CS 6348 Spring 2023: HW 3

Due Date April 22th, midnight.

No late submissions are accepted. Please submit your work to elearning. Please make sure that you have your name on the submission (i.e., inside the pdf file).

Please start as soon as possible. Good Luck.

1. (40 pts) Write a program P such that $P(M, k)$ takes two input where M could be an arbitrary string and k is an integer. The program would **randomly generate nonce values** n_i (64 bit) until the hash (use SHA-256) of message and nonce (i.e., $H(M||n_i)$) have the first k **bits equal to zero** (in your implementation, just concatenate nonce to the end of the message without adding any special characters between the message and the nonce). Once such a nonce is found, P should output '$H(M||n_i)$, n_i, i' where $H(M||n_i)$ and n_i are in hexadecimal, i (number of tries) as integer and just one comma between them.

   - Run P with M ='I Love Data Security Class So Much. It is so great :)' and k={2,4,6,8}, for each k value, run the P 10 times and report the average number of tries and the standard deviation of the tries needed to find the required nonce.
   - Submit your source code, and information on how to compile/run your program. Please try to use java, python, or C/C++. If you want to use different programming language, please let the TA know.

2. (60 pts) Using any XACML implementation [1], please do a simple implementation of BLP mechanism in XACML. You can assume that you have only to access levels (high, low) and no category set, two operations (read, write). You will be given a set of access requests in a text file, each request is on a separate line, each field is comma separated, using the following format:

   Object Name, Object Access Level, Subject Name, Subject Access Level, Operation
   For example,

   File A, High, Murat, Low, Read

   File B, Low, Murat, Low, Read

   Based on the XACML policies you have written in the XACML implementation framework you have chosen, your program should output a text file with each request decision corresponding to the original request on separate lines. For the above example, your implementation should return:

   Deny

   Permit

[1] E.g., https://github.com/att/xacml-3.0/

. Please **submit your source code, and information on how to compile/run your program.** In addition, please submit **at most two page description on how you have implemented the BLP policy in the XACML framework you have chosen with some code snippets.**.