International Institute of Information Technology

Hyderabad

System and Network Security (CS5470)

Lab Assignment 3: *Formal Security Verification of Security Protocols*

Using the AVISPA backends

Hard Deadline: March 16, 2021 (23:59 P.M.)

Note:- *It is strongly recommended that no student is allowed to copy programs from others. Hence, if there is any duplicate in the assignment, simply both the parties will be given zero marks without any compromise. Rest of assignments will not be evaluated further and assignment marks will not be considered towards final grading in the course. No assignment will be taken after deadline. Please upload in the HLPSL code along with a README file in the course moodle portal through a ZIP file (**GroupNo-AnyOneRollNofromGroup.zip**).*

Implement the protocol using HLPSL language of AVISPA specifying clearly the basic roles for the parties involved in the network, and mandatory roles for session, goal and environment. Your code must be well-commented and easy-to understand. You must also specify the secrecy and authentication goals in the implementation. Simulate the protocol using the OFMC and CL-AtSe backends.

Group ID/Number	Assigned Paper ID
#i	Pi (paper_i.pdf)

Where "i" denoted the group id of a group i. For example, if the group id/number is 3 (i=3), then the paper id/number will be P3 (paper_3.pdf).

Question:

Group #i needs to implement the given assigned (described in the table) authentication/key agreement/access control protocol (paper) using AVISPA tools.

Remark

In HLPSL, bitwise XOR operation: A ⊕ B is represented as xor(A, B). For elliptic curve point (scalar) multiplication of the k.G = G + G + · · · + G(k times), you can define a hash function, say EccMul. Then, express it as EccMul(K, G). All other descriptions regarding HLPSL implementation (AVISPA installation) are available at http://www.avispa-project.org/.

Find the uploaded file (excel file) for paper details.

All the best!