Multi-threaded Blowfish encryption/decryption algorithm

Summer Session 2014
(only valid for exams till September 2014)

Project Description

In this project, you have to implement a multi-threaded implementation of the Blowfish encryption/ decryption algorithm.

Blowfish is a block cypher, i.e. Blowfish has a 64-bit block size[1] and a variable key length from 32 bits up to 448 bits. The detailed description of the Blowfish algorithm has to be retrieved from the web (start from wikipedia).

Your goal is to design a multi-threaded version of Blowfish able to assign the encryption/decryption to a separate thread (the number of threads and the way they handle with data is up to your algorithm engineering design).

The program, at the end of the encryption/decryption task, has:

1. To save the result in a separate file (the file name is provided by the user)

2. To print the total encryption/decryption time and the average encryption/decryption time of each thread (with ms precision).

Rules:

1. Write the program in C.
2. You can work in groups of **at most two**.
3. Download the input files from Poltio Didattica website (see project_1_input_files.zip).
4. Submit your program using the Polito Didattica website along with the output for each input file.
5. Run tests to make sure the program is fully functional.
6. **Write a well-organized report**, which will include:

[1] Fixed-size data type can be found in stdint.h C library.

a. A detailed but clear description of the algorithm and data structures you used in your implementation.
b. Graphs showing the algorithm performances with different number of threads and text size

7. **Grading**:
    a. Encryption only: **max 23 points**
    b. Encryption and decryption: **max 28 points**.
    c. Encryption, decryption, and performance engineering: **max 33 points**.