CRYPTOGRAPHY MISSION 10

Deadline: Thursday, 16 November 2017 at 10:50am
This mission covers Sections 9.1, 9.2

1. Graded Problems

1. (Final Project) Provide a list of legitimate references/sources for your project that you have considered (at least 3). They might not be included in your final project, but you should be doing thorough background research.

2. (RSA Signature) Alice has a public key $(e_A, n) = (5, 119)$.
   a. Bob's message is $m = 22$. Eve (the mail carrier) gives Bob a signed version of the message in which Alice's signature is $y = 71$. Is the signature valid? Explain.

   b. Bob finds a second letter on his desk that is signed "Alice" with $(m, y) = (17, 67)$. Is this letter actually from Alice? Explain.

3. (Modified from T&W 9.6 # 4) There are many variations to the ElGamal digital signature scheme that can be obtained by altering the signing equation $s \equiv k^{-1}(m - ar) \bmod (p-1)$. Here are some variations.
   a. Consider the signing equation $s \equiv a^{-1}(m - kr) \bmod (p-1)$. Show that the verification $\alpha^m \equiv (\alpha^a)^s r^r \bmod p$ is a valid verification procedure.

   b. Consider the signing equation $s \equiv am + kr \bmod (p-1)$. Show that the verification $\alpha^s \equiv (\alpha^a)^m r^r \bmod p$ is a valid verification procedure.

   c. Create an example (possibly using CoCalc) with $m = 10$ and the prime $p = 11$. Be sure to show the setup stage, the signing stage, and the verification process. Email any code to Dr. Ho.

4. (Honors - Modified from T& W # 8) Consider the following variation of the ElGamal signature scheme. Alice chooses a prime p and a primitive root α. She also chooses a function $f(x)$ that, given an integer x with $0 \leq x < p$, returns an integer $f(x)$ with $0 \leq f(x) < p-1$. For example, $f(x) = x^7 - 3x + 2 \bmod (p-1)$. She chooses a secret integer a and computes $\beta \equiv \alpha^a \bmod p$. The numbers p, α, β and $f(x)$ are made public.
   - Signing m:
     1. Alice chooses a random integer k with $\gcd(k, p-1) = 1$.
     2. She computes $r \equiv \alpha^k \bmod p$.
     3. She computes $s \equiv k^{-1}(m - f(r)a) \bmod (p-1)$. The signed message is (m, r, s).
   - Verifying:
     1. Bob computes $v_1 \equiv \beta^{f(r)} r^s \bmod p$.
     2. He also computes $v_2 \equiv \alpha^m \bmod p$.
     3. If $v_1 \equiv v_2 \bmod p$, then the signature is valid.

   Show that if all the procedures are followed correctly, then the verification equation is true (Hint: Start by solving $s \equiv k^{-1}(m - f(r)a) \bmod (p-1)$ for $f(r)$. Then, plug this into v_1 and use definitions until you get v_2.)

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 9.6 # 1, 2, 5, 6
- Section 9.7 # 1