# INTE2401/2402 Lab 9

Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This week’s lab concentrates on password-based authentication between two parties. We implement a **Java** program to perform the **reflection attack** against the mutual authentication with secret key.

AES encryption/decryption algorithm, crypto (pseudo) random generator, and crypto hash function will be used as building blocks. Some hints are provided below.

* Apache commons crypto lib provides an optimised AES, crypto random generator. Download at (<https://commons.apache.org/proper/commons-crypto/download_crypto.cgi>).
* **Example of AES encryption/decryption** can be found at (<https://commons.apache.org/proper/commons-crypto/xref-test/org/apache/commons/crypto/examples/CipherByteBufferExample.html>).

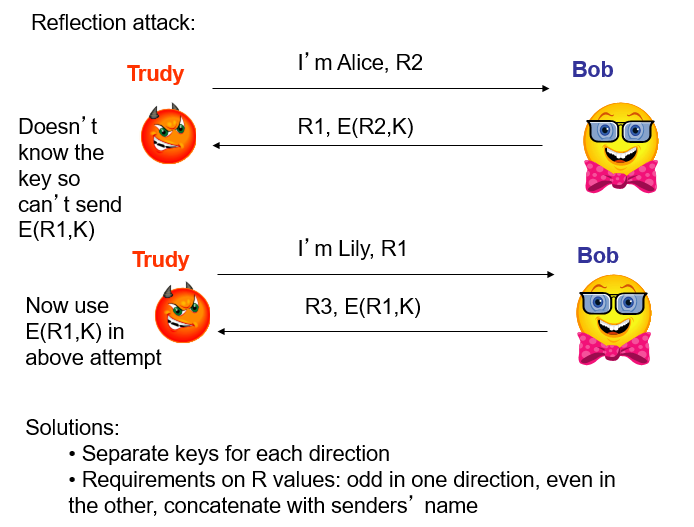


Figure 1. Reflection attack against mutual authentication

Figure 1 illustrates the reflection attack against mutual authentication protocol with secret key. The attacker Trudy initiates a connection to Bob, and Bob attempts to authenticate Trudy by sending him a challenge R1. After receiving R1, Trudy opens another connection to Bob, and sends R1 to Bob as its own. Bob responds to the challenge R1 with E(R1, K). Then Trudy sends that response back to Bob on the original connection. As a result, Trudy can impersonate a legitimate client and communicate with Bob.

Q. Implement a Java program of reflection attack against mutual authentication protocol. Output the intermediate results and shared secret between Alice and Bob. K=student no. repeats 4 times.

Sample:

