the control or stepping rotor by Q (3) yields the following deck order:

4D KD QD 9H 8D QH 3D AH 7D 7H 9D 6H 3H 8H 6D KH JH 5D 2H 5H 10H 10D JD 2D 4H AD
16 25 24 8 20 11 15 0 19 6 21 5 2 7 18 12 10 17 1 4 9 22 23 14 3 13

Encryption:

Encryption of the first letter begins by looking up “H” in the black substitution deck. In our example, “H” is enciphered to “U” or the card in the 20 position or 8S.

Decryption:

In order to decrypt a letter, the card index value is looked up in the black substitution deck and it’s index number is used as the plain text value. In our example “U” is also substituted for “H” being at the 7 index space or 8C.

Test Vector:

Substitution Deck:

JC AC 6C JS 7C 4S 10C 8C 8S 4C 9C 5C QS QC 10S 6S 2S 7S AS KS 9S 2C KC 3C 5S 3S
10 0 5 23 6 16 9 7 20 3 8 4 24 11 22 18 14 19 13 25 21 1 12 2 17 15

Control Deck:

4D KD QD 9H 8D QH 3D AH 7D 7H 9D 6H 3H 8H 6D KH JH 5D 2H 5H 10H 10D JD 2D 4H AD
16 25 24 8 20 11 15 0 19 6 21 5 2 7 18 12 10 17 1 4 9 22 23 14 3 13

Example message: HELLOMYNAMEISGRETA
Example cipher text: UKHONDDONHCMSYEDQO