ATK4 - Computer- und Mediensicherheit
FHS Hagenberg
2. Übungsblatt für den 18. März 2003
(1 Seite)

Realisieren Sie den folgenden DH-Schlüsselaustausch. Alice und Bob vereinbaren (öffentlich) die Primzahl $p = 3571$ und die Primitivwurzel $g = 10$ modulo p.

(1) Alice wählt zufällig $a = 17$ und Bob wählt $b = 87$. Berechnen Sie, welche Zahlen die beiden einander schicken.
(2) Berechnen Sie den gemeinsamen Schlüssel, auf den die beiden sich so einigen.
(3) Zeigen Sie, wie Eve die beiden als "(wo)man in the middle" täuschen könnte. Berechnen Sie dazu alle Nachrichten, die Eve erzeugen und verschicken muss und die vereinbarten Schlüssel.
(4) Kann Eve durch eine "man in the middle"-Attacke die geheimen Zahlen a und b herausfinden?
(5) Realisieren Sie das MTI/A0-Protokoll für Alice und Bob, sodass Eve nicht mehr einfach ihre Attacke durchführen kann. Teile können Sie aus Beispiel 1 und 2 wiederverwenden. Berechnen Sie wieder alle versandten Nachrichten und den gemeinsamen Schlüssel.
(6) Berechnen Sie den diskreten Logarithmus von 1612993232 zur Basis 128958 in der Gruppe $(\mathbb{Z}_{8795098123}, +, -, [0])$.
(7) Lösen Sie Beispiel (7) vom 1. Übungsblatt.