MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Enigma Combinatorics

Author: Bernhard Esslinger

November 2010

Enigma

The Enigma is an electro-mechanical rotor machine used for encryption and decryption. Several different Enigma models were produced. One of the most commonly discussed Enigma machines is the ENIGMA-1, which was used during the Second World War by the German army.

One main part of the Enigma is changeable rotors. For the ENIGMA-1 there are two kinds of rotors. First, the normal, rotating rotors (I to V), where you choose three out of five different rotors and their position in the Enigma slots. Second, two reflectors (B and C) from which you choose one.

Enigma

Any rotating rotor has one input and one output for each of the 26 capital letters in the alphabet.
One rotating rotor is performing a simple substitution. When chaining the three rotors, every character is substituted once by each of the three rotors before reaching the reflector. The reflector gets the output from the third rotor as input and outputs another value as input for the third rotor. This means that the signal is passing through the three rotors two times.
Since the reflector does not allow a mapping of a character to itself and since the result of the three normal rotors is a bijective mapping, it is not possible that an input is mapped to itself.

Enigma

After the encryption of one character, the rotor on the right position, the fast rotor, rotates once.
If the fast rotor reaches a specific position, which can be adjusted with the help of a ring, the middle rotor rotates once, too.
Reaching a specific position with the middle rotor, the left, slow rotor rotates once.
These rotations are done to perform a polyalphabetic substitution.
Additionally, it is possible to place cables into a plugboard to perform a character permutation of the input character before processed by the rotors.

Challenge

The key space is calculated using four factors: First, the election of the three rotors and their arrangement in the Enigma slots. Second, the position of the rings. Third, the start position of the rotors used. Fourth, the number of cables used for character permutation.

The solution of this challenge is the sequence of the results (numbers) of the following eight questions, padded without a delimiter:

Challenge

1. How many possible ways are there of positioning three rotors in three slots of the ENIGMA-1?
2. How many possible ways are there of positioning five rotors in three slots of the ENIGMA-1?
3. How many total possible ways are there of choosing the rotors (including the reflecting rotors) in the ENIGMA-1?
4. How many possible start positions exist for the chosen reflector?
5. Once you have chosen the start position for two of the three normal rotors, how many possibilities are there for the start position of the third rotor?

Challenge

6. How many possibilities are there to place two cables for character permutation in the plugboard?
7. Consider, your Enigma machine has four normal rotor slots and you already chose the order. How many possibilities are there to choose the start position without considering the ring settings?
8. The length of your message is 350 characters. How often can the slow rotor rotate at most?