Cryptography and Network Security Lab-8

Let:

- M, M1, M2 be messages
- K be a key
- A and B are agents

We denote by:

- **$\{M\}_K$** The message M encrypted with the key K
- **A--->B: M** A sends the message M to B.
- **I(A)--->B: M** I impersonates A to send the message M to B
- **A--->I(B): M** The message M sent by A to B is intercepted by I

Asymmetric Encryption:

- The public key (K_A) is given all agents
- The private key (K_A^{-1}) is only by A
- Decrypt **($\{M\}_{KA}$, K_A^{-1}) = M**

1. **Protocol 0 (B-->A: B, s)**

   Here, B sends a secret message to A through the public communication channel. Specify the protocol 0 in HLPSL (High Level Protocol Specification Language) and Implement in AVISPA tool to check whether the protocol is safe or unsafe. If the protocol 0 is unsafe then generate Message Sequence Chart (MSC) and display the intruder and attack simulation using Security Protocol Animator (SPAN).

2. **Protocol 1 (B-->A: {B, s} K_A)**

   Here, B sends the encrypted secret message to A through the public communication channel. Implement the protocol using HLPSL and check for the secrecy property using AVISPA tool.

Resources:

- ✓ AVISPA+SPAN: http://people.irisa.fr/Thomas.Genet/span/
- ✓ Installation: https://www.youtube.com/watch?v=YvgHw5pr5bA&feature=youtu.be