Indian Institute of Technology Jodhpur

Computer Science and Engineering Department

Lab 7

CSL6010 - Cyber Security

Date: 30-03-2023 **Marks: 10**

Duration: 1.5 Hrs

Aim: Design a simple key exchange protocol with SPAN+AVISPA

Please refer the following link for download and install AVISPA SPAN tool, demo video and documentation: http://people.irisa.fr/Thomas.Genet/span/

Define Three agents: A, B, and a Trusted Third Party T

A and T share a symmetric key ANT

B and T share a symmetric key BAT

A wants to establish a symmetric session key AKB shared with B

Protocol development using SPAN+AVISPA

1 - Specifying protocol and properties

2 - Debugging specification using animation: Find the blocking transition, monitor the variables

3 - Attack discovery, strengthening the protocol

4 - Tuning and optimizing the protocol

You have to submit all code (in text) along with a detailed report including screenshots, observations, etc. on the tasks performed **in a single PDF file.**

Note: No other file format than PDF will be accepted for evaluation.