Distributed brute-force deciphering system

Task description

Vladimir Petkov

Zdravko Donev

Alexander Kanchev

Our team is going to implement a distributed brute-force deciphering system. It will decipher a ciphered text with Vigenere cipher.

We will implement the task with the following steps:

1. Input enciphered text.
2. Trying to guess the key length.
3. For each guess of the key length, generate all possible keys of that length.
4. Decipher text.
5. Check the percentage of real English words contained in the text. If the percentage is high enough, we will mark it as possible answer.

Steps 4 and 5 will be distributed among several threads or processes.

1. Modules
   1.1. UI - There will be a user interface that will control the application. Part of it functionalities will be to accept an enciphered text using the Vigenere cipher, show the possible deciphered text, run more workers.
   1.2. Cipher key length predictor - After the text is received the program will try to predict the length of the key using overlapping and frequency analysis.
   1.3. Cipher key generator – After the possible cipher key lengths are found this module will generate all possible cipher key with this length. Then they will be uploaded into the database.
   1.4. Database – The database will be used for storing the state of the system - enciphered text, generated keys, processed keys and deciphered texts.
   1.5. Decipher – This module is responsible to decipher a given text enciphered with Vigener.
   1.6. Evaluator – This module is responsible to evaluate the likelihood of the deciphered text being the originally send text. It will be done by dictionary analysis. for example over 50% of the deciphered words are indeed English words then this will be considered as the original text.