Thuật toán

Yêu cầu 1: Thuật toán băm khóa là thuật toán SHA256, cho kết quả là chuỗi khóa có độ dài 128 bit.[1]

Yêu cầu 2: Thuật toán có thể mã hóa nhanh

Yêu cầu 3:

Thuật toán mã hóa bằng phương pháp mã hóa khối CBC, với mỗi khối là 1 ký tự.[2]

Mã hóa:

Text

Description automatically generated with medium confidence

Giải mã:

Text

Description automatically generated

Với EK(P) = p + k, 0 <= i <= len(p)

Dữ liệu trước khi được mã hóa: <thời gian mã hóa>.<dữ liệu mã>

Kết quả:

Sau khi mã hóa sẽ cho ra định dạng

<dòng đầu tiên là khóa sha2>

<dữ liệu mã>

Reference:

1. Copyright (C) 2005, 2007 Olivier Gay [olivier.gay@a3.epfl.ch](mailto:olivier.gay@a3.epfl.ch). Retrieved from: <http://www.zedwood.com/article/cpp-sha256-function>

2. Retrieved from: <https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_block_chaining_(CBC)>