ISM 2020- Challenge 2

You hacked the ACME Inc file system and you got the files storing the binary keys for their users (User1.key, User2.key, …..)

You have their personnel list and you know the SHA2 value as Base64 associated with the key file of each user. Check *Accounts.txt* file.

Assuming that you search for your name, try to figure it out what is your associated file. Once you find it, use it to extract the AES 128 bit key from it and decrypt the associated encrypted file (the one with the *.secret* extension). You know that the files where encrypted in CBC mode, with AES and the IV is known (each byte in it has the 1st bit from right to left equal to 1 and all the rest are 0)

Once you decrypt the file upload the secret from it as string. The plaintext file should contain your name in it also.