C&O 487/CM 432: Assignment #4

Due date: April 3 (Friday) or April 7 (Tuesday)

1. **RSA signatures** (10 marks)
   Consider the variant of the basic RSA signature scheme in which no hash function is used. That is, to sign a message m, where $0 \le m \le n-1$, Alice computes $s = m^d \bmod n$ and sends (m, s) to Bob. (Here, (n, e) is Alice's RSA public key, and d is Alice's RSA private key.) To verify, Bob computes $m' = s^e \bmod n$ and checks that $m' = m$.

   (a) Show that this signature scheme is existentially forgeable under a key-only attack.

   (b) Show that this signature scheme can be totally broken under a chosen-message attack.

2. **Chinese Remainder Theorem** (5 marks)
   Let m and n be two positive integers satisfying $\gcd(m, n) = 1$, and let a and b be two integers. Recall (from Math 135) that the Chinese Remainder Theorem states that the pair of congruences

   $$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

   has a unique solution $x \in [0, mn-1]$. The following is an efficient algorithm for finding x.

   i) Using the extended Euclidean algorithm, find integers s, t such that $sm + tn = 1$. (Note that such integers exist because $\gcd(m, n) = 1$.)

   ii) Compute $x = (atn + bsm) \bmod (mn)$.

   iii) Return(x).

   Prove that the output of the algorithm is correct.

3. **Error attack on the RSA signature scheme** (15 marks)
   Suppose that a smart card is using the Chinese Remainder Theorem for RSA signature generation. That is, if (n, e) is the RSA public key and d is the corresponding private key, then signing a message M is performed as follows:

   i) Compute $m = H(M)$.

   ii) Compute $s_p = m^{d_p} \bmod p$ and $s_q = m^{d_q} \bmod q$, where $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$.

   iii) Find s, $0 \le s \le n-1$, such that

   $$\begin{cases} s \equiv s_p \pmod{p} \\ s \equiv s_q \pmod{q}. \end{cases}$$

   (a) Prove that s is the correct signature of M (that is, prove that $s = H(M)^d \bmod n$).

   (b) Explain why it might be advantageous to compute s using the procedure described above instead of computing $s = m^d \bmod n$ directly using the repeated square-and-multiply algorithm.

   (c) Suppose now that an adversary can somehow induce the smart card to compute s_p incorrectly (and s_q correctly) while signing a message. Let s' be an resulting (incorrect) signature on M. Suppose that the adversary has access to the public key (n, e) and also the signed message (M, s'). Show how the adversary can efficiently factor n.

   (d) Suggest a (realistic and practical) method for preventing this attack.

4. **Discrete logarithms** (10 marks)
$g = 256$ is an element of order 71 in $\mathbb{Z}_{569}^*$. Use the baby-step giant-step algorithm to find $\log_g 327$. (Show the main steps of the algorithm.)

5. **Poor random number generator in DSA** (10 marks)
We recall the DSA signature scheme. The system parameters consist of a 1024-bit prime p, a 160-bit prime divisor q of $p-1$, and an element $g \in \mathbb{Z}_p^*$ of order q. Suppose further that $q \equiv 3 \pmod 4$. Alice's private key is $a \in_R [0, q-1]$, while her public key is $h = g^a \bmod p$. To sign a message $M \in \{0,1\}^*$, Alice does the following:

   (i) Select $k \in_R [1, q-1]$.
   (ii) Compute $m = \text{SHA-1}(M)$.
   (iii) Compute $r = (g^k \bmod p) \bmod q$, and check that $r \neq 0$.
   (iv) Compute $s = k^{-1}\{m + ar\} \bmod q$, and check that $s \neq 0$.
   (v) Alice's signature on M is (r, s).

   To verify A's signature (r, s) on M, Bob does the following:

   (i) Obtain an authentic copy of Alice's public key h.
   (ii) Compute $m = \text{SHA-1}(M)$.
   (iii) Check that $1 \leq r, s \leq q-1$.
   (iv) Compute $u_1 = ms^{-1} \bmod q$ and $u_2 = rs^{-1} \bmod q$.
   (v) Accept iff $r = (g^{u_1} h^{u_2} \bmod p) \bmod q$.

   Suppose now that in order to avoid having to generate random per-message secrets k for each message, Alice chooses an initial random value $k_0 \in_R [1, q-1]$, and then signs the ith message using the per-message secret $k_i = k_0^i \bmod q$ for all $i \geq 1$. Suppose that Bob observes three *consecutively* signed messages, say $(M, \text{sig}(M))$, $(M', \text{sig}(M'))$, and $(M'', \text{sig}(M''))$. Describe how Bob can, with very high probability, efficiently compute Alice's private key a given this information.

6. **Elliptic curve computations** (10 marks)
Consider the elliptic curve $E : y^2 = x^3 + 2x + 5$ defined over $\mathbb{Z}_{11}$.

   (a) Find $E(\mathbb{Z}_{11})$, the set of $\mathbb{Z}_{11}$-rational points on E.
   (b) What is $\#E(\mathbb{Z}_{11})$?
   (c) Let $P = (0, 7)$, $Q = (3, 4)$, $R = (3, 7)$, $S = (4, 0) \in E(\mathbb{Z}_{11})$. Compute the following points:
   (i) $P + Q$. (ii) $Q + R$. (iii) $2R$. (iv) $2S$.

Please note that assignments are not weighted equally. The total marks received on assignments will be added together at the end of the course.

You are welcome to collaborate on assignments with your colleagues. However, solutions must be written up by yourself. If you do collaborate, please acknowledge your collaborators in the write-up for each problem. If you obtain a solution with help from a book, paper, wikipedia, a web site, solutions from previous offerings of the course, *or any other source*, please acknowledge your source. You are not allowed to solicit help from online bulletin boards, chat groups, or newsgroups.

The assignment is due at the *beginning* of class on April 3. *You may also submit the assignment in my office (MC 5037) anytime before 4pm on April 7 (Tuesday).*
