CS 758

Assignment 1

due by Noon on Monday, September 30, 2013

General Instructions

- Assignments must be handed in by the designated time. I prefer an electronic copy (.pdf file) submitted by email, but I will also accept a hard copy that is dropped off in class or at my office. Due to the large number of students in the class, no extensions will be given.
- You are permitted to discuss assignment questions *informally* with a partner. However, when you hand in the assignments you must indicate who you had discussions with, and all solutions must be written up separately. No "copied" solutions or computer code are allowed; copied assignments are considered to be plagiarism and are subject to severe penalties.
- It is recommended that you attempt to solve every question on your own. If you do use an external information source (a book or a research paper, for example), give an appropriate citation.
- Computational questions can be done using any desired programming tools, languages or calculators. Maple is **strongly recommended** as the easiest way to do the questions. Please include all source code, and sufficient output so I can verify the main steps in the computations.
- I am available to provide extra help or hints if you get stuck on a question.

Questions

In the questions below, numbered theorems, etc., refer to the mathematics notes on the course web page.

1. (a) Suppose that $G = (X, \cdot)$ is a cyclic group of order n. Prove that there are exactly $\phi(d)$ elements in G having order d, for any d dividing n. (Hint: use Theorem 1.22 along with the fact that every element can be expressed as a power of a generator.)
   (b) For every divisor d of 10008, determine the number of elements in $(\mathbb{Z}_{10009}{}^*, \cdot)$ having order d.
   (c) Find all elements in $(\mathbb{Z}_{10009}{}^*, \cdot)$ having order 72. Try to do this in an efficient way (i.e., not by an exhaustive search).
2. In the *RSA Cryptosystem*, we specify that $ab \equiv 1 \pmod{\phi n}$, where a and b are the decryption and encryption exponents, respectively. Suppose that $ab \equiv 1 \pmod{\lambda n}$, where $\lambda(n) = \phi(n)/\gcd(p-1, q-1)$. then prove that a and b still work correctly as decryption and encryption exponents for *RSA*. You only need to prove this for $x \in \mathbb{Z}_n{}^*$, though it is true for all $x \in \mathbb{Z}_n$. (Hint: use Remark 1.62 and Theorem 2.15.)
3. Prove the two statements in Theorem 1.36.
4. The purpose of this question is to implement three attacks on the *RSA Cryptosystem*. Further details about the attacks can be found in the textbook *Cryptography Theory and Practice, Third Edition*. I will post relevant sections from the textbook on the course website. Note that all the computations required for these attacks are *extremely fast* when implemented in Maple.

(a) The first attack can be carried out if the value of $\phi(n)$ is somehow revealed to an attacker. Since n is public, it is a simple matter for an attacker to compute p and q by solving a quadratic equation. You are required to carry out the attack on an instance of *RSA Cryptosystem* where n and $\phi(n)$ are as follows:

$n = 830892577313438492450346705008861812232734816257559195105330039974415727857032354336070902237316065623567990177909714846475311722928917736876038997323707780332218996621712606459714764337434967470056606232880417130973688537907387873512354863354163169918976169026130023738473899168235145408215280782350833627513$

$\phi(n) = 830892577313438492450346705008861812232734816257559195105330039974415727857032354336070902237316065623567990177909714846475311722928917736876038997323707595018948063796808134497403496282996630572813400264487154981925422989623841698252252680007506132154431804816283291586521163527968811494194785750612951117521$

(b) The second attack can be carried out if the decryption exponent, a, is revealed to the attacker (the encryption exponent, b, is public). The algorithm to factor n, given a and b, is presented in Algorithm 5.10. Note that this is a randomized algorithm, and it might be necessary to try a few different values of w until the algorithm succeeds. You are required to carry out the attack on the following instance of the *RSA Cryptosystem*:

$n = 855867310282100354595612457320077197528307639452895460750105596695485807329101436797829925645700893774265485865579390543649036773344957654576478932675936778058228123793758086480592321816013818686674153646264154496725366956284528387754732629057124622381546944917816890781114982568578978067970027095911246370831$

$a = 638006763320915794391171543647205501133635794555109100487196204885399889781384250458918574508400391571129138110688774416082623105449780942612170202734203144846256126892403053506803883761560308231727911978535022760531257722795359224569440542317082386038197294617098833175310591290027864165336390130302701683 7$

$b = 708038453858869235154880132976317330039001162933023133632704705866110384668515788774659341151303677896887027407375750530641681472453437576546219528998556625882643496032671206773906208893925632971949470447687550935109299112375252984512778515513689533555637589962340069486821387037663567542433577550156359608 45$

(c) The third attack can be carried out if the decryption exponent, a, happens to be "short" (in practice, this means that $a \ll n^{1/4}$, i.e., a has as most 1/4 the number of bits that n has). The algorithm to factor n when a is small, given n and b, is presented in Algorithm 5.11. This algorithm explicitly computes the convergents of the continued fraction of b/n. However, you can instead obtain these convergents directly from Maple (see the Maple hints I have provided on the course web site). For each convergent c_j/d_j, you just need to compute n' as described in the algorithm. If n' is an integer, then solve the quadratic equation and see if the roots are positive integers that are the factors of n. You will just keep trying successive convergents until the attack succeeds. If the attack fails, it means that the decryption exponent is not "short".

You are required to carry out the attack on the following instance of the *RSA Cryptosystem*:

$n = 1177266283402023652205772465354220471204515351844505120970680095098434453706684150481094064348630628189730182159750611597518359064443907341903562334318613950063281822318325915691633401653190076603005961761195401663947647170646661397229310973452262877019784478330693367563199441224160119504013024435126999530 49$

$b = 12855396565093252995255029034847247486297904562017933999145220378195963871757067226246161478038634307824358156709335945255042011876370681959464837724674810028047010881242413767772945174240561635676185186745741498210598696129908894924326088612170796012849343481735886428528720568619607804190975778287495934259$