# Cryptography and Network Security Lab-9

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

1. **Protocol 2 (B-->A: B, {S}_$Kb^{-1}$)**

   In this protocol scenario, B sends the encrypted message S to A via insecure communication channel. Specify the protocol 2 in HLPSL using AVISPA tool to check whether the protocol is safe or unsafe. If the protocol 2 is unsafe then generate Message Sequence Chart (MSC) and display the intruder and attack simulation using Security Protocol Animator (SPAN).

   Security goals to be achieved:

   - **Secrecy (Confidentiality)**
   - **Weak authentication**

2. **Protocol 3 (B-->A: {B, {S}_$Kb^{-1}$}_$K_A$)**

   In this scenario, B sends the enciphered message to A through the public communication channel. Implement the protocol in HLPSL using AVISPA and check whether the protocol is safe or unsafe. The security goals to be achieved:

   - **Confidentiality**
   - **Strong authentication**

   Further, use Security Protocol Animator (SPAN) to check the intruder knowledge and attack simulation.