CISC 367 – Spring 2016

Homework Assignment – Man-in-the-Middle Attack on Authentication with Public Key Cryptography

---

1. The following figure depicts how **nonce** (R) and **public key cryptography** (public and private key pair) work together (termed protocol *ap5.0*) to solve the end-point authentication problem by replacing the symmetric sceret key used in protocol *ap4.0*.

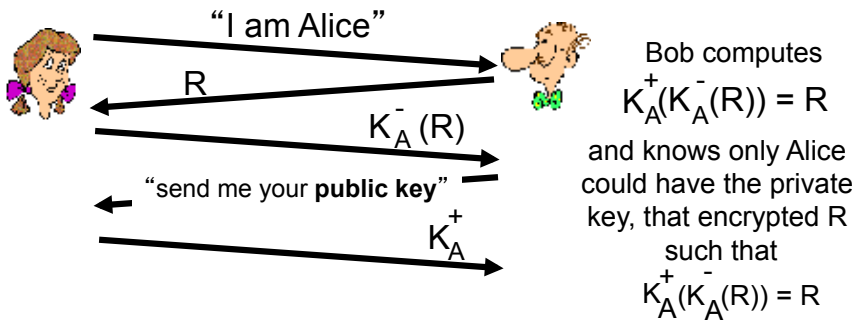

Figure 1: End-point authentication with nonce and public key cryptography

However, protocol *ap5.0* suffers from the *man-in-the-middle* attack, where Trudy can pose as Alice (to Bob) and as Bob (to Alice), *i.e.*, Trudy could intercept and insert new messages.

Diagram the operations of a man-in-the-middle attack launched by Trudy by using notations K_X^+ and K_X^- for public and private keys, respectively, for party X.