HW 2 Answers – Question 1

CSCI-UA.0480-63

October 8, 2025

1. Public key crypto at toy security levels

(a) $p = 10007$, $g = 3$

1. Order of g mod p: 5003.
2. Shamir three-pass with $m = 1337$, $a = 2461$, $b = 4319$:
   - $a^{-1} \bmod (p-1) = 7103$, $b^{-1} \bmod (p-1) = 5259$.
   - Transmissions: $x_1 = m^a \bmod p = 792$, $x_2 = x_1^b \bmod p = 1441$, $x_3 = x_2^{a^{-1}} \bmod p = 5629$ (Bob recovers m by raising to b^{-1}).
3. Diffie–Hellman with $a = 2461$, $b = 4319$:
   - $A = g^a \bmod p = 5974$, $B = g^b \bmod p = 7413$, shared secret $s = B^a \bmod p = A^b \bmod p = 6122$.

(b) RSA with $p = 383$, $q = 401$

1. $\varphi(N) = (p-1)(q-1) = 152800$.
2. With $e = 11$, the private exponent $d \equiv e^{-1} \bmod \varphi(N) = 13891$.
3. Encrypting 1337: $c = m^e \bmod N = 113846$.
4. Signing 1337: $\sigma = m^d \bmod N = 101732$.