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.)

   Answer: Let a be a generator of G, so $\mathsf{ord}(a) = n$. Let $n = kd$. We know that $\mathsf{ord}(a^i) = n/\gcd(n, i)$, so $\mathsf{ord}(a^i) = d$ if and only if $\gcd(n, i) = n/d = k$. This happens only if $i = k\alpha$ where $0 \leq \alpha \leq d-1$. Now, $\gcd(n, i) = \gcd(kd, k\alpha) = k\gcd(d, \alpha)$, so $\gcd(n, i) = k$ only if $\gcd(\alpha, d) = 1$. There are precisely $\phi(d)$ values of α such that $0 \leq \alpha \leq d - 1$ and $\gcd(\alpha, d) = 1$.

   (b) For every divisor d of 10008, determine the number of elements in $({\mathbb{Z}_{10009}}^*, \cdot)$ having order d.

   Answer: $10008 = 2^3 \times 3^2 \times 139$. There are $(3 + 1)(2 + 1)(1 + 1) = 24$ divisors of 10008, and for each such divisor d, there are $\phi(d)$ elements in $({\mathbb{Z}_{10009}}^*, \cdot)$ having order d. The result is as follows:

d	$\phi(d)$	d	$\phi(d)$	d	$\phi(d)$	d	$\phi(d)$
2	1	3	2	4	2	6	2
8	4	9	6	12	4	18	6
24	8	36	12	72	24	139	138
278	138	417	276	556	276	834	276
1112	552	1251	828	1668	552	2502	828
3336	1104	5004	1656	10008	3312		

(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).

Answer: Let a be a primitive element in $(\mathbb{Z}_{10009}{}^*, \cdot)$ (the smallest primitive element in $(\mathbb{Z}_{10009}{}^*, \cdot)$ is 11, which is a permissible value for a). From the proof of part (a), we know that $\mathsf{ord}(a^i) = 72$ if and only if $i = 139\alpha$, where $0 \leq \alpha \leq 71$ and $\gcd(\alpha, 72) = 1$ (i.e., $\alpha \equiv 1, 5 \pmod 6$). We have that $11^{139} \bmod 10009 = 9698 = \beta$, say, and hence the elements of order 72 are computed to be

$$\begin{array}{llll} \beta^1 = 9698 & \beta^5 = 3986 & \beta^7 = 3244 & \beta^{11} = 4155 \\ \beta^{13} = 4396 & \beta^{17} = 2360 & \beta^{19} = 6315 & \beta^{23} = 6086 \\ \beta^{25} = 4707 & \beta^{29} = 8383 & \beta^{31} = 3071 & \beta^{35} = 1931, \\ \beta^{37} = 311 & \beta^{41} = 6023 & \beta^{43} = 6765 & \beta^{47} = 5854 \\ \beta^{49} = 5613 & \beta^{53} = 7649 & \beta^{55} = 3694 & \beta^{59} = 3923 \\ \beta^{61} = 5302 & \beta^{65} = 1626 & \beta^{67} = 6938 & \beta^{71} = 8078 \end{array}$$

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.)

Answer: Let $d = \gcd(p-1, q-1)$. Then $\lambda(n) = (p-1)(q-1)/d$. Observe that $\lambda(n) \equiv 0 \pmod{p-1}$ and $\lambda(n) \equiv 0 \pmod{q-1}$. Suppose $x \in \mathbb{Z}_n{}^*$. Then, $x^{\lambda(n)} \equiv 1 \pmod{p-1}$ since $\lambda(n) \equiv 0 \pmod{p-1}$ and $x^{\lambda(n)} \equiv 1 \pmod{q-1}$ since $\lambda(n) \equiv 0 \pmod{q-1}$. We have that $ab = k\lambda(n) + 1$. therefore,

$$x^{ab} \equiv x^{k\lambda(n)+1} \equiv x^{k\lambda(n)} x \equiv 1^k x \equiv x \pmod p.$$

Similarly, $x^{ab} \equiv x \pmod q$. By the Chinese remainder theorem, $x^{ab} \equiv x \pmod n$.

3. Prove the two statements in Theorem 1.36.

Answer: Suppose Y is a subgroup of a group $(G, \cdot)$ and suppose $a \in G$. Consider the mapping $f : Y \to Ya$ defined by $f(y) = ya$, $y \in Y$. f is surjective because $ya = f(y)$ for any $ya \in Ya$. f is injective because $ya = y'b$ implies $y = y'$. Therefore f is a bijection and hence $|Y| = |Ya|$.

Now consider two cosets Ya and Yb where $Ya \cap Yb \neq \emptyset$. Suppose that $y_1 a = y_2 b$, where $y_1, y_2 \in Y$. Then $a = {y_1}^{-1} y_2 b = y_0 b$, where $y_0 = {y_1}^{-1} y_2 \in Y$. Therefore, for any $y \in Y$, we have $ya = yy_0 b \in Yb$. Hence $Ya \subseteq Yb$. Since $|Ya| = |Yb| = |Y|$, we have $Ya = Yb$.

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:

$n = 830892577313438492450346705008861812232734816257559195105330039974415727857032354336070902237316065623567990177909714846475311722928917736876038997323707780332218996621712606459714764337434967470056606232880417130973688537907387873512354863354163169918976169026130023738473899168235145408215280782350833627 51$

$\phi(n) = 830892577313438492450346705008861812232734816257559195105330039974415727857032354336070902237316065623567990177909714846475311722928917736876038997323707595018948063796808134497403496282996630572813400264487154981925422989623841698252252680007506132154431804816283291586521163527968811494194785750612951117 52$

Answer:

$p = 109279701453806504134911179496244402787546033854059677749198023595293320696145336537094301191303598613105799958759215353763069327699069428900235370084315573$

$q = 760335694790184003370511317718100355493512093519087155129510246702549628500299235650890454657341659312584098879729365989725709386348445915947963677981944 3$

(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*:

$n = 855867310282100354595612457320077197528307639452895460750105596695485807329101436797829925645700893774265485865579390543649036773344957654576478932675936778058228123793758086480592321816013818686674153646264154496725366956284528387754732629057124622381546944917816890781114982568578978067970027095911246370833$

$a = 638006763320915794391171543647205501133635794555109100487196204888539988978138425045891857450840039157112913811068877441608262310544978094261217020273420314484625612689240305350680388376156030823172791197853502276053125772279535922456944054231708238603819729461709883317531059129002786416533639013030270168373$

$b = 708038453858869235154880132976317330039001162933023133632704705866110384668515788774659341151303677896887027407375750530641681472453437576546219528998556625882643496032671206773906208893925632971949470447687550935109299112375252984512778515513689533555637589962340069486821387037663567542433577550156359608453$

Answer:

$p = 92292106551787924645284839581942369149833555199616414994622671526220467269986012136815621269013036920685713800536196635890046106358585137595112747055433793$

$q = 92734616454100223804316250947883987134877366055973137341831735923164504938589961766796170206094053030870223522272487571958125423292400918282932513175217177$

(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*:

$n = 1177266283402023652205772465354220471204515351844505120970680095098434453706684150481094064348630628189730182159750611597518359064443907341903562334318613950063281822318325915691633401653190076603005961761195401663947647170646661397229310973452262877019784478330693367563199441224160119504013024435126999530493$

$b = 12855396565093252995255029034847247486297904562017933999145220378195963871757067226246161478038634307824358156709335945255042011876370681959464837724674810028047010881242413767772945174240561635676185186745741498210598696129908894924326088612170796012849343481735886428528720568619607804190975778287495934259$

Answer:

$p = 9187462345423844484724945251636213564517313199168547196608462965099571523450698968437622434967107879789821890217198819834701873137945475318275730943851377$

$q = 1281383519344059873212607401466517280096153790292928010810327795889061000004748042838104628108057087111057661271315139378025273802958871696494170113120733 7$