SAP Exam – July 2022

You have received a challenge to respond to a simple question. There are 1000 files in the given archive, each having a mathematical expression that will give you a key. You need to determine which question is yours based on the next clues

- **The first text line from the** file associated to you has a HashMac value equal to the one given int the **Clues.pdf** file (check the table for your name)
- The HMAC has been generated using SHA 2 algorithm
- The secret key is “ismsecret” (without the quotes)

1. Write a Java program that will print at the console the file name that corresponds to the previous clues. (**7.5 pts**)
2. Once you find your Message file use it to solve the mathematical puzzle. Compute the MD5 hash of the math operation and print it on the screen. You can define the operation result in your code as a variable (**5 pts**)
3. Once you found your Message file use it to decrypt the associated *Question.enc* file (**7.5 pts**)
   - The associated *Question.enc* file (has the same number as your Message file is encrypted with AES in Counter mode
   - The IV used is known and has the value 0011 0011 in binary
   - The key to decrypt the file is the MD5 hash binary value of the previous computed value (the addition sum)
4. Generate a text file with your answer to the secret question. Encrypt the response with AES in ECB mode. Name this file ***response.enc***. Use the same key as earlier (**5 pts**)

Upload

- The .java file with your solution
- The **response.enc** file

All solutions will be cross-checked with MOSS. Solutions similar more than 30% will be canceled.