0688447: Computer Networks and Security, Summer 2017
Solution to Assignment 4

Problem 1 in Assignment 4:

(a).
phi(17x19) = 16x18 = 288;
from 11d = 1 mod 288, we solve d = 131;

(b).
- Bob computes h(101) = 3;
- Bob computes y = 3^131 mod 323 = 129;
- Bob put (m, y) = (101, 129) at a public domain;

(c).
- Alice obtains (m, y) = (101, 129) from the public domain;
- Alice computes h(m) = 3;
- Alice computes h'(m) = y^e mod n = 129^11 mod 323 = 3;
- Alice compare h'(m) to h(m): Since they both equal to 3, Alice accepts the signature.

Problem 2 in Assignment 4:

(a). Alice performs:
- compute 2^11 mod 133 = 53; and send it to Bob

(b). Bob performs:
- Bob received 53 and computes 53^59 mod 133 = 2, which is the shared key with Alice.

Note that 133 = 7 x 19 and phi(133) = 6 x 18 = 108.
From 11d = 1 mod 108, it follows d = 59.

Problem 3 in Assignment 4:

- Alice chooses a = 7 and computes 2^7 mod 19 = 14;
- Alice sends 14 to Bob;
- Alice receives 16 from Bob;
- Alice computes 16^7 mod 19 = 17. So their shared key is 17.

- Bob chooses b = 4 and computes 2^4 mod 19 = 16;

- Bob sends 16 to Alice;
- Bob receives 14 from Alice;
- Bob computes 14^4 mod 19 = 17. So 17 is their shared key.

Problem 4 in Assignment 4:

- Alice chooses a = 5 and computes x^5 mod f(x) = x^2 + 1;
- Alice sends x^2 + 1 to Bob;
- Alice receives x^4 + x^2 from Bob;
- Alice computes (x^4 + x^2)^5 mod f(x) = x^4.
  So their shared key is x^4.

- Bob chooses b = 7 and computes x^7 mod f(x) = x^4 + x^2;
- Bob sends x^4 + x^2 to Alice;
- Bob receives x^2 + 1 from Alice;
- Bob computes (x^2 + 1^7 mod f(x) = x^4.
  So x^4 is their shared key.