MAD 6478 Assignment 2 (Due **Apr 19, 5pm**)

(1) (6 marks) (Shamir) Let $N = pq$ where $q \approx 2^{4960}$ and $p \approx 2^{512}$.
- Give a crude estimate of the bit-security for such RSA modulus using the asymptotic complexity of ECM and NFS. Hypothetically if one founds an ECM-like factoring method that runs in time $\mathrm{L}_p(1/4, 1)$. How do we set the p and q to achieve a security level of more than 2^{128}.
- Suppose a RSA scheme uses CRT for decryption: given ciphertext c, one decrypts m with,
$$m_1 \equiv c^{d_1} \pmod{p}$$
$$m_2 \equiv c^{d_2} \pmod{q}$$
where $d_1 \equiv d \pmod{p-1}$ and $d_2 \equiv d \pmod{q-1}$ for the secret key d. It is observed that if the message $0 \leq m < p$, there is no need to compute m_2 since $m = m_1$. Hence this scheme just computes $m_1 \equiv c^{d_1} \pmod{p}$ and return m_1 for the decryption. Show that this scheme is not secure under a chosen-ciphertext attack.

(2) (7 marks) (Floyd, Brent) Given a fixed integer N. Suppose that we are generating a sequence of integers $\{x_0, x_1, x_2, \cdots\}$ in the range $0 \leq x_0 < N$ in the following way: let $f(x)$ be any function such that $0 \leq x < N$ implies $0 \leq f(x) < N$. The sequence is then generated by the iteration $x_{i+1} = f(x_i)$ with some random x_0 such that $0 \leq x_0 < N$.

Note the sequence is ultimately periodic and there exist numbers λ and μ such that $x_0, x_1, \cdots, x_{\mu+\lambda-1}$ are distinct, but $x_{n+\lambda} = x_n$ for $n \geq \mu$.
- Show that there exists some $n > 0$ such that $x_n = x_{2n}$, and the smallest such value of n lies in the range $\mu \leq n \leq \mu + \lambda$. Find a formula that express the smallest such n in terms of μ and λ. In particular, if $\mu \leq \lambda$, what is the smallest such value of n? If $\mu > \lambda$, what is the smallest such value of n?
- Let $l(n)$ be the greatest power of 2 that is less than or equal to n. For instance, $l(15) = 8$ and $l(l(n)) = l(n)$. Show that there exists an $n > 0$ such that $x_n = x_{l(n)-1}$. Find a formula that express the least such n in terms of μ and λ.

(3) (7 marks) Given DLP $5^x \equiv 15657 \pmod{16103}$. Note that $16102 = 2 \cdot 83 \cdot 97$. Use the Pohlig-Hellman method to find x, e.g. find $x \pmod 2$, $x \pmod{83}$ and $x \pmod{97}$ respectively and then use CRT.
- Use the baby-step giant-step method to find $x \pmod{83}$. Hint: using a table of 10 elements. Please document the table elements and collision.
- Use the Pollard's two-kangaroo method to find $x \pmod{97}$. A way to define the iterating function is to use a tame sequence $x_{i+1} = x_i \cdot g^{h(x_i)}$ where $x_0 = g^b$ for $b = 96$ and define $h(x_i) = 4^{x_i \pmod 4}$. Note the wild kangaroo walks on $y_{i+1} = y_i \cdot g^{h(y_i)}$ with an appropriate y_0. Please document the footprints of the kangaroos; show where the trap is and the collision. You may need to iterate the functions for about $\sqrt{97} \approx 10$ times.
- Finally, compute x using CRT.

You will need to use a computer algebra system (that can do modular exponentiation) for this question.